ISSN 2949-2750

САНКТ-ПЕТЕРБУРГСКИЙ
ЮРИДИЧЕСКИЙ ИНСТИТУТ
(ФИЛИАЛ)
УНИВЕРСИТЕТА ПРОКУРАТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УГОЛОВНОЕ ПРАВО РОССИИ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

(преступления, совершаемые с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»))

IX Всероссийская научно-практическая конференция

Волженкинские чтения

Санкт-Петербург, 24 ноября 2023 года

МАТЕРИАЛЫ

Санкт-Петербург, 2024

САНКТ-ПЕТЕРБУРГСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ (филиал)
УНИВЕРСИТЕТА ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

УГОЛОВНОЕ ПРАВО РОССИИ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

(преступления, совершаемые с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»))

IX Всероссийская научно-практическая конференция

Волженкинские чтения

Санкт-Петербург, 24 ноября 2023 года

МАТЕРИАЛЫ

Санкт-Петербург
2024

УДК 34(08)
ББК 67я43
У26

Под общей редакцией **А. А. САПОЖКОВА**, заместителя директора Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидата юридических наук, доцента.

Ответственный за выпуск А. В. ЗАРУБИН, кандидат юридических наук, доцент.

Уголовное право России: состояние и перспективы (преступления, совершаемые
У26 с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)) : материалы IX Всероссийской научно-практической конференции «Волженкинские чтения», Санкт-Петербург, 24 ноября 2023 года / Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации ; под общ. ред. А. А. Сапожкова. — Санкт-Петербург : СПбИ (ф) УП РФ, 2024. — 1 CD-R (7,99 Мб). — Систем. требования: ПК с процессором Intel Core i3 и более ; 512 Mb и более ; CD/DVD-ROM дисковод ; Microsoft Windows XP и выше ; SVGA 800×600.16 bit и более ; Adobe Acrobat Reader 8.0 и выше. — Загл. с экрана. — Текст : электронный.

УДК 34(08)
ББК 67я43

Сборник издается в соответствии с оригиналом, подготовленным оргкомитетом конференции

Электронное научное издание

Уголовное право России: состояние и перспективы
(преступления, совершаемые с использованием средств массовой информации
либо электронных или информационно-телекоммуникационных сетей
(включая сеть «Интернет»))

IX Всероссийская научно-практическая конференция

Волженкинские чтения

Санкт-Петербург, 24 ноября 2023 года

М а т е р и а л ы

Подписано к использованию 27.02.2024. Уч.-изд. л. 35,5. Печ. л. 86,0.

Тираж 9 экз. Заказ 3/24.

1 электрон. опт. диск (CD-R). 7,99 Мб

Отдел научной информации и издательской деятельности
Санкт-Петербургского юридического института (филиала)
Университета прокуратуры Российской Федерации

Санкт-Петербургский юридический институт (филиал)
Университета прокуратуры Российской Федерации

191014, Санкт-Петербург, Литейный просп., 44

СОДЕРЖАНИЕ

П Р Е Д И С Л О В И Е

К МАТЕРИАЛАМ IX ВСЕРОССИЙСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ «ВОЛЖЕНКИНСКИЕ ЧТЕНИЯ»

УДК 34

А. П. СПИРИДОНОВ

С появлением сети «Интернет» его использование при совершении преступлений стало вопросом времени. Сегодня возможности информационно-телекоммуникационных сетей, включая сеть «Интернет», востребуются в противоправных целях, вследствие чего информационная сфера становится криминогенной, что создает угрозу информационной безопасности государства. Отражение этой угрозы нашло место в Стратегии национальной безопасности Российской Федерации[1].

В нормах уголовного права признак «с использованием сети “Интернет”» стал использоваться все чаще.

Совершение преступления посредством сети «Интернет», как правило, повышает общественную опасность преступления, что обусловило включение такого использования в качестве квалифицирующего признака состава преступления.

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

За последние восемь лет число преступлений, совершаемых с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), в стране выросло более чем в 25 раз. С января по сентябрь 2023 года в этой сфере зарегистрировано на 29,2 % преступлений больше, чем за аналогичный период прошлого года. С применением информационно-телекоммуникационных технологий совершается каждое третье преступление.

Немаловажную роль в противодействии киберпреступлениям играет уголовно-правовая политика, которая призвана обеспечить правовую основу для адекватного противодействия угрозам информационной безопасности, исходящим от противоправного поведения человека.

В декабре 2022 года Верховным Судом Российской Федерации обобщена судебная практика применения уголовного законодательства об ответственности за компьютерные и другие преступления, совершаемые с использованием информационно-телекоммуникационных сетей[1].

Особую значимость приобрели вопросы уголовно-правовой защиты информационной безопасности, в том числе путем совершенствования законодательства и правоприменительной практики.

В обстановке стремительного развития информационных технологий, создания глобальной информационной системы и, как следствие этого, вовлечения в данную сферу большого количества людей актуализируются вопросы снижения уголовно-правовыми средствами обусловленных человеческим фактором рисков в сфере использования средств массовой информации

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

либо электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», в частности вопрос совершенствования законодательной и правоприменительной оценки рассматриваемых преступлений.

В условиях изменяющегося и не в полной мере сформированного законодательства в информационной сфере сложные по технике описания бланкетные диспозиции абсолютно всех статей главы 28 УК РФ не дают полной ясности в понимании основных признаков большинства составов преступлений рассматриваемой категории.

Между тем залогом эффективной правоприменительной деятельности является правильное уяснение содержания уголовно-правовых запретов, сформулированных в вышеуказанной главе Уголовного кодекса Российской Федерации, с учетом правовых позиций судебной практики, видения определенности границ оснований уголовной ответственности за данные преступления, знания возможностей уголовно-правового реагирования на новые криминальные угрозы для информационной безопасности.

I. УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

УДК 343

А. Г. АЙВАЗЯН

УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ ЖИЗНИ, СВЯЗАННЫХ С САМОУБИЙСТВОМ ПОТЕРПЕВШЕГО, СОВЕРШЕННЫХ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

По данным Всемирной организации здравоохранения примерно каждые 40 секунд в мире происходит самоубийство. Самоубийства являются четвертой по значимости ведущей причиной смертности в возрастной группе 15–29 лет[1]. По официальным данным Росстата с 1994 г. по настоящее время уровень суицидальной смертности в России снижается[2]. Вместе с тем, по мнению некоторых исследователей, уровень латентной суицидальной смертности превышает данные официальной статистики примерно в 4 раза[3].

Настоящим потрясением для государства и общественности стала прокатившаяся в 2016 г. по стране волна детских самоубийств. По данным уполномоченного по правам ребенка в 2016 г. количество детских суицидов возросло

[1] Всемирная организация здравоохранения : офиц. сайт. URL: https://www.who.int/ru/news-room/fact-sheets/detail/suicide (дата обращения: 28.10.2022).

[2] Федеральная служба государственной статистики : офиц. сайт. URL: https//rosstat.gov.ru/sdg/data/goal3 (дата обращения: 15.11.2023).

[3] Пучнина М.Ю. Криминологическая оценка уровня латентных самоубийств // Вестник Московского университета МВД России. 2018. № 2. С. 66—69.

на 57%, основной причиной такого роста называли «группы смерти»[1]. Модераторы (организаторы) таких групп намеренно создавали сообщества в социальных сетях, основной тематикой которых являлось самоубийство. Используя манипулятивные и игровые методы, с помощью электронных и информационно-коммуникационных сетей (включая сеть «Интернет»), злоумышленники возбуждали у детей желание совершить самоповреждения (порезы на руках, ногах и т. д.), а также самоубийство.

Основной проблемой для правоприменителя являлся тот факт, что в большинстве случаев к самоубийству жертву приводили действия злоумышленников, не носящие насильственный характер (угрозы, жестокое обращение, систематическое унижение человеческого достоинства, предусмотренные диспозицией ст. 110 УК РФ, не применялись), что исключало возможность квалификации таких деяний по ст. 110 УК РФ (Доведение до самоубийства).

Поскольку уголовное законодательство Российской Федерации не содержало в себе норм, предусматривающих ответственности за такое поведение, лица совершающие подобные безнравственные и аморальные действия оставались безнаказанными, а несовершеннолетние продолжали совершать самоубийства. Сложившаяся ситуация потребовала внесения изменений в Уголовный кодекс Российской Федерации и в 2017 г. он был дополнен статьями 110.1 УК РФ (Склонение к совершению самоубийства или содействие совершению самоубийства) и 110.2 УК РФ (Организация деятельности, направленной на побуждение к совершению самоубийства). Кроме того, в статью 110 УК РФ (Доведение до самоубийства) также внесены изменения, она дополнена второй частью, включающей в себя ряд квалифицирующих признаков.

Единственным квалифицирующим признаком, который предусмотрен во всех составах преступлений суицидальной наклонности, является признак, предусматривающий совершение преступных деяний в публичном выступле-

[1] Кондрашова Н. Детский омбудсмен обвинила «группы смерти» в росте самоубийств на 57 %. // RBC : офиц. сайт. URL: https://www.rbc.ru/society/20/03/2017/58cf9b479a7947a44e938b51 (дата обращения: 31.08.2023).

нии, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»). По логике законодателя, преступления, совершенные публично, либо с использованием современных информационных технологий являются более общественно опасными, поскольку могут охватить больший круг жертв, а также облегчить и ускорить сам процесс совершения преступления.

Согласно сведениям о состоянии преступности, представленным Генеральной прокуратурой Российской Федерации, в 2022 году в России зарегистрировано 327 преступлений суицидальной направленности, в 2021 г. – 417 преступлений; в 2020 году – 388 преступлений. В доле общей преступности суицидальные преступления составляют объем в диапазоне от 0,01 % до 0,02 %. Это довольно-таки низкие показатели, однако до суда доходит еще меньшее число дел, а осуждаются и вовсе десятки человек по всей стране. Выявляемость и раскрываемость преступлений анализируемой категории ничтожно мала. Так, по результатам рассмотрения уголовных дел, связанных с самоубийством потерпевшего, в 2022 г. осужден 21 человек, в 2021 – 21 человек, 2020 – 8 человек[1].

Отдельной статистики по суицидальным преступлениям, совершенным в информационно-телекоммуникационных сетях (включая сеть «Интернет»), в России нет, однако изучение судебной практики по статьям 110, 110.1, 110.2 УК РФ, показало, что большинство случаев склонения к самоубийству, содействия самоубийству и организации деятельности, направленной на побуждение к совершению самоубийства, совершаются с использованием информационно-коммуникационных технологий.

Подобная практика, на наш взгляд, объясняется тем, что в настоящее время общение и коммуникации между людьми, в том числе подростками, происходят не в режиме реального времени, как говорится «с глазу на глаз»,

[1] Судебный департамент при Верховном Суде Российской Федерации : офиц. сайт. URL: https://cdep.ru/index.php?id=79&item=5669 (дата обращения: 07.08.2023).

а в онлайн формате. Огромный массив человеческой жизни перешел в онлайн формат, что очевидно сказывается и на преступности, совершаемой в интернет-пространстве. Об этом неоднократно заявляет известный криминолог Я.И. Гилинский, отмечая, что преступность ушла в «виртуальный мир Интернета»[1].

Так, в 2017 г. году гражданка Ш. узнав о существовании в сети «Интернет» игр суицидальной направленности, подражая другим лицам, создала собственную игру и разработала ее правила. Игроку предлагалось выполнять поэтапно задания, направленные на причинение себе телесных повреждений, после чего направлять куратору фотоотчет о выполненном задании. Информацию о своей игре злоумышленница распространила в социальной сети, а также в беседах по мобильному телефону другим несовершеннолетним. Кроме того, Ш. и ее брат Г. под вымышленными именами в социальной сети «ВКонтакте», осуществляли переписку с подростками, позиционируя себя кураторами игры суицидальной направленности и пытались вовлечь в нее несовершеннолетних. Распространяемая ими информация была доступна неопределенному кругу лиц. Собинским городским судом в 2018 г. Ш. и Г. признаны виновными в организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства, и призывов к совершению самоубийства, сопряженной с использованием информационно-телекоммуникационной сети «Интернет» и склонении к совершению самоубийства путем уговоров и предложений, совершенное группой лиц по предварительному сговору в отношении двух несовершеннолетних лиц в информационно-телекоммуникационной сети «Интернет»[2].

[1] Гилинский Я. И. Девиантология: социология преступности, наркотизма, проституции, самоубийств и других «отклонений» : монография. 4-е изд., исправ. и доп. СПб., 2021. С. 226—227.

[2] Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=29581838 (дата обращения: 16.11.2023).

При доведении до самоубийства также активно стали использоваться информационные технологии, в первую очередь «Интернет». Одним из самых распространенных способов доведения до самоубийства в информационно-телекоммуникационных сетях является публикация недостоверных сведений, порочащих честь и достоинство другого лица либо публикация интимных фотографий и видео потерпевших, полученных в ходе личной переписки со злоумышленником. Опаснейшим последствием таких публикаций является буллинг (с англ. «травля») со стороны пользователей сети «Интернет» и социальных сетей. Доведенная до отчаяния поступком злоумышленника жертва, вдобавок получает волну осуждения, негативных комментариев, отзывов; травля может перейти из онлайн формата в реальную жизнь. Подобные обстоятельства и приводят потерпевших к единственному на их взгляд, выходу, - самоубийству. Жертвами таких преступлений становятся как несовершеннолетние, так и взрослые мужчины и женщины[1].

Еще с 2012 г. в России стала популярной схема вымогательства денежных средств у молодых девушек. Различными способами злоумышленники вступали в диалог с девушками, втирались к ним в доверие, обещая хороший заработок в модельном бизнесе или в эскорт-услугах («escort», с англ. «сопровождение»), красивую и богатую жизнь, заработки за границей. Для продолжения сотрудничества девушки должны были выслать собеседнику свои откровенные фотографии и видео, так называемые «нюдсы». После получения этих файлов, злоумышленники начинали процесс вымогательства, угрожая девушкам публикацией откровенных снимков и видео в сети «Интернет». В случае отказа, данные файлы публиковались на специальном сайте, куда также прикреплялись скриншоты (screenshot, с анг. «снимок экрана») переписок с девуш-

[1] В Рязани 16-летний подросток совершил самоубийство из-за шантажа интимными фото // Аргументы и Факты. Рязань : сайт. URL: https://rzn.aif.ru/incidents/ryazanskiy_16-letniy_podrostok_pokonchil_s_soboy_iz-za_shantazha_intimnymi_foto (дата обращения: 15.11.2023) ; Преподаватель английского языка из Москвы покончила с собой после публикации фотографий на сайте по предоставлению эскорт-услуг // NEWS.ru : сайт. URL: https://news.ru/moskva/uchitel-anglijskogo-pokonchila-s-soboj-posle-publikacii-foto-na-eskort-sajte/ (дата обращения: 15.11.2023).

ками, которые согласны оказывать услуги интимного характер взамен на финансовое обеспечение[1]. Некоторые девушки не выдерживали такой психологической атаки и совершали суицид. Роскомнадзор неоднократно обращался в суд в защиту прав субъектов персональных данных, информация о которых была опубликована на интернет-ресурсах без их согласия[2]. По решению судов подобного рода сайты блокируются, однако каждый раз появляются новые ресурсы, распространяющие такую информацию.

По официальным данным за 2022 год Роскомнадзор совместно с профильными ведомствами заблокировал либо удалил более 61 тыс. материалов о способах совершения самоубийства и с призывами к нему[3]. Причем к таким материалам стали относить фильмы, книги, музыкальные произведения современных авторов или музыкантов двадцатого века.

Логика правоохранителей понятна, если не говорить о самоубийствах, не распространять информацию о способах их совершения, то их количество может сократиться. Но действительно ли, всему виной развитые информационные технологии и распространяемый в них контент?

В связи с резонансом, произошедшим в обществе после публикаций в СМИ сведений о самоубийствах детей, по инициативе Следственного комитета России в 2018 г. специалистами Санкт-Петербургского государственного университета проведено исследование «Саморазрушающее поведение подростков: причины и профилактика». В ходе исследования изучалось деструктивное поведение подростков, проводилась экспертиза материалов уголовных дел по преступлениям, связанным с суицидальным поведением несовершеннолетних, а также анализировались аспекты суицидального поведения детей, которое могло быть связано с активным освоением интернет-технологий и их

[1] Петров И. Срам себе режиссер: как шантажисты доводят девушек до суицида // Известия iz : портал. URL: https://iz.ru/876398/ivan-petrov/sram-sebe-rezhisser-kak-shantazhisty-dovodiat-devushek-do-suitcida (дата обращения: 15.11.2023).

[2] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : офиц. сайт. URL: https://rkn.gov.ru/news/rsoc/news30701.htm (дата обращения: 12.11.2023).

[3] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: офиц. сайт. URL: https://rkn.gov.ru/ (дата обращения: 15.11.2023).

пребыванием в социальных сетях. В результате: не выявлено ни одного случая самоубийства под влиянием «кураторов» или администраторов «групп смерти» в социальных сетях. Причинами суицидального поведения становились: буллинг, конфликт в семье или школе, прием психоактивных веществ, нарушение самооценки, потеря концепции будущего и др. По мнению исследователей формирование у несовершеннолетних саморазрушающего поведения зарождается чаще всего из-за семейного неблагополучия — жестокого обращения, безнадзорности и отсутствия доверительных отношений с родителями[1]. Находясь в неблагополучной атмосфере: дома и в школе, ребенок острее реагирует на раздражители из вне, которыми могут выступать и «группы смерти» и просто сверстники, которые по тем или иным причинам говорят о суициде. С этим исследованием трудно не согласиться, поскольку оно также подтверждается судебной практикой.

Так, из приговора Звериноголовского районного суда Курганской области следует, что гражданин П., обвиняемый в совершении преступлений, предусмотренных пп. «а», «в», «д» ч. 3 ст. 110.1 УК РФ, «будучи пользователем общедоступной социальной сети «ВКонтакте» в информационно-телекоммуникационной сети «Интернет», достоверно зная о повышенном интересе значительной части пользователей указанной социальной сети к темам самоубийства, депрессии и иного деструктивного контента (информации), используя свой телефон умышленно разместил общедоступную для неограниченного круга пользователей социальной сети «ВКонтакте» информацию суицидального характера, а также данные своей электронной страницы, тем самым завлекая лиц, в том числе несовершеннолетних, имеющих намерения совершить суицид, вступить с ним в переписку с целью дальнейшего склонения данных лиц к совершению самоубийства»[2].

---

[1] Санкт-Петербургский государственный университет : офиц. сайт. URL: https://spbu.ru/news-events/novosti/uchenye-spbgu-ni-odnogo-sluchaya-suicida-detey-pod-vliyaniem-administratorov (дата обращения: 14.11.2023).

[2] Приговор Звериноголовского районного суда Курганской области от 10 января 2019 г. по делу № 1-3/2019 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/1TI4EL3Mum16/ (дата обращения: 15.11.2023).

Приговором Люберецкого городского суда Московской области гражданин Г. признан виновным в совершении преступления, предусмотренного ч. 2 ст. 110.2 УК РФ. Из текста приговора следует, что Г. «будучи пользователем общедоступной социальной сети «ВКонтакте», достоверно зная о повышенном интересе значительной части пользователей указанной социальной сети к темам самоубийства, депрессии и иного деструктивного контента (информации), используя свой смартфон систематически размещал на в социальной сети общедоступную информацию суицидального характера, в том числе с использованием гиперссылок, объединяющих публичные сообщения определенной тематики, размещенные в информационно-телекоммуникационной сети «Интернет» (хештег), тем самым завлекал на свои страницы лиц, имеющих намерения совершить суицид, с целью дальнейшего склонения данных лиц к совершению самоубийства[1].

Таким образом, получается, что интерес к самоубийству и желание его совершить у потерпевших возникали еще до знакомства с злоумышленниками, они намеренно искали пользователей и сообщества, распространяющие информацию о суициде.

Самоубийство как социальный феномен всегда являлось спутником человеческой цивилизации. Самоубийства могут происходить на почве религиозных верований, в связи с утратой смысла жизни, потерей близкого человека, любовными неурядицами, проблем со здоровьем. Однако не каждый человек под давлением обстоятельств может принять решение о суициде. Некоторых людей трудности мотивируют, другие – отчаиваются и не видят благополучного исхода.

Существует также категория людей, которых к самоубийству могут подтолкнуть произведения искусства, музыка, литературные произведения, смерть кумиров и т.д. Одно самоубийство, широко освещенное в книгах,

[1] Приговор Люберецкого городского суда Московской области от 6 марта 2019 г. по делу № 1-74/2019 // Люберецкий городской суд Московской области : офиц. сайт. URL: https://luberetzy.mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=3856958&delo_id=1540006&new=0&text_number=1 (дата обращения: 14.11.2023).

прессе и иных источниках всеобщей информации, может спровоцировать волну самоубийств.

Так, например, после публикации в 1774 г. романа Гете «Страдания юного Вертера» по Европе прокатилась волна самоубийств[1]. Сюжет этого произведения заключался в том, что молодой человек по имени Вертер, страдая от неразделенной любви к замужней девушке, совершает самоубийство с помощью огнестрельного оружия. Такая же судьба ожидала произведение Н.М. Карамзина «Бедная Лиза», кульминацией которого выступило самоубийство главной героини, которая бросилась в Сергиев пруд, у стен Симонова монастыря[2]. Первую утопленницу нашли спустя всего неделю после выхода книги, после чего последовала череда самоубийств девушек. Чтобы прекратить эти массовые самоубийства в Российской империи придумали оригинальный метод сокращения числа самоубийств – это их высмеивание. Возле прудов и озер в городах Российской империи установили столбы с надписью: «Здесь в воду кинулась Эрастова невеста. Топитесь, девушки, в пруду довольно места». Этот простой способ оказался очень действенным и впоследствии волна самоубийств прекратилась.

Явление, возникшее после публикаций романов Гете и Н.М. Карамзина, социолог Д. Филипс в 1970 г. назвал синдромом или эффектом Вертера. Изучая это социальное явление, Филипс пришел к выводу, что сразу после публикации на первых полосах газет сообщений о самоубийстве число совершенных суицидов резко увеличивается. Причем именно в тех регионах, где трагический случай получил особенно широкую огласку. Получатся, что информация о совершенном суициде не останавливает потенциальную жертву, а наоборот провоцирует ее к подражанию.

Возможно пристальное внимание к теме подростковых суицидов, постоянно освещение таких случаев в СМИ, публичное обсуждение законодатель-

[1] Гете И. В. Страдания юного Вертера. М., 1981. 296 с.

[2] Карамзин Н. М. Избранные сочинения. В 2 т. Т. 1. Письма русского путешественника М. ; Л., 1964. С. 605—622.

ных инициатив, отягчающих ответственность злоумышленников за совершение преступлений против жизни, направленных на самоубийство потерпевшего, породили тот самый эффект Вертера и в современной России.

Спасут ли наше поколение от суицида запреты и блокировки сайтов, пропагандирующих суицид, запреты книг и музыкальных произведений, описывающих данное явление, трудно предсказать. Полагаем, что в первую очередь необходимо вести профилактическую работу с населением страны, развивать институт психологической помощи в России, ведь самоубийства – это не только проблема молодежи, пожилые люди, инвалиды и иные категории граждан также подвержены данному негативному явлению.

УДК 343

Е. Ю. АНТОНОВА

ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ: ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ

Развитие цифровых технологий создало новые криминальные возможности и оказало существенное влияние на способы совершения преступлений. Как писал Б.В. Волженкин, «научно-технический прогресс, к которому стремится человеческое общество и который невозможно остановить, влечет за собой и новые опасности для человечества и активно используется криминалитетом, берущим на вооружение средства, адекватные своему времени»[1].

В современных реалиях такими средствами совершения преступлений стали различные цифровые технологии, изменилось и место совершения отдельных преступлений, в качестве которого стало выступать цифровое пространство. Это, в свою очередь, оказало влияние на уголовно-правовую политику государства и модернизацию уголовного законодательства, что логично обусловлено современными вызовами, под которыми А.Э. Жалинский,

[1] Современные проблемы и стратегия борьбы с преступностью / Ю. М. Антонян, В. Н. Бурлаков, В. В. Вандышев [и др.] ; науч. ред. В. Н. Бурлаков, Б. В. Волженкин. СПб., 2005. С. 213.

понимал «существующие потребности в обновлении законодательства, т. е. в его адаптации к изменениям, происходящим в обществе». Одним из оснований такого вызова является «причинение или угроза причинения реального ущерба гражданам, обществу, государству»[1].

В результате этого процесса основные, квалифицированные и особо квалифицированные составы преступлений стали дополняться соответствующим признаком – их совершение «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»; «с демонстрацией в информационно-телекоммуникационных сетях, (включая сеть «Интернет»)». Но всегда ли это оправдано?

Согласимся с мнением А.И. Коробеева и А.И. Чучаева, которые справедливо отмечают, что «уголовная политика … должна основываться на четком и ясном понимании того, каких изменений в состоянии, структуре и динамике преступности можно будет добиться, совершенствуя соответствующие институты и нормы»[2]. При этом основополагающей целью модернизации уголовного закона является удержание преступности в контролируемых государствах рамках, снижение конкретных видов преступной деятельности, в нашем случае, реализуемой в цифровом пространстве или с использованием цифровых технологий.

Важно иметь в виду, что любые изменения в уголовном законодательстве должны быть научно обоснованными; криминологически и социально обусловленными, последовательными и системными. Только при соблюдении данных условий можно выработать оптимальные, эффективные механизмы защиты личности, общества и государства от преступных посягательств[3]. Для принятия соответствующих уголовно-политических решений,

---

[1] Жалинский А. Э. Избранные труды. В 4 т. Т. 3. Уголовная политология. Сравнительное и международное уголовное право / сост. К. А. Барышева, О. Л. Дубовик, И. И. Нагорная, А. А. Попов ; отв. ред. О. Л. Дубовик. М., 2015. С. 41.

[2] Коробеев А. И., Чучаев А. И. Перспективы развития уголовно-правовой политики России: поиски реальной модели // Государство и право. 2023. № 8. С. 96—105.

[3] Антонова Е. Ю. Уголовно-правовая политика и качество уголовного закона // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции, г. Москва, 25—26 января 2018 года / Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). М., 2018. С. 29—32.

необходимо, в том числе установить, что криминализируемое деяние или установление дополнительного признака в уже криминализированное деяние должны обладать высокой степенью общественной опасности, быть относительно распространенными, обусловлены детерминантами, делающими невозможными их устранение другими, менее репрессивными способами.

Ключевым основанием криминализации деяний является характер и степень их общественной опасности. В настоящее время законодатель, как правило, усиливает ответственность за преступления, совершаемые в цифровом пространстве или с использованием цифровых технологий. Отсюда возникает вопрос всегда ли использование таких технологий и площадок может привести к изменению степени общественной опасности преступления?

Исследования показывают, что не во всех случаях увеличение распространенности деяний является оправданным основанием для установления роста их общественной опасности и, как следствие, отнесения преступления к категории более тяжких[1]. Е.А. Русскевич иллюстрирует это на примере действий по созданию вредоносной компьютерной программы, полагая, что оно не всегда представляют большую общественную опасность, нежели ее фактическое использование, и тем более распространение (например, изготовление такой программы из профессионального интереса без намерения его дальнейшего использования)[2].

Отсутствие должного понимания особенностей, в том числе технических, совершения преступлений в цифровом пространстве или с использованием цифровых технологий, также приводит к неверной оценке степени общественной опасности деяний и соответствующим законодательным решениям, только усложняющим судебно-следственную практику и к спорам в доктрине

[1] Вельтмандер А. Т. Общественная опасность преступлений, совершенных с использованием информационно-коммуникационных (цифровых) технологий // Уголовная политика в условиях цифровой трансформации : сборник статей материалов II Всероссийской научно-практической конференции, г. Казань, 27 апреля 2023 г. / Российский государственный университет правосудия (Казанский филиал). Казань, 2023. С. 11—16.

[2] Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. 2-е изд., перераб. и доп. М., 2022. С. 158.

уголовного права, в том числе относительно квалификации таких деяний. В качестве наглядного примера можно привести ст. 258.1 и 260.1 УК РФ, в которых законодатель предусмотрел ответственность в одной части нормы за описанные в диспозициях действия с использованием СМИ либо электронных или информационных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», а в другой – за совершение этих же деяний с публичной демонстрацией, в том числе в СМИ или информационно-телекоммуникационных сетях (включая сеть «Интернет»).

Разграничение названных признаков вызывает сложности как с теоретической, так и практической позиций. Это приводит к тому, что правоприменитель в идентичных ситуациях квалифицирует деяние по разным частям нормы, что нарушает принцип справедливости, тем более что законодатель увидел разницу в степени общественной опасности данных признаков, установив, с одной стороны, выше ответственность за деяние, связанное с «публичной демонстрацией» указанных в статьях предметов в, в том числе на цифровых площадках, а, с другой стороны, добавление иных квалифицирующих признаков к названным (таких как совершение этих же деяний с использованием служебного положения, в соучастии) увеличивает степень общественной опасности деяний, совершенных «с использованием» данных площадок, что также не может не вызывать вопросы[1].

Деяния, связанные с распространением в цифровом пространстве различной деструктивной информации/дезинформации (например, призывы к само-

[1] Антонова Е. Ю. Уголовная политика в сфере охраны особо ценных диких животных и водных биологических ресурсов // Байкальский природоохранный форум : сборник статей Международной научно-практической конференции, г. Иркутск, 9 июня 2023 года / Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации. Иркутск, 2023. С. 164—167 ; Её же. Норма об ответственности за посягательства на особо ценные растения и грибы: некоторые вопросы законодательной техники // Енисейские политико-правовые чтения : сборник трудов XV Всероссийской научно-практической конференции с международным участием, г. Красноярск 29—30 сентября 2023 г. / Сибирский федеральный университет, Юридический факультет ; отв. ред. Г. Л. Москалев. Красноярск, 2023. С. 23—27.

убийству, к террористической, диверсионной или экстремистской деятельности, реабилитация нацизма и др.), обладает достаточной степенью общественной опасности для установления соответствующего признака в основном или квалифицированном/особо квалифицированном составах.

Это обусловлено, во-первых, особенностями предмета таких преступлений, в качестве которого выступает цифровая информация, выраженная «в виде сведений (сообщений, данных), обращающихся в информационно-телекоммуникационных устройствах, их системах и сетях». «Именно противоправным, виновным воздействием на нее» детерминируется вред, причиняемый общественным отношениям[1].

Во-вторых, объективная сторона таких преступлений реализуется на просторах цифровых площадок, причем за считанные секунды на неопределенно широкую территорию и аудиторию.

Важным вопросом уголовно-правовой политики в части криминализации рассматриваемых преступлений является выработка и использование единой терминологии. В настоящее время законодатель необоснованно варьирует терминологией формулируя рассматриваемый признак, употребляя такие конструкции как: «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», «через ... электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»)» или «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», либо «с публичной демонстрацией, в том числе в информационно-телекоммуникационных сетях (включая сеть «Интернет»)». При этом если на законодательном уровне раскрывается понятие «информационно-телекоммуникационная сеть», то категории «электронные сети» и «Интернет» нормативно нигде не закреплены.

[1] Бегишев И. Р., Бикеев И. И., Галимов А. Г. Признаки преступления в сфере обращения цифровой информации // Международный форум KAZAN DIGITAL WEEK — 2021 : сборник материалов, г. Казань, 21—24 сентября 2021 года. Казань, 2021. Ч. 1. С. 261—268.

Поднимается и вопрос о соотношении понятий «информационные технологии», «цифровые технологии», «компьютерная информация» и др.[1] В научных публикациях встречаются термины «кибернетические технологии», «информационные технологии», «высокие технологии» (технологии искусственного интеллекта), «IT-технологии» и др.

Данное обстоятельство существенно осложняет правоприменительную практику. Для единообразия применения норм уголовного закона требуется определиться с понятийно-категориальным аппаратом и дать легальное определение категорий, используемых в нормативных правовых актах.

Кроме того, следует иметь в виду, что с точки зрения возможностей представляется очевидным ожидать роста преступности в цифровом пространстве в условиях, когда все больше людей погружаются в него. Однако можно ли утверждать, что такая тенденция одинакова для всех типов преступлений? Думается, что нет.

Утверждается, что в отдельных случаях совершение преступлений в цифровом пространстве или с использованием цифровых технологий является краткосрочным явлением, отдельные виды преступлений могут просто вернуться к первоначальной тенденции или даже находиться в пределах нормальной изменчивости преступности[2]. В некоторых случаях цифровое пространство используется в процессе приготовительных действий (например, для приискания орудий и средств совершения преступлений, приискания соучастников, сговору между ними, приискания жертв и т. д.), тогда как само преступление совершается в офлайн-среде.

Так, исследования показывают, что распространение сети «Интернет» не может привести к увеличению, например, интенсивности террористических

---

[1] Голенко Д. В. Особенная часть Уголовного кодекса Российской Федерации и цифровые технологии // Цифровые технологии и право : сборник научных трудов I Международной научно-практической конференции, г. Казань, 23 сентября 2022 г. : в 6 т. / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. Казань, 2022. Т. 2. С. 54—56.

[2] Kemp S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., Díaz-Castaño, N. Empty Streets, Busy Internet : A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19 // Journal of Contemporary Criminal Justice. 2021. Vol. 37(4). P. 480—501.

атак, поскольку непосредственные исполнители полагаются на тесные личные офлайн-связи[1].

Резюмируя сказанное, отметим, что в процессе формирования уголовно-правовой политики по противодействию преступлениям, совершаемых в цифровом пространстве или с использованием цифровых технологий, требуется серьезный научный анализ всех оснований криминализации (изменения интенсивности пенализации) таковых. Кроме того, в настоящее время требуется ревизия всего уголовного закона в целях выявления пробелов уголовно-правовой защиты отдельных объектов от преступных посягательств, совершаемых в цифровом пространстве или с использованием цифровых технологий, определения потребности усиления или смягчения ответственности в конкретных случаях.

Важно иметь в виду и то, что мер уголовно-правового характера недостаточно для противодействия таким преступлениям. Для достижения положительного результата требуется усиление сил и средств на воспитательно-просветительскую деятельность, в том числе в цифровом пространстве, обучение сотрудников правоохранительных органов, выявляющих и расследующих преступления, совершаемых в цифровом пространстве или с использованием цифровых технологий, расширение полномочий сотрудников правоохранительных органов для обеспечения четкого и эффективного контроля цифрового контента и др.

УДК 34

А. С. АРТЕМЬЕВА

ВОПРОСЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРЕДОСТАВЛЯЕМЫХ ПОЛЬЗОВАТЕЛЯМИ СЕТИ «ИНТЕРНЕТ»

XXI век — время развития и стремительного распространения информационных технологий. Подобно законам экономики, где спрос рождает предложение, новая потребность и новая технологическая реакция рождаются из тех

[1] Khokhlov N., Korotayev A. Internet, Political Regime and Terrorism : A Quantitative Analysis // Cross-Cultural Research. 2022. Vol. 56(4). P. 385—418.

объятий, в которые заключает нас уже существующая технология; и этот процесс не прекращается[1].

На каждом историческом этапе своего развития человечество стремится оптимизировать собственные ресурсы, затрачиваемые на удовлетворение потребностей, связанных вначале с выживанием, затем жизнеобеспечением, а сегодня — с созданием комфортных условий жизнедеятельности, досуга и коммуникации. Внедрив достижения научно-технического прогресса в хозяйственную, промышленную и производственную сферы, человек стремится усовершенствовать и другие стороны бытия, начиная с образовательного, спортивного, культурно-развлекательного сегментов, заканчивая вопросами бытовой активности, передвижения, общения и отдыха. Образ жизни и профессиональная деятельность становятся вариативными. В результате экономика и социальная политика ориентируются на возможности технологического развития и науки, где человек становится контролирующим звеном в мире высоких технологий. Будучи современниками постиндустриального общества, где основным производственным ресурсом является информация, мы наблюдаем характерно высокие темпы развития социальных и экономических процессов. При этом в постоянно трансформирующихся условиях качественные изменения претерпевает как сама информация, так и способы работы с ней.

Президент России Владимир Владимирович Путин призывает массово внедрять искусственный интеллект в различные сферы жизнедеятельности, отдавать предпочтение развитию «сквозных технологий», которые бы оказывали влияние на развитие отдельных отраслей[2].

К таким технологиям в первую очередь отнесен искусственный интеллект наряду с цифровой средой в рамках развития информационного общества.

---

[1] Маклюэн, Г. М. Понимание медиа : Внешние расширения человека / пер с англ. В. Николаева ; заключительная статья М. Вавилова. М., 2003. 464 с.

[2] ТАСС : информ. агентство России : сайт. URL: https://tass.ru/ekonomika/7416737 (дата обращения: 18.11.2023).

Конкурентным преимуществом на мировом рынке обладают государства, отрасли экономики которых основываются на технологиях анализа больших объемов данных. Наша страна, идя по заданному направлению и успешно реализуя Стратегию развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденную Указом Президента Российской Федерации от 9 мая 2017 г. № 203, заняла прочные позиции в международных рейтингах, подтверждая свое место среди ведущих стран мира.

По итогам 2021-2022 годов Россия заняла 14 место в подготовленном «Ростелекомом» рейтинге стран по уровню технологического развития, вошла в топ-10 стран по научной и изобретательской активности в сфере робототехники и квантовых технологий, также оказалась в «десятке» по изобретательской активности в сфере искусственного интеллекта.

В 2023 году Россия продемонстрировала не меньшие успехи и заняла пятое место в рейтинге стран с самым развитым информационным обществом, что подтверждает активное использование современных технологий и доступность интернет-сервисов для населения, а также второе место в рейтинге стран с самым высоким уровнем образования.

Россия значительно продвинулась вперед в международных рейтингах экономического развития, таких как Глобальный индекс конкурентоспособности (GCI) — с 30 позиции в 2022 году на 25 позицию в текущем году, в Индексе человеческого развития (HDI) — с 50-ой позиции в 2022 году на 46 позицию в текущем.

Такое улучшение позиций отражает эффективные усилия правительства России по развитию цифровой экономики, повышению качества жизни граждан и укреплению социальной защищенности. Информационное общество в современной России характеризуется широким распространением и доступностью мобильных устройств, беспроводных технологий, сетей связи, возможностью предоставления государственных и муниципальных услуг в электронной форме. Информационные и коммуникационные технологии стали ча-

стью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Кроме того, они становятся обыденностью и для каждого из нас при ежедневном пользовании гаджетами, оформлении покупок, производстве платежей, обеспечении доступа в жилище и т. п.

Однако, технологические новшества нельзя рассматривать только лишь в позитивном ключе прогресса. Как справедливо замечал Нейл Постман: «Всякая технология — это и бремя, и благо: никогда не «или—или», а всегда то и другое».

На первом в России Национальном конгрессе по когнитивным исследованиям, искусственному интеллекту и нейроинформатике академик Константин Анохин - один из руководителей проекта «Мозг и информация: От естественного интеллекта к искусственному» — определил искусственный интеллект следующим образом: «...на самом деле современный ИИ — это «черный ящик». Мы знаем, что на его входе есть задача, а на выходе — решение. А что происходит внутри, в десятках и сотнях скрытых слоев искусственной нейронной сети - пока мало понятно»[1].

Люди давно предоставляют коммерческим организациям отпечатки пальцев, биометрические параметры лица, голоса, в некоторой степени беспечно, не заботясь о последствиях, но стремясь сиюминутно завладеть тем или иным товаром, оформить услугу, в то время как операторами этих данных долгие годы могли быть непроверенные компании, включая иностранные неконтролируемые Российской Федерацией фирмы.

Сегодня хранение и использование биометрических персональных данных становится все более прозрачным, ответственным и контролируемым на государственном уровне процессом. Об этом свидетельствует создание Единой биометрической системы (ЕБС), внедрению которой предшествовали задачи, озвученные главой государства: «Я считаю, что такая предельно личная

[1] Национальный конгресс по когнитивным исследованиям, искусственному интеллекту и нейроинформатике : сборник тезисов конференции / Российская ассоциация искусственного интеллекта ; под общ. ред. В. Л. Ушакова, Д. А. Юдина. М., 2020. 139 с.

информация должна храниться в единой государственной системе биометрической идентификации. То есть государство должно взять на себя ответственность за ее хранение и при этом обеспечить свободный доступ к ней [информации] банкам, другим организациям, но в полностью зашифрованном виде, исключающем любое внешнее вмешательство, открытый доступ к персональным данным человека»[1].

Таким образом, на пути к информационному, телекоммуникационному и цифровому развитию государство осуществляет комплексный подход, включающий как технологическое совершенствование, так и обеспечение основ Конституции Российской Федерации, регламентирующей право каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

От степени защищенности биометрических персональных данных граждан Российской Федерации зависит и степень обеспечения национальной безопасности государства в целом. Среди национальных интересов современной России Стратегией национальной безопасности Российской Федерации выделяются развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия, а также устойчивое развитие российской экономики на новой технологической основе[2].

Из описанного следует, что использование биометрических персональных данных на современном этапе развития носит необходимый в долгосрочной перспективе, масштабный и важный характер, а значит требует разработки широкого и эффективного комплекса мер по защите такого рода информации. Для точного отражения мер всесторонней защиты биометрических

[1] ТАСС : информ. агентство России : сайт. URL: https://tass.ru/obschestvo/12909643 (дата обращения: 20.11.2023).

[2] Стратегия национальной безопасности Российской Федерации : утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

персональных данных, видим необходимым определить, что требует защиты и от чего.

В соответствии с ч. 1 ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» биометрическими персональными данными являются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. Среди ученых существуют разные точки зрения о том, что именно относить к биометрическим персональным данным.

Так, Н. И. Платонова выражает несогласие с законодательной формулировкой, относя к биометрическим данным именно биологические особенности человека, тогда как физиологические определяются научной теорией как составная часть биологических, а следовательно постановка законодателем между этими понятиями знака «равно» является, по мнению ученого, логической ошибкой[1].

С позиции Г. Г. Камаловой к биометрическим персональным данным относится дактилоскопическая, антропометрическая, габитоскопическая, генотипическая информация, а также строение папиллярных узоров, метрика тела и отдельных его частей, особенности внешнего облика (красная кайма губ, строение радужной сетчатки глаза, кровеносных сосудов глазного дна), особенности артикуляции речевого аппарата и голоса, походки, жестикуляции, мимики, письма и т. д.[2].

Классификация биометрических параметров в зависимости от их значимости для идентификации предлагается Е. Г. Барковской: 1) сведения о физических и физиологических особенностях человека, обладающие высокой степенью устойчивости; 2) биологические параметры человека, которые имеют меньшую идентификационную значимость ввиду меньшей уникальности, устойчивости и более высокой изменчивости; 3) физиологические параметры

[1] Платонова Н. И. Современные правовые подходы к пониманию биометрических данных // Информационное право. 2018. № 1. С. 22—26.

[2] Камалова Г. Г. Биометрические персональные данные: определение и сущность // Информационное право. 2016. № 3. С. 8—12.

человека, проявляющиеся в динамике и характерные для подсознательных движений; 4) привычки и навыки, проявляемые в ходе деятельности[1].

Как видим, приведенные позиции авторов не столько противоречат друг другу, сколько взаимодополняют. Главная идентификационная ценность биометрических показателей в их устойчивости и уникальности. Следовательно небезопасный подход к предоставлению, обработке, использованию и хранению биометрических персональных данных влечет значительные риски, от угрозы личной безопасности гражданина до подрыва суверенитета целого государства с системой его национальной безопасности.

Выделим основные направления угроз в рамках использования биометрических персональных данных:

1. Преступные деяния.

В связи со стремительным распространением информационно-коммуникационных технологий меняется и характер преступности. С каждым годом все большее количество преступлений совершаются с помощью компьютерной техники и ИТС. Интернет-преступность растет быстрыми темпами.

Информационная инфраструктура позволяет злоумышленникам действовать скрытно, не оставляя прямых координат, совершать преступные действия из любой точки мира. Согласно статистическим сведениям МВД России о состоянии преступности за девять месяцев текущего года, с использованием информационно-телекоммуникационных технологий совершается каждое третье преступление. В этой сфере за отчетный период зарегистрировано на 29,2 % преступлений больше, чем с января по сентябрь 2022 года[2]. Данные свидетельствуют о том, что наблюдается значительный прирост преступлений, совершаемых в сфере, уязвимой к злоупотреблению, манипуляции и утечке персональных данных.

---

[1] Барковская Е. Г. Концепция создания криминалистических учетов на основе баз данных биометрии // Общество и право. 2009. № 1 (23). С. 277.

[2] Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/news/item/42987324?year=2023&month=11&day=18 (дата обращения: 20.11.2023).

2. Проблемы технического характера.

С технической точки зрения биометрические персональные делятся на две категории:

— непосредственно «сырые» биометрические данные — фотография в системе контроля и управления данными, снятая в соответствии с ГОСТом, следы отпечатков пальцев, запись голоса и т. д.;

— результаты математических вычислений.

Утечка непосредственных биометрических данных чревата возникновением 1 группы угроз, а именно использованием утерянной / добытой информации посредством создания на ее основе дипфейков для совершения мошеннических действиях, незаконного проникновения на охраняемые объекты, оформления несанкционированных финансовых операций, компрометации тайной переписки и т. д.

То есть в случае кражи биометрических персональных данных злоумышленники имеют возможность «подделать» личность человека, и совершать от его имени юридически значимые действия.

Что же касается математических моделей, то завладение ими без доступа к непосредственным образцам биометрии не принесет подобных рисков.

3. Некомпетентность субъектов использования биометрических персональных данных.

В данном случае, речь идет о системе подготовки квалифицированных кадров, способных не только благодаря высокому уровню технической подготовки, но и по своим моральным, этическим представлениям и личным качествам работать с биометрическими персональными данными граждан, осознавая ответственность выполняемой деятельности не только перед клиентом и субъектом персональных данных, но и перед буквой закона, в том числе Конституции Российской Федерации, а также безопасностью общества и государства.

4. Недоверие со стороны населения.

Данный риск прямо пропорционален росту первых трех направлений угроз, а также может проистекать из низкой просвещенности отдельных кате-

горий граждан о возможности и удобстве пользования банковскими и государственными услугами на базе предоставления системам биометрических персональных данных. Рост недоверия среди населения к внедряемым технологиям способствует замедлению процессов развития цифровой экономики, информационного общества, а значит и снижению конкурентоспособности государства на мировой арене, что неблагоприятным образом отразится на качестве международных отношений, а значит явится угрозой и внутренней нестабильности.

Разбив возможные угрозы по основным направлениям, предлагаем к разработке следующий комплекс мер защиты биометрических персональных данных:

1. Уровень предупреждения преступных посягательств и борьбы с преступностью:

— интеграция ЕБС с автоматизированными системами учетов правоохранительных органов;

— совершенствование административного и уголовно-правового законодательства применительно к сфере использования биометрических персональных данных;

— виктимологическая профилактика среди граждан, предоставляющих биометрические персональные данные;

2. Уровень технического обеспечения безопасности:

— отлаживание и совершенствование механизмов защиты, разработанных Минцифрой;

— делегирование как можно большего числа операций искусственному интеллекту во избежание рисков, вызванных человеческим фактором;

— подготовка квалифицированных специалистов в области информационной безопасности, в том числе в правоохранительных органах, и создание для них достойных условий труда.

3. Уровень кадровой политики:

— воспитательная и просветительская работа с кадровым резервом на должности, связанные обработкой биометрических персональных данных на протяжении всех этапов подготовки;

— совершенствование механизма отбора кандидатов на работу с биометрическими персональными данными с точки зрения соответствия их личных морально-нравственных качеств предстоящей деятельности;

— воспитательная и просветительская работа с действующими сотрудниками в сфере обработки биометрических персональных данных;

4. Уровень работы с населением:

— информирование населения о современных и удобных способах совершения банковских операций, обращения в государственные и муниципальные органы, пользования услугами общественного транспорта и т. д.;

— правовое просвещение по рассматриваемому вопросу и информирование о безопасности современных технологий на уровне государственных услуг и банковского сектора.

— разработка и регулярное разъяснение гражданам алгоритма действий в случае обнаружения ими угрозы утечки биометрических персональных данных.

Такой комплексный подход к обеспечению безопасности биометрических персональных данных, на наш взгляд, послужит прочным фундаментом к бесперебойному развитию информационно-телекоммуникационной, цифровой и инновационно-технологической сфер без ущерба суверенитету и национальной безопасности Российской Федерации на долгие годы вперед.

УДК 343

М. В. БАРАНЧИКОВА

ТРАНСПОРТНЫЕ СРЕДСТВА КАК ПРЕДМЕТ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В последние годы мошенничество является самым распространенным преступлением, совершаемым с использованием информационно-телекоммуникационных сетей. Его современные виды отличаются значительным разнообразием и постоянно модифицируются.

Особым предметом мошенничества выступают транспортные средства, а также связанные с их приобретением, использованием и обслуживанием денежные средства. Такое мошенничество все чаще совершается с помощью информационно-телекоммуникационных сетей. Его инновационные способы реализуются в рамках взаимодействия пользователей сети «Интернет», в сфере безналичных расчетов.

Онлайн-оборот транспортных средств и услуг осуществляется все чаще, а автопроизводители планируют сделать онлайн основным каналом продаж на российском рынке. Начиная со сделок купли-продажи транспортных средств до управления ими в дорожных условиях, процессе эксплуатации и страхования возможно незаконное вмешательство в оборот денежных средств, связанных с их использованием.

Тенденцией современного российского авторынка является значительный рост цен на автомобили. По данным Росстата, новые российские автомобили подорожали в 2022 году на 29,65 %, новые иномарки — на 39,11 %, а подержанные автомобили — на 6,75 %. Темп роста цен в последние два года составил 45,3 % новых отечественных автомобилей, 78,7 % новых иномарок, 47,9 % подержанных автомобилей[1].

Несмотря на увеличение стоимости транспортных средств спрос на них остается достаточно устойчивым, отмечается высокая клиентская активность на авторынке. Поскольку предпосылок для изменения тренда пока нет, в условиях значительного сокращения предложений новых автомобилей, дефицита их определенных моделей, прогнозируется, что такая ситуация благоприятно отразится на рынке автомобилей с пробегом.

С 2022 по 2023 годы количество автомобилей, реализованных на вторичном рынке, превысило объем проданных новых моделей более чем в два раза[2].

---

[1] Рынок авто – 2023 // Национальное Рейтинговое Агентство : сайт. URL: https://www.ra-national.ru/wp-content/uploads (дата обращения: 15.09.2023).

[2] Дашкова А. С. Проблематика возврата автомобилей, похищенных путем мошенничества, потерпевшему: аспект противостояния виктимности жертвы и добросовестности приобретателя. Пути превенции инцидента // Российский следователь. 2021. № 12. С. 16—19.

За девять месяцев 2023 года продажи автомобилей на вторичном рынке в России выросли на 23,6 % по сравнению с показателями 2022 года. Только в сентябре 2023 года рост составил 10,9 %[1].

Концентрирование на направлении «автомобили с пробегом», трансформация сделок купли-продажи автотранспорта в направлении роста числа онлайн-режимов, оказываются тесно связанными с мошенничеством.

Популярными способами мошенничества на вторичном рынке транспортных средств остаются осуществляемые в ходе их купли-продажи подделка документов, искажение данных о комплектации, пробеге, умолчание о наличии обременений, и даже подмена автомобиля «двойником».

Мошенничества совершаются путем размещения на сетевых ресурсах объявлений о продаже таких транспортных средств, доступ к которым может получить неопределенное количество лиц. Другим вариантом является направление личного сообщения на любом из сетевых ресурсов или приложений, использующих информационно-телекоммуникационную сеть для передачи информации и имеющих функционал, позволяющий пользователям обмениваться сообщениями.

Как мошенничество по ст. 159 УК РФ квалифицируется хищение чужого имущества или приобретение права на чужое имущество, если оно осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет», состоит в создании поддельных сайтов, использовании электронной почты[2].

Сеть выступает средством коммуникации между преступником и жертвой, где распространение ложной информации увеличивает вред за счет отсутствия физических ограничений для преступника, полуавтоматического или автоматического совершения мошенничества.

---

[1] Аналитики «Автостата» зафиксировали рост продаж на 10,9 % на вторичном рынке РФ // За рулем : сайт. URL: https://www.zr.ru/content/news/948103-analitiki-avtostata-zafiksir (дата обращения: 15.09.2023).

[2] О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 : текст с изм. и доп. на 15 дек. 2022 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Мошенничество состоит в создании фейковых сайтов, групп в соцсетях и каналов в мессенджерах, которые якобы специализируются на подборе, покупке и таможенном оформлении автомобилей из-за границы. Пользователей часто убеждают перевести аванс за доставку автотранспорта из Японии, Казахстана или Китая, после чего преступники перестают выходить на связь, а клиента блокируют[1].

Число регистраций доменов, связанных с покупкой и продажей автомобилей, ежегодно растет. Их появление связано с тем, что многие российские карты не работают за границей. Соответственно у людей нет возможности взаимодействовать с поставщиком напрямую, и они пользуются услугами третьих лиц.

Часть из зарегистрированных сайтов принадлежит реальным компаниям, посредникам, занимающимся параллельным импортом, а другая - используется мошенниками. Последние могут осуществить незаконные сделки, похищать деньги с банковских счетов, получать доступ к кредитным картам или заниматься идентификационным мошенничеством. Кибермошенничество часто приводит к значительным финансовым потерям для жертв[2].

Информационно-телекоммуникационная сеть используется непосредственно при совершении преступления как некий инструмент, который позволяет преступнику оставаться неизвестным и наносить более серьезный ущерб объекту противоправного посягательства[3].

Мошенничество с использованием такой сети связано с созданием поддельных сайтов, размещением вредоносных вложений, фишинговых ссылок, переход по которым приводит к незаконному доступу в личные кабинеты, банковской карте потерпевшего.

---

[1] Тачки сгущаются: россиян массово обманывают с перегоном авто из-за рубежа // Autonews : сайт. URL: https://www.autonews.ru/news (дата обращения: 15.09.2023).

[2] Белодед Д. Р. Некоторые психологические особенности жертв преступлений, совершаемых с использованием цифровых технологий // Виктимология. 2023. Т. 10, № 3. С. 327.

[3] Кочои С. М. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей. М., 2023. С. 19.

В отличии от случаев предоставления самими потерпевшими мошенникам реквизитов банковских карт, паролей и СМС-кодов, по которым производится списание денег их владельцев, при продаже автомобилей через сеть «Интернет» может происходить автоматическое незаконное хищение различных платежей. Например, при продаже подержанных автомобилей через сеть «Интернет» в сети выкладывается объявление об этом, с привлекательной ценой товара. Заранее преступник записывает сообщение на автоответчик и программирует звонок таким образом, что с каждого абонента, прослушавшего это сообщение, автоматически списывается определенный платеж.

Распространение получает размещение объявлений-двойников, где мошенники вместо реального объявления о продаже делают его дубликат со своим номером телефона. При этом цена в объявлении-близнеце занижена с целью привлечения покупателей. Когда мошенники находят реального покупателя они начинают с ним общаться от имени продавца, а продавцу звонят от имени покупателя. На протяжении всей сделки оба ее участника даже не подозревают, что ведут диалог с преступником, который на определенном этапе просит внести авансовый платеж, который присваивает себе.

Другую угрозу представляют собой продажи автомобилей с помощью электронной цифровой подписи (ЭЦП), где в зоне риска может оказаться каждый автовладелец. Получение доступа к такой подписи и ее использование для хищения является новым способом совершения мошенничества.

В перспективе предполагается, что договоры купли-продажи транспортных средств будут заключаться онлайн – через портал «Госуслуги». Для подписания договора здесь не потребуется даже цифровой подписи, что создает дополнительные риски для автовладельцев. В случае завладения паролем к данному порталу мошенник, действуя от имени его собственника может продать автомобиль дропу, который перепродает его новому владельцу.

Обман может быть направлен не только на завладение транспортными средствами, но и на денежные средства, связанные с их эксплуатацией.

Его новым видом является отправка ложных СМС с требованием погасить задолженность за проезд транспортного средства по платной дороге[1]. Под видом уведомлений о задолженности за такой проезд водителям приходит СМС-сообщения от мошенников. Из общего числа тех, кому рассылаются сообщения, какое-то количество водителей действительно ехало по платной трассе. Расчет мошенников ориентирован на то, что они попытаются оплатить проезд, потому что на ряде платных трасс действует безбарьерная система, когда в течении пяти дней необходимо внести плату за него самостоятельно.

С использованием информационных технологий связано мошенничество, когда клиентов заманивают на фишинговые сайты, продвигающие покупку или продление ОСАГО. Происходит рассылка СМС, сообщений в мессенджерах или электронных писем. У жертв выманивают важную личную информацию, в частности данные банковской карты и пароли интернет-банкинга, после чего похищают деньги.

Рассылка разного рода электронных писем на почтовые ящики, текст которых вводит в заблуждение получателя, акцентируя его внимание на необходимости определенного рода платежей, передачи товара приобретает распространенность. В ходе их оплаты происходит неправомерное завладение регистрационными данными разных учетных записей для их последующей реализации.

Одним из самых распространенных приемов обмана покупателей автомобилей является размещение «фейкового» объявления исключительно для получения аванса. Таким видом мошенничества часто занимаются группы с собственными call-центрами. Они создают привлекательное объявление, где предлагается автомобиль, востребованный на первичном или вторичном рынке, преимущественно с заниженной ценой. Потенциальному покупателю предлагают перевести авансовый платеж, после чего псевдопоставщик или псевдовладелец исчезает.

[1] Юрист рассказал о схеме мошенничества с требованием оплаты проезда по трассе // Москва24 : сайт. URL: https://www.m24.ru/news/bezopasnost (дата обращения: 15.09.2023).

Преступная деятельность в сфере купли-продажи транспортных средств с развитием информационных технологий постоянно возрастает, все чаще граждане становятся жертвами мошенников. Онлайн-продажи в автосегменте оказываются тесно связаны со спросом на подержанные транспортные средства. Они постоянно обеспечиваются сегментом покупателей, желающих приобрести машину, по цене ниже представленной на первичном рынке.

Стремительный рост вторичного рынка автомобилей происходит в условиях трансформации дилерских сетей и дистрибьютеров, изменений в цепочках поставок, связан с остановкой ряда автомобильных производств, и увеличением стоимости транспортных средств. Его трендом является увеличение объема сделок вне личного контакта участников, в рамках интернет-торговли, онлайн-платежей, где возникают угрозы вмешательства в них путем мошенничества.

Удобство и комфорт современной дистанционной системы приводит к изменению системы безналичной оплаты услуг, связанных с транспортными средствами. Концентрирование на онлайн-расчетах наращивает традиционные и создает новые схемы мошенничества. Противодействие ему является важным направлением, обеспечивающим удовлетворение спроса российских потребителей на продукцию автомобильной отрасли, провозглашенному в рамках реализации Стратегии развития автомобильной промышленности Российской Федерации до 2035 года.

УДК 343

Д. А. БЕЗБОРОДОВ,
В. В. СОМКО

СОЦИАЛЬНО-ПРАВОВАЯ ОБУСЛОВЛЕННОСТЬ КРИМИНАЛИЗАЦИИ РАСПРОСТРАНЕНИЯ МАТЕРИАЛОВ, ПРОПАГАНДИРУЮЩИХ КУЛЬТ НАСИЛИЯ И ЖЕСТОКОСТИ, В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

В современном мире сложно переоценить влияние информационных сетей на общество. Каждый представитель цивилизованного государства в той или иной степени вовлечен в движущие силы социальных сетей, мессенджеров, видеохостингов независимо от возрастной категории.

Еще десятилетие назад общество столкнулось с интенсификацией информационных процессов: неуклонное возрастание скорости передачи сообщений; увеличение объема передаваемой информации и ускорение ее внедрения; ускорение обработки информации; использование обратных связей; наглядное отображение информации в процессах управления[1].

Сеть цифровых каналов связи продолжает активно расширять и охватывать новые территории, позволяя свободно искать, получать, передавать, производить и распространять цифровую информацию[2].

Цифровизация проникает в различные сферы человеческой деятельности, предоставляя новые условия и возможности для экономического, социального и правового развития. Однако, как любое технологическое изменение, она несет в себе новые риски и угрозы, формируя новую и удобную площадку для субъектов девиации.

Социальные сети, видеохостинги, сайты, мессенджеры – платформы, используемые СМИ и другими пользователями для быстрого распространения информации. Они могут быть использованы как в позитивных целях (распространение новостей, культурное и правовое просвещение), так в негативных (пропаганда, вербовка, устрашение населения).

Среди наиболее популярных и общественно опасных материалов, которые распространяются среди пользователей — материалы, пропагандирующие культ насилия и жестокости.

Общественная опасность данной информации характеризуется несколькими формами. К первой и наиболее общественного опасной форме относится криминализация общественного сознания. Это связано с криминогенной деформацией ценностно-нормативной системы общества, размыванием и девальвацией социально позитивных ценностей, установок, стереотипов поведения, нравственных идеалов людей[3].

---

[1] Абдеев Р. Ф. Философия информационной цивилизации. Диалектика прогрессивной линии развития как гуманная общечеловеческая философия для XXI в. М., 1994. С. 66.

[2] Пащенко И. Ю. Информация как объект публично-правового регулирования в условиях цифровизации : дис. ... канд. юрид. наук. Краснодар, 2022. 229 с.

[3] Клочкова А. В. Пропаганда насилия и жестокости в средствах массовой информации (криминологический аспект) // Культура: управление, экономика, право. 2006. № 4. С. 2—7.

Это сопровождается формированием антиобщественных взглядов, представлений, установок, оправдывающих даже поощряющих нарушение уголовно-правовых запретов.

Вторая формой угрозы является воздействие на сознание зрителей и читателей сценами, которые связаны с жестокостью, физическими расправами, садизмом, порождающими у людей ощущение беспомощности, безысходности от постоянной потенциальной угрозы криминальных посягательств, а также гипертрофированное чувство страха перед уличной и насильственной преступностью[1]. Представляется, что данной угрозе подвержены не все пользователи сети «Интернет», а наиболее восприимчивые или психически нестабильные лица.

Наиболее опасным представляется последствие, связанное с криминализацией общественного сознания.

При первичном изучении вопросов распространения материалов, пропагандирующих культ насилия и жестокости, возникает вопрос: почему при очевидной опасности данных материалов, она остается востребованной среди зрителей читателей и пользователей?

Ответ на данный вопрос неоднозначен. Социологи выделяют три категории лиц, среди которых сцены насилия пользуются наибольшим спросом. К первой категории относятся лица, склонные к переживанию интенсивных эмоций, испытывающие прилив сил после просмотра насильственных действий («адреналиновые наркоманы»). Ко второй категории относятся лица, стремящиеся получить опыт выживания от насильственных сцен в целях получения новых навыков («белые дубинки»). К последней группе относятся лица, которые соединяет в себе обе потребности вышеуказанных категорий – они получают яркие эмоции и стремятся приобрести навыки («темные копы»).

Распространение материалов носит разную форму и вид, к ним относятся: художественные фильмы, публикации СМИ, публикации пользователей.

---

[1] Клочкова А. В., Пристанская О. В. Информационные предпосылки криминализации общественного сознания // Вестник Московского университета. Серия: Право. 1999. № 2. С. 17—42.

Кинокартины обладают особым влиянием на общественность. «Бригада», «Бандитский Петербург», «Мир! Дружба! Жвачка!», «Закон каменных джунглей» — сериалы, где главные герои занимаются организованной преступностью, но их образы романтизированы для зрителя и заставляют сопереживать. Например, главным героем сериала «Мир! Дружба! Жвачка!» является Алик Афганец — криминальный авторитет, «крышующий рынок». Он выступает в роле потерянного человека — героя Афганской войны, который после раскола СССР был брошен на произвол судьбы, после чего становится лидером банды «Афганцев». Что привлекает в образе главного героя? Он настоящий, справедливый, храбрый, обладает всеми качествами, свойственными настоящему мужчине. Он предстает как настоящий друг, любящий парень и дядя. Кроме того, его хочется пожалеть за пережитый боевой опыт и развившийся посттравматический синдром, после которого Алик вынужден пристегивать себя к батарее на ночь. Основной акцент сделан на высокодуховности персонажа, трудно выделить недостатки. Зрители забывают, что в сериале демонстрируются преступления и криминальный мир. Такие художественные картины, как «Мир! Дружба! Жвачка!», вызывают повышенный общественный интерес, с точки зрения криминологии, играют крайне негативную социальную роль, романтизируя образы представителей криминального мира, представляют их в качестве образца для подражания.

Подобным образом два десятилетия назад отразился на обществе показ известного сериала «Бригада», где первостепенно демонстрировались не противоправные деяния, совершаемы бандой, а взаимодействие внутри группировки, содержащие преданность, благородство, взаимовыручку. После выхода сериала учеными-криминологами прогнозировались и подтверждались факты создания в регионах бригад, а также совершения ими отдельных преступлений, аналогичных изображенным в кинокартине[1].

Однозначно можно сказать, что запретить демонстрацию всех сцен насилия в художественных произведениях невозможно, разумеется, если они не

[1] Клочкова А. В. Указ. соч.

содержат в себе пропаганду культа жестокости или насилия. Однако прибегнуть к таким мерам, как демонстрировать фильмы со сценами исключительно в ночное время, добавить дисклеймер о содержании в фильме сцен с особой жестокостью и рекомендацией не просматривать контент детям, людям с неустойчивой психикой. Ранее были разработаны критерии присвоения кинокартинам возрастного ограничения, однако этот недостаточно для предупреждения просмотра подобных произведений несоответствующей аудитории.

Неоднозначный эффект оказывает на население просмотр публикаций в СМИ, содержащих повествование и сцены насилия и жестокости, оказывающие потенциальное криминогенное влияние на общественное сознание.

Во-первых, это эффект массового устрашения, повышение социального напряжения и нарастающего пессимизма в обществе. Связь между публикацией и подобным последствием очевидна – при просмотре возникает страх оказаться на месте жертвы описанного в новостном источнике преступления.

Во-вторых, рост уровнять терпимости к преступлениям в общественной жизни. Аудитория привыкает к объему информации о проявлениях жестокости и насилия в общественной среде, воспринимает преступность как неотъемлемый атрибут социальной жизни. Это является неадекватным отображением в массовом сознании общественной опасности различных противоправных деяний и повышением толерантности по отношению к преступникам. Каждый третий студент, участник опроса, готов иметь дружбу с лицом, имеющим судимость за насильственное преступление умышленного характера.

В силу отмеченных обстоятельств существует, как представляется, необходимость ограничить демонстрацию насильственных сцен в публикациях СМИ в сети «Интернет». Так, прикрепление к публикации, содержащей в себе текстовое описание случаев незаконного применения физического насилия, фотографий или видеозаписей произошедшего, в том числе без надлежащей цензуры, (причинение вреда здоровью, убийство и т. д.) является способом привлечения масс к конкретному источнику. Представляется, ограничение в сопровождении текстовых сообщений видео- и фотоматериалами сможет

снизить уровень информационного насилия на пользователей сети «Интернет», телезрителей и читателей печатных изданий.

Информационное насилие в широком смысле, предполагающем существование информации в любых социальных системах — это не силовое упорядоченное воздействие на объекты, носящее антисоциальный либо антиличностный характер. Информационное насилие в узком смысле — это несиловое воздействие на ментальную сферу, противоречащее закономерному ходу событий[1].

Отметим, что понятия «насилия» и «жестокости» есть ни одно и то же. Обратимся к энциклопедическому словарю Ф. А. Брокгауза, И. А. Ефрона для дачи определения понятию «насилие»: незаконное употребление силы против личности потерпевшего, принуждение его что — либо сделать или не делать, что — либо испытать или перенести.

В свою очередь, жестокость — это оценочная категория, которая не получила так же, как и насилие, законодательного закрепления понятия. Ю.М. Антонян и В.В. Гульдан под жестокостью как чертой личности понимают стремление к причинению страданий, мучений людям или животным, выражающееся в действиях, бездействии, словах, а также фантазировании соответствующего содержания.

Насилие не всегда сопровождается жестокостью, его мотивы могут быть не просто правомерны, но и гуманны, общественно полезны (крайняя необходимость, самооборона). В то время, как жестокость всегда сопровождается насилием как физическим, так и психологическим.

Так, например, О. Ю. Михайлова полагает, что жестокость является вполне конкретным свойством личности насильственного преступника, которое проявляется в антиобщественном поведении, направленном на причинение страданий. В основе жестокости лежат дефекты ценностно-нормативной сферы человека, а именно нарушение ценности другого человека.

[1] Борщов Н. А. Информационное насилие в сетевом обществе // Вестник ЧелГУ. 2010. № 31. URL: https://cyberleninka.ru/article/n/informatsionnoe-nasilie-v-setevom-obschestve (дата обращения: 14.11.2023).

Сеть «Интернет» выступает удобной площадкой для демонстрации, а также пропаганды культа насилия и жестокости — без дополнительных усилий привлечь массы к тому или иному насильственному деянию проще.

Необходимо различать еще два понятия: демонстрация и пропаганда. Пропаганда — это распространение и углубленное разъяснение каких-либо идей, учения, знаний среди широких масс населения или круга специалистов; политическое или идеологическое воздействие на широкие массы[1].

Демонстрация же представляет собой несколько иное действие, предполагая наглядное изображение того или иного события или явления. Не любая демонстрация несет в себе цель на идеологическое воздействие. Однако грань между демонстрацией и пропагандой достаточно тонкая и на практика не редки случаи разночтения в зависимости от сложившейся практики применения.

В большинстве сообщениях СМИ, художественных фильмах демонстрируются, но не пропагандируется культ насилия и жестокости. Отметим, что это также имеет влияние на социум, однако в большей степени опасность для общества представляют лица, которые публикуют в сети «Интернет» материалы, призывающие к совершению насильственных действий. Призыв может быть в форме разъяснения способов убийства или причинения вреда здоровью, причем направленных, в том числе на причинение боли без явных физических увечий. Также призыв может быть выражен демонстрацией удовольствия и удовлетворения от совершаемых действий.

Относительно новым явлением является «треш-стриминг» — прямая трансляция на видеостриминговом сервисе с целью демонстрации широкой аудитории сцен насилия и жестокости. В ряде случаев пользователи преследуют не только с гедонистистическими цели, но и корыстные. Аудитория «треш-стримера» оказывает финансовую поддержку, нередко с конкретной просьбой на причинения жертве преступления большего физического вреда или вреда, определенного характера. Пользователи с деформацией психики

[1] Патрахина Т. Н. Пропаганда: сущность научной дефиниции, подходы к классификации // Молодой ученый. 2015. № 4 (84). С. 305—308.

получают удовольствие от просмотра сцен жестокости в прямом эфире. Личности, склонные к совершению преступлений с особой жестокостью, испытывают удовольствие и физическое удовлетворения от визуализации желаемых действий, благодаря «треш-стримеру» они могут за денежные средства («донат») это реализовать.

Например, блогер Станислав Решетников регулярно транслировал на своем канале «YouTube» сцены, на которых различные лица подвергались физическому насилию, издевательствам, унижению человеческого достоинства. В декабре 2020 года на очередном «стриме» указанный блогер избивал свою знакомую, заливал лицо перцовым баллончиком, а затем выставил в нижнем белье на мороз, после чего девушка скончалась.

Проведенная судмедэкспертиза констатировала у погибшей закрытую черепно-мозговую травму, множественные кровоподтеки на различных частях тела, субдуральную гематому, образовавшуюся вследствие многократных ударов по лицу.

Следственными органами было предъявлено обвинение Решетникову в совершении преступления, предусмотренного ч. 4 ст. 111 УК РФ.

В настоящее время в России отсутствует наказание за пропаганду насильственных действий в сети «Интернет», в том числе в сообщениях СМИ и художественных фильмах.

В статье 4 в Законе Российской Федерации от 27.12.1991 № 2124-1 (ред. от 13.06.2023) «О средствах массовой информации» содержится запрет на использование средств массовой информации в целях распространения материалов, содержащих насилие и жестокость. Однако ни в КоАП РФ, ни в УК РФ не существует юридической ответственности за подобное деяние, что представляется несоответствующим уровню общественной опасности рассматриваемых действий.

Отметим, что изготовление или распространение произведений, пропагандирующих культ насилия и жестокости, было криминализировано в Уголовном кодексе РСФСР и наказывалось лишением свободы на срок до 2 лет,

либо исправительными работами на тот же срок, либо штрафом до трех минимальных размеров оплаты труда, с конфискацией произведений и средств изготовления и демонстрации.

Также, например, в настоящее время в республике Казахстан криминализировано незаконное изготовление в целях распространения или рекламирования, распространение, рекламирование, демонстрация кино- и видеоматериалов, и других произведений, пропагандирующих культ жестокости и насилия, а равно незаконная торговля печатными изданиями, кино- или видеоматериалами, пропагандирующими культ жестокости и насилия.

Дополнение подобной статьей законодательства Российской Федерации целесообразно в связи с выраженной степенью общественной опасности пропаганды культа жестокости и насилия, а также в связи уже содержащимся в одном из федеральных законов запретов на распространение указанных материалов, в том числе в сети «Интернет».

Есть несколько возможных форм криминализации распространения материалов:

— дополнение КоАП РФ составом административного проступка, содержащего наказание за распространение материалов, пропагандирующих культ жестокости и насилия;

— дополнение УК РФ составом преступления, содержащего наказание за распространение материалов, пропагандирующих культ жестокости и насилия.

Представляется, что второй вариант является более подходящим для деяния подобного характера общественной опасности.

Предусмотреть новый состав логично в главе 25 («Преступления против здоровья населения и общественной нравственности») и дополнить ее ст. 239.1 УК РФ «Распространение материалов, содержащих пропаганду культа жестокости и насилия», определив объектом преступления общественную нравственность.

Общественная опасность распространения материалов, пропагандирующих культ жестокости и насилия, заключается, как уже указывалось ранее,

в негативном воздействии на нормальное развитие и функционирование психики человека, в том числе на несовершеннолетних лиц. Пропаганда подобных материалов в ряде случаев провоцирует совершение умышленных насильственных преступлений.

Предметом преступления могли бы являться произведения, сообщения СМИ и пользователей сети «Интернет», пропагандирующие культ жестокости и насилия, характеризующиеся циничностью, пренебрежительным отношением к нравственности и моральным нормам. Это могут быть художественные фильмы, сообщения СМИ на сайтах, в социальных сетях, в telegram-каналах, видеозаписи и трансляции на видеохостингах и стриминговых платформах, фотографии, рисунки (в том числе изготовленные с помощью электронных технологий), скульптуры, аудиозаписи и прочее.

Как уже указывалось ранее, не любая демонстрация материалов содержит в себе пропаганду. Предполагая дискуссионность отнесения того или иного произведения к предмету рассматриваемого преступления, необходимо отметить возможность использования правоприменителями полномочий по проведению экспертиз (лингвистических, психолингвистических, искусствоведческих). Соответственно, после дополнения Уголовного закона новой нормой, целесообразно разработать экспертными центрами критерия отнесения сообщений или произведений к материалам, пропагандирующим культ жестокости и насилия.

Объективная сторона ст. 239.1 УК РФ могла бы быть выражена действием – изготовлением или распространением с целью ознакомления с материалами другими лицами. Изготовление – это создание материалов любыми способами: съемка, фотографирование, изготовление изображений, написание статей и сценариев и другие. Отметим, что тиражирование также стоит относить к изготовлению, так как цель распространения уже готового результата – ознакомление с пропагандисткой информацией широкого круга лиц.

Формы распространения могут быть различными: передача, дарение, продажа. Кроме того, необходимо учитывать, что распространение может носить

публичный характер: демонстрация публике видеозаписей и изображений пропагандистских материалов; размещение в сети «Интернет».

Отметим, что распространение указанных материалов в сети «Интернет» является одним из способов совершения преступления. Целесообразно было бы данный способ сделать в рамках нормы 239.1 УК РФ квалифицированным составом.

Логично в данной норме выделить общий (лицо, достигшее 16-летнего возраста) и специальный субъекты (журналисты и иные лица, использующие служебное положение).

Выделение специального субъекта обусловлено потенциальным увеличением круга лиц, которые могут ознакомиться с материалами. Например, журналист распространяет материалы, используя интернет-сайт, канал или аккаунт в социальной сети, ТВ-программу на телевидении, печатное издание и другие ресурсы с большой аудиторией, а соответственно, повышает уровень общественной опасности деяния.

Кроме того, выделение специального субъекта обусловлено возможностью использования должностного положения при изготовлении материалов. Например, съемка военнослужащими пыток и жестокого обращения над мирным населением или над пленными; съемка военными корреспондентами сцен жестокости и насилия в «горячих точках» и т. д.

Совершение преступления планируемой к введению в УК РФ ст. 239.1 специальным субъектом необходимо выделить как квалифицированный состав преступления.

Субъективная сторона могла бы характеризоваться прямым умыслом. Обязательным признаком субъективной стороны могла бы стать цель — распространение материалов, пропагандирующих культ жестокости и насилия, с целью ознакомлениями с ними неопределенного круга лиц. Факультативным признаком субъективной стороны выступает также корыстный мотив.

На основании вышеизложенного, можно сделать выводы о необходимости и социальной обоснованности криминализации изготовления и распространения материалов, пропагандирующих культ жестокости и насилия и дополнения УК РФ ст. 239.1: «Распространение материалов, содержащих пропаганду культа жестокости и насилия», в следующей редакции:

1. Незаконное изготовление и распространение кино- и видеоматериалов, фотографий, изображений и других материалов, пропагандирующих культ жестокости и насилия, с целью ознакомления с ними неопределенного круга лиц,

наказывается <…>

2. Те же деяния, совершенные:

а) лицом с использованием своего служебного положения;

б) с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», наказываются <…>

УДК 343

О. Ф. БОГОВАЯ,
Е. Л. КОСЯК

ПРОБЛЕМНЫЕ ВОПРОСЫ РАЗГРАНИЧЕНИЯ ПУБЛИЧНЫХ ПРИЗЫВОВ К ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

В современных условиях глобального роста количества экстремистских проявлений особую общественную опасность представляет собой политический экстремизм, являющийся одним из негативных последствий аномального развития мировой цивилизации.

Политический экстремизм опасен тем, что отдельные социальные группы как субъекты политической деятельности в борьбе за достижение публичной власти используют не общепризнанные мировой практикой методы завоевания доверия электората на выборах, а для достижения цели прихода к власти прибегают к общественным беспорядкам, парализации экономики путем массовых забастовок, организации акций неповиновения и массовых беспорядков, террористическим актам.

События, происходящие на территории Украины с 2014 года, показывают, что финансируемые иностранными государствами и аффилированными с ними международными неправительственными организациями прозападные украинские политические группировки в своем желании удержаться у власти используют прикрываемую национал-патриотической идеологией такую крайнюю форму политического экстремизма, как задействование силовых структур и интегрированных в них откровенно криминальных организаций (так называемые «добровольческие» военизированные формирования) для подавления протестных выступлений населения.

Данная форма политического экстремизма была легализована под видом проводимой с апреля 2014 года так называемой «антитеррористической операции» (с апреля 2018 года – «операции объединенных сил»).

Наиболее опасным проявлением экстремизма, в том числе политического, является такая его разновидность, как терроризм. Несмотря на то, что террористическая деятельность является одной из форм экстремистской деятельности, они имеют определенные различия.

Термин «экстремизм» (от лат. extremus – крайний) определяется Ю.М. Антоняном как «приверженность к крайним взглядам и радикальным мерам, а также реализация этих мер»[1]. Соглашаясь с данным определением, целесообразно дополнить его таким способом реализации таких мер как применение насилия.

Экстремистская деятельность законодательно определена в ст. 1 Федерального закона от 25 июля 2002 г. № 114-ФЗ (в ред. от 28.12.2022) «О противодействии экстремистской деятельности». Необходимо обратить внимание, что законодатель относит террористическую деятельность к разновидности экстремистской деятельности.

Понятие «терроризм» происходит, как справедливо указывает Ю.С. Горбунов, от латинского terreo, что означает «наводить страх», «пугать». То есть,

[1] Экстремизм и его причины / В. В. Аванесян, Л. А. Айвар, Ю. М. Антонян [и др.] ; под ред. Ю. М. Антоняна. М., 2010. С. 10.

терроризм представляет собой устрашение политического противника насильственными методами вплоть до физического уничтожения для достижения конкретных целей[1].

В соответствии со ст. 3 Федерального закона от 6 марта 2006 года № 35-ФЗ (в ред. от 10.07.2023) «О противодействии терроризму», терроризм понимается как идеология насилия и практика воздействия на принятие решения органами публичной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Таким образом, по нашему мнению, основной критерий разграничения экстремистской и террористической деятельности состоит в использовании в террористической деятельности идеологии насилия и устрашения.

В то же время, экстремистская деятельность также предполагает публичные призывы к связанному с применением насилия нарушению прав, свобод и законных интересов человека и гражданина. Представляется, что сами по себе призывы к насилию, если они не направлены на устрашение кого-либо для достижения политических целей, охватываются понятием призывов к экстремистской деятельности.

Думается, что если такие призывы осуществляются для устрашения и являются средством для достижения конкретных политических целей, то они должны быть оценены как призывами к террористической деятельности.

Приведенные теоретические положения позволяют разграничить призывы к экстремистской и призывы к террористической деятельности.

Так, в соответствии с п. 5 Постановления Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 (ред. от 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» публичное распространение информации, в которой обосновывается необходимость совершения противоправных действий в отношении лиц по признаку расы, национальности, религиозной принадлежности и т.д., либо информации,

[1] Горбунов Ю. С. Что такое терроризм // Вестник Санкт-Петербургского университета МВД России. 2006. № 4 (32). С 17—25.

оправдывающей такую деятельность, следует квалифицировать по ст. 282 УК РФ при наличии иных признаков этого состава преступления.

Публичные призывы к осуществлению террористической деятельности в силу предписаний ч. 3 ст. 17 УК РФ подлежат квалификации не по ст. 280 УК РФ, а в зависимости от обстоятельств дела по ч. 1 или ч. 2 ст. 205.2 УК РФ.

При этом исходя из содержания призывов преступления могут быть квалифицированы и по совокупности преступлений, предусмотренных ст. 205.2 и ст. 280 УК РФ.

Так, например, Главным следственным управлением СК России 3 марта 2014 г. возбуждено уголовное дело в отношении руководителя террористической организации «Правый сектор» Яроша Д.А. по признакам преступлений, предусмотренных ч. 2 ст. 205.2 и ч. 2 ст. 280 УК РФ в связи с совершением им публичных призывов к активизации вооруженной борьбы против Российской Федерации с целью побуждения третьих лиц к осуществлению экстремистской и террористической деятельности путем распространения их 1 марта 2014 г. в сети «Интернет» на странице организации «Правый сектор» в социальной сети «ВКонтакте» в виде «Обращения лидера «Правого сектора» Дмитрия Яроша к Доку Умарову».

Этим же следственным органом 21 марта 2014 г. возбуждено уголовное дело по признакам преступлений, предусмотренных ч. 2 ст. 205.2 и ч. 2 ст. 354 УК РФ, в отношении лидера украинской радикальной организации «Братство» Корчинского Д.А. (бывшего участника УНА-УНСО) в связи с высказанными им в интервью телеканалу «Россия 1» призывами к осуществлению террористической деятельности, а также к развязыванию агрессивной войны путем ведения диверсионно-партизанских действий на территории Российской Федерации, в том числе в Крыму[1].

[1] Решение Верховного Суда Российской Федерации от 17 ноября 2014 г. по делу № АКПИ14-1292С. О признании украинских организаций экстремистскими и запрете их деятельности на территории Российской Федерации. Доступ из справ.-правовой системы «КонсультантПлюс».

Кроме этого, исследуемые преступления могут быть совершены и в разное время в условиях реальной совокупности.

Например, Шепелев признан виновным и осужден за то, что он, испытывая неприязнь к органам государственной власти и правоохранительным органам, используя устройство, имеющее выход сеть «Интернет», с целью доведения до неопределенного круга лиц информации, призывающей к террористической и экстремистской деятельности, путем размещения в свободном доступе в социальной сети указанных в приговоре материалов, совершил:

— 14, 17 октября 2017 г., 21 марта, 2 октября 2018 г., а также 3 августа 2019 г. публичные призывы к осуществлению террористической деятельности;

— 9, 14 октября 2017 г., а также в период с 24 декабря 2019 г. по 7 января 2020 г. публичные призывы к осуществлению экстремистской деятельности[1].

Подводя итог изложенному в настоящей статье, следует отметить недостаточно четкое определение критериев призывов к террористической деятельности, данное в п. 18 Постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 года № 1 (в ред. от 3.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

Так, в данном пункте указано, что «под публичными призывами к осуществлению террористической деятельности в статье 205.2 УК РФ следует понимать…обращения к другим лицам с целью побудить их к осуществлению террористической деятельности, то есть к совершению преступлений, предусмотренных ст. ст. 205-206, 208, 211, 220, 221, 277, 278, 279, 360, 361 УК РФ».

По нашему мнению, данный пункт Постановления Пленума Верховного Суда Российской Федерации целесообразно дополнить приведенными выше критериями относимости конкретных призывов к призывам к осуществлению террористической деятельности, изложив его в следующей редакции: «под

[1] Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 22 марта 2023 г. № 223-УД23-4-А6. Доступ из справ.-правовой системы «КонсультантПлюс».

публичными призывами к осуществлению террористической деятельности в статье 205.2 УК РФ следует понимать… обращения к другим лицам с целью побудить их к осуществлению террористической деятельности, то есть к совершению преступлений, предусмотренных статьями 205-206, 208, 211, 220, 221, 277, 278, 279, 360, 361 УК РФ. Такие обращения должны осуществляться для устрашения адресатов и являться по мнению лица, их высказывающего, средством достижения конкретных политических целей».

УДК 343

И. Д. БОРИСОВ

К ВОПРОСУ О СООТНОШЕНИИ СОСТАВОВ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЯМИ 165 И 272 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Современная информатизация всех сфер жизнедеятельности в огромной степени влияет на все сферы жизни общества. Развитие информационно-телекоммуникационных технологий существенно упростило и структурировало взаимодействие субъектов рыночных отношений. Надлежащее функционирование сферы собственности в настоящее время невозможно представить в обособленном от информационно-телекоммуникационных технологий виде.

Так, охраняемое уголовным законом имущество граждан давно вышло за пределы материального мира, а устоявшееся до недавнего времени доктринальное понимание предмета хищения, как имеющего внешне физическое выражение, потеряло всякую актуальность, о чем, в свою очередь, свидетельствуют судебные решения, расширяющие толкование понятия «имущества», на которое, помимо прочего, может быть совершено преступное посягательство.

Тенденции экономического развития, обусловливающие динамику сферы собственности, обязывают законодателя к беспрерывной актуализации уголовно-правовой защиты рассматриваемых общественных отношений.

В самом общем виде информационно-телекоммуникационные технологии можно определить, как совокупность информационных процессов посредством компьютерных систем и сетей связи. Информация в данном случае выступает ключевым звеном, затрагивающим различные сферы жизнедеятельности человека. Однако, масштаб данной системы свидетельствует о колоссальной уязвимости одновременно нескольких групп общественных отношений в случае неправомерного воздействия.

Большинство преступлений, указанных в главе 21 УК РФ, относятся к категории хищений, то есть имеют ряд обязательных признаков. При этом, по данным Министерства внутренних дел Российской Федерации, практически каждое четвертое зарегистрированное 2022 году преступление является хищением с использованием информационно-телекоммуникационных технологий[1].

Однако рассматриваемая глава УК РФ предусматривает и иные преступления против собственности, не связанные с хищением, к которым относится причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ).

Проблематика рассматриваемой уголовно-правовой нормы, несмотря на ее частичную декриминализацию 2011 года, является весьма актуальной в свете отсутствия единообразия в правоприменительной и судебной практике, что, в свою очередь, подрывает принципы законности и справедливости, а также свидетельствует о значимости рассмотрения отдельных механизмов совершения указанного преступления[2].

Практическая значимость ст. 165 УК РФ состоит в том, что указанная норма на данный момент является одним из единственных механизмов защиты прав собственника имущества в случае причинения последнему уста-

[1] Краткая характеристика состояния преступности в Российской Федерации за январь—декабрь 2022 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 09.11.2023).

[2] Харина Е. А. К вопросу о проблемных аспектах квалификации и криминализации мошенничества в сфере компьютерной информации // Российский следователь. 2023. № 3. С. 29—33.

новленного законодателем ущерба при отсутствии признаков хищения. Безусловно, специальные составы преступления, предусмотренные статьями 194, 198, 199, 199.3, 199.4 УК РФ, выполняют схожие со ст. 165 УК РФ охранительные функции, однако последняя носит универсальный характер, что, в свою очередь, также порождает ряд правоприменительных проблем.

Как уже отмечалось выше, компьютеризация общества способствует упорядочиванию общественных отношений в сфере собственности, но, вместе с тем, она также является детерминантой делинквентного поведения отдельных лиц.

В этой связи уголовно-правовой охране компьютерной информации законодателем предусмотрено отдельное место в системе уголовного закона. Так, глава 28 УК РФ включает в себя несколько составов преступлений, которые выступают гарантом прав граждан в информационно-телекоммуникационной среде[1].

Для целей данной работы наибольший интерес представляет выявление критериев соотношения «компьютерного преступления», предусмотренного ст. 272 УК РФ, и упомянутого выше причинения имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ).

В рамках соотношения с диспозициями частей 2 и 3 ст. 272 УК РФ прослеживается некая схожесть данных деяний, что, на первый взгляд, может указывать на ее специальный по отношению к ст. 165 УК РФ характер.

В данном случае идет речь о таких квалифицирующих признаках статьи 272 УК РФ, как крупный ущерб (ч. 2), а также признак совершения преступления организованной группой (ч. 3, совершенная с причинением крупного ущерба).

Так, при совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ, крупный ущерб причиняется посредством неправомерного доступа к компью-

[1] Овсюков Д. А. Корыстные преступления против собственности с использованием информационно-телекоммуникационных сетей: вопросы квалификации : монография / под науч. ред. С. М. Кочои. М., 2023. С. 18.

терной информации, повлекшего ее уничтожение, блокирование, модификацию либо копирование. Вместе с этим, если указанный способ будет признан разновидностью обмана, используемого для целей совершения преступления, предусмотренного ст. 165 УК РФ, то в данном случае может прослеживаться конкуренция уголовно-правовых норм, причем сложность будет состоять в том, что рассматриваемые статьи уголовного закона по отношению друг к другу не являются ни привилегированными, ни квалифицированными.

Однако для начала представляется необходимым установить критерии, относящие способ совершения деяния, предусмотренного ст. 272 УК РФ, к категории обмана.

Так, согласно Постановлению Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», под обманом, помимо прочего, понимается сознательное предоставление заведомо ложных, не соответствующих действительности сведений, а также в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение. Кроме того, обман может заключаться в несанкционированном подключении к энергосетям, создающем возможность неучтенного потребления электроэнергии. В широком же смысле ученые расценивают обман, в первую очередь, как разновидность психического воздействия на сознание человека[1].

Исходя из вышесказанного к непосредственным критериям обмана, как способа совершения преступления, можно отнести совершение умышленных, в том числе ложных действий, направленных на введение лица в заблуждение путем психологического воздействия на его сознание.

В этой связи представляется, что совершение деяния, предусмотренного ч. 1 ст. 272 УК РФ, причинившего крупный ущерб, при определенных обстоятельствах может единовременно являться обманом, то есть способом, предусмотренным ст. 165 УК РФ.

[1] Знаков В. В. Психология понимания правды. СПб., 1999. С. 36.

Безусловно, минимальный порог указанного квалифицирующего признака в соответствии с примечанием к ст. 272 УК РФ составляет один миллион рублей, что в четыре раза больше, чем аналогичная граница ответственности по ст. 165 УК РФ. Однако если лицо путем обмана, выраженного, к примеру, модификацией компьютерной информации путем искажения достоверных данных, ложно свидетельствующих о его освобождении от платы за коммунальные услуги, причиняет ущерб собственнику имущества на общую сумму свыше одного миллиона рублей, то его действия попадают как под признаки ч. 2 ст. 165 УК РФ, так и под признаки ч. 2 ст. 272 УК РФ.

Здесь сразу стоит отметить упомянутый выше психологический критерий, ведь воздействие при обмане возможно исключительно на физическое лицо, к примеру, на сотрудника организации, который оказался введен в заблуждение посредствам модификации виновным лицом соответствующей информации как в вышеуказанном случае.

Так, если действия виновного влияют исключительно на компьютерные системы и сети связи, при этом собственник либо иной владелец имущества, а также уполномоченные ими лица фактически в заблуждение не вводятся, то обман, как рассматриваемый нами способ совершения преступления, иметь место не будет, а квалификация деяния, при отсутствии в действиях виновного признаков иных составов преступлений, будет исключительно по соответствующей части ст. 272 УК РФ.

Обращаясь к юридической природе специальных составов преступления, можно отметить, что такие составы преступления обладают всеми признаками другого (общего) состава преступления при наличии хотя бы одного дополнительного (специального) признака, который по, общему правилу, не является ни квалифицирующим, ни привилегированным[1].

При этом кажется последовательным, что процесс криминализации специального состава преступления, должен вытекать из каких-либо объектив-

[1] Иванчин А. В., Зосиева М. В. Проблемы конструирования специальных составов преступлений // Юридическая наука. 2017. № 4. С. 133—137.

ных обстоятельств. Они могут заключаешься в специфике предмета посягательства, субъектного состава, а также содержания социальных ценностей, выступающих в качестве охраняемых общественных отношений.

Однако главной функцией института специальных составов преступления является дифференциация уголовной ответственности, которая основывается на упомянутых выше обстоятельствах.

Исходя из логики законодателя, ст. 272 УК РФ по общему правилу не является специальной нормой по отношению к ч. 2 ст. 165 УК РФ. Вместе с тем при определенных обстоятельствах, в том числе отмеченных выше, частях 2 и 3 ст. 272 УК РФ обладают всеми признаками специального состава преступления.

Представляется, что «специальный» характер рассматриваемой нормы осознано законодателем введен не был. Однако дополнительный (специальный) по отношению к ч. 2 ст. 165 УК РФ признак в виде обмана посредством неправомерного доступа к компьютерной информации безусловно имеется, что требует дифференциации уголовной ответственности. В противном случае инкриминирование совокупности преступлений, предусмотренных ст.ст. 165 и 272 УК РФ, при совершении одного деяния посредством «слияния» способов рассматриваемых статей, повлекшего причинение единого ущерба свыше одного миллиона рублей, будет противоречить принципу справедливости, установленного ч. 2 ст. 6 УК РФ.

При этом в доктрине уголовного права зачастую рассматривались вопросы совокупности преступлений, предусмотренных ст.ст. 165 и 272 УК РФ. Так, по мнению В.Г. Степанова-Егиянца, использование виновным для доступа в сети «Интернет» чужих логина и пароля с последующим совершением действий, повлекших причинение имущественного ущерба путем обмана или злоупотребления доверием, необходимо квалифицировать по совокупности преступлений, предусмотренных ст.ст. 272 и 165 УК РФ[1].

[1] Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М., 2016. С. 40.

Безусловно, совокупность указанных преступлений будет иметь место в большинстве случаев, когда совершенное «компьютерное» преступление предшествует и (или) содействует причинению имущественного ущерба путем обмана или злоупотребления доверием. Однако возможные вопросы «слияния» рассматриваемых деяний по признаку способа не нашли должного отражения в научных работах.

Так, в зависимости от конкретных обстоятельств, ст. 272 УК РФ (части 2 и 3) будет переходить в разряд специальных по отношению к ч. 2 ст. 165 УК РФ при совокупности в совершенном деянии ряда условий:

Во-первых, причиненным ущербом будет являться сумма свыше одного миллиона рублей;

Во-вторых, деяние, предусмотренное ч. 1 ст. 272 УК РФ, будет обладать юридической природой обмана, то есть вводить лицо в заблуждение посредством психологического воздействия на его сознание;

В-третьих, необходимо наличие прямой причинной связи между приведенными выше пунктами. Иными словами, деяние, совершенное способом, указанным в диспозиции ч. 1 ст. 272 УК РФ и который обладает признаками обмана должно предшествовать наступлению общественно опасных последствий в виде причинения крупного ущерба (превышающего один миллион рублей), содержать в себе реальную возможность их наступления и являться главной, решающей и непосредственной причиной таких последствий.

Применительно к ч. 3 ст. 272 УК РФ, помимо выделенных условий необходимо наличие признака организованной группы.

Так, при совпадении указанных обстоятельств действия лица необходимо будет квалифицировать, в зависимости от конкретных обстоятельств, лишь по ч. 2 либо 3 ст. 272 УК РФ без совокупности со ст. 165 УК РФ во избежание двойного вменения за одно совершенное деяние.

При несовпадении хотя бы одного из условий специальный характер статьи 272 УК РФ утрачивает свою силу, и, в зависимости от обстоятельств произошедшего, действия виновного подлежат квалификации по совокупности ст.ст. 165 и 272 УК РФ.

Здесь же стоит отметить такой альтернативный способ совершения преступления, предусмотренного ст. 165 УК РФ, как злоупотребление доверием. Данный способ априори не может породить указанную выше конкуренцию норм, предусмотренных ст.ст. 165 и 272 УК РФ. Ведь необходимым признаком злоупотребления доверием является наличие особых отношений доверия между субъектом преступления и потерпевшим[1].

Злоупотребление доверием в качестве самостоятельного способа совершения преступления против собственности в чистом виде и так встречается крайне редко, а его обособленное проецирование на диспозицию ч. 1 ст. 272 УК РФ по аналогии с обманом представляется вовсе невозможным.

Так, правовая природа неправомерного доступа к компьютерной информации, повлекшего ее уничтожение, блокирование, модификацию либо копирование, не предусматривает возможность «слияния» злоупотребления доверием со специальным, предусмотренным ст. 272 УК РФ способом.

Доверительные отношения в данном случае могут лишь облегчить возможность такого доступа, однако говорить о прямой причинной связи наличия таких отношений и злоупотребления ими с наступившими общественно опасными последствиями в виде имущественного ущерба говорить вряд ли приходится.

Резюмируя вышесказанное нельзя игнорировать тот факт, что, признавая специальный характер ч. 2 ст. 272 УК РФ по отношению к ч. 2 ст. 165 УК РФ, при очевидной повышенной общественной опасности «компьютерного» преступления в силу нарушения сразу нескольких объектов уголовно-правовой охраны, максимальная санкция такого преступления будет меньше конкурирующего с ним преступления против собственности, что необоснованно делает его в определенном роде привилегированным по отношению к ст. 165 УК РФ.

[1] Ботвин И. В. Обман и злоупотребление доверием как способы причинения имущественного ущерба // Юридический вестник Дагестанского государственного университета. 2014. № 4. С. 105—107.

А в случае причинения имущественного ущерба менее одного миллиона рублей, но более двухсот пятидесяти тысяч рублей лицо и вовсе будет подлежать ответственности по совокупности преступлений, предусмотренных статьями 165 и 272 УК РФ в силу полного отсутствия конкуренции норм по признаку ущерба.

Единственным решением несоразмерности санкций с общественной опасностью рассматриваемых деяний, а также решения вопросов их конкуренции, является введение в ст. 165 УК РФ квалифицирующего признака, охватывающего неправомерный доступ к компьютерной информации, который не будет противоречить основному способу совершения указанного состава преступления.

УДК 343

Г. А. ГОЛУБЕВ

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ СБЫТОМ НАРКОТИКОВ И СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Преступления, совершаемые в сфере незаконного оборота наркотических средств (психотропных веществ или их аналогов) продолжают занимать одну из лидирующих позиций в структуре преступности Российской Федерации. Научно-технический прогресс обуславливает появление новых способов совершения таких преступлений, в том числе с использованием сети «Интернет».

Согласно сведениям Судебного департамента при Верховном Суде Российской Федерации в первом полугодии 2023 года осуждено 268 921 лицо, 9 495 лиц (3,5 %) из которых за совершение незаконного сбыта наркотических средств, из них – 4 327 лиц (45,6 %) при наличии в их действиях квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ, то есть с использованием сети «Интернет»[1].

[1] Сводные статистические данные о состоянии судимости в России за 1 полугодие 2023 года // Судебный департамент при Верховном Суде Российской Федерации : офиц. сайт. URL: https://www.cdep.ru/index.php?id=79&item=7900 (дата обращения: 10.11.2023).

Однако, несмотря на длительное существование указанного квалифицирующего признака в ст. 228.1 УК РФ, правоприменительная практика оставляет некоторые проблемы квалификации незаконного сбыта наркотических средств с использованием сети «Интернет».

Например, до конца нерешенным остается вопрос окончания сбыта наркотических средств с использованием сети «Интернет».

Так, согласно п. 13.2 Постановления Пленума Верховного Суда Российской Федерации от 15.06.2006 № 14 (в ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами», согласно которым, незаконный сбыт наркотических средств следует считать оконченным с момента выполнения лицом всех необходимых действий по передаче приобретателю указанных средств независимо от их фактического получения приобретателем. В противном случае действия лиц должны быть квалицированы как неоконченное преступление[1].

Для судов определяющим обстоятельством является установление того, что лицо выполнило все зависящие от него действия, направленные на передачу наркотического средства приобретателю через сеть «Интернет».

Так, судебной коллегией Третьего кассационного суда общей юрисдикции 26.01.2023 действия А. переквалифицированы с п. «г» ч. 4 ст. 228.1 УК РФ на ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ, и из его действий исключен квалифицирующий признак «с использованием сети «Интернет»[2].

Удовлетворяя кассационное представление прокурора, судебная коллегия указала, что суд первой инстанции, квалифицируя действия А., как два оконченных преступления, предусмотренных п. «г» ч. 4 ст. 228.1 УК РФ, не учел разъяснения, содержащиеся в п. 13.2 Постановления Пленума Верховного

[1] Квалификация преступлений против здоровья населения и общественной нравственности : учебное пособие / Д. А. Безбородов, А. В. Зарубин, Р. М. Кравченко [и др.] ; под общ. ред. А. Н. Попова. СПб., 2021. С. 17.

[2] Кассационное определение Третьего кассационного суда общей юрисдикции от 26 января 2023 г. № 77-193/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

Суда Российской Федерации от 15.06.2006 № 14 (в ред. от 16.05.2017) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами», поскольку при описании преступных деяний, совершенных последним, отсутствуют данные о том, что места сделанных «закладок» заранее оговорены с их приобретателями, либо информация об этих тайниках доведена до их сведения с использованием сети «Интернет».

По аналогичным причинам 20.04.2023 судом кассационной инстанции действия Л., разместившего наркотические средства в тайниках и передавшего сведения о них через сеть «Интернет» участнику организованной группы, который разместил сведения о «закладках» на витрине интернет-магазина, переквалифицированы с п. «г» ч. 4 ст. 228.1 УК РФ на ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ[1].

Однако, с данными выводами суда, по нашему мнению, согласиться нельзя, поскольку Л. совместно с соучастниками уже разместили в интернет-магазине сведения о сделанных «закладках» (об их наименовании, массе, координатах, внешнем виде и точном местонахождении с приложением фотографий). Суть такой незаконной деятельности заключается именно в предварительном размещении «закладок», выгрузки сведений о них на «витрину» интернет-магазина, то есть создание «оферты», и последующего получения прибыли.

Использование при незаконном обороте наркотических средств компьютерных программ, осуществляющих без участия оператора передачу потребителям информации о местах расположения тайников с наркотическими средствами, указывает на то, что виновное лицо, подготовив указанную информацию, выполнило все необходимые действия по передаче приобретателю наркотических средств[2].

---

[1] Кассационное определение Третьего кассационного суда общей юрисдикции от 20 апреля 2023 г. № 77-1080/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Кассационное определение Верховного Суда Российской Федерации от 19 июля 2022 г. № 44-УД22-18-К7. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, по нашему мнению, в случае пресечения противоправных действий сотрудниками правоохранительных органов такие лица должны нести уголовную ответственность за оконченное преступление, а в случае, когда информация о сделанных «закладках» не была размещена в интернет-магазине, то действия злоумышленников надлежит оценивать как неоконченное преступление. В противном случае наказуемость действий лиц, не успевших разместить сведения о тайниках с наркотическими средствами в интернет-магазине, и лиц, представивших всю необходимую информацию о «закладках» неограниченному кругу потребителей, будет определяться одинаково, с учетом правил, предусмотренных ч. 3 ст. 66 УК РФ, что не будет отвечать принципу справедливости, закрепленному в ст. 6 УК РФ.

Несмотря на описанное выше количество лиц, осужденных за совершение преступления, предусмотренного соответствующей частью статьи 228.1 УК РФ, при установлении в их действиях квалифицирующего признака «с использованием сети «Интернет», суды вышестоящих инстанций не всегда соглашаются с выводами районных судов относительно наличия в их действиях указанного квалифицирующего признака.

Например, 02.11.2023 судебной коллегией по уголовным делам Первого кассационного суда общей юрисдикции из действий осужденного, признанного виновным по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ, исключен квалифицирующий признак «с использованием сети «Интернет», поскольку при установленных судом первой инстанции обстоятельствах и квалификации действий осужденного не указано, какие именно устройства и программы использовались последним и какие действия совершены им с их помощью с использованием сети «Интернет»[1].

По смыслу закона преступление квалифицируется как совершенное с использованием сети «Интернет» независимо от стадии совершения преступле-

[1] Кассационное определение Первого кассационного суда общей юрисдикции от 2 ноября 2023 г. № 77-5043/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

ния, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такую сеть[1].

В частности, по признаку, предусмотренному п. «б» ч. 2 ст. 228.1 УК РФ, квалифицируются действия лица, которое с использованием сети «Интернет» разместило информацию для приобретателей наркотических средств.

Кроме того, Верховный Суд Российской Федерации разъяснил, что по указанному признаку квалифицируется и совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием сети «Интернет».

Например, при вынесении 04.10.2023 кассационного определения в отношении З. судебная коллегия по уголовным делам Верховный Суд Российской Федерации отметила, что действия соучастников и фактические обстоятельства уголовного дела свидетельствуют о том, что ими создана система взаимоотношений, когда члены группы напрямую не контактировали между собой и с ее организатором, а все взаимодействие, связанное с незаконным оборотом наркотических средств и психотропных веществ, осуществлялось через сеть «Интернет», ввиду чего указанный квалифицирующий признак признан доказанным в действиях осужденного.

Однако, по нашему мнению, основополагающим критерием наличия в действиях лица, квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228. 1 УК РФ, является именно факт осуществления сбыта наркотического средства, либо его предложение потребителю через сеть «Интернет»[2]. Анализ значительного числа уголовных дел показывает, что соучастники (например, так называемые «закладчик» и «куратор») осуществляют свое взаимодействие

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Комментарий к Уголовному кодексу Российской Федерации. В 3 т. Т. 3. Особенная часть (разделы IX—XII) / под общ. ред. О. С. Капинус ; науч. ред. К. В. Ображиев, Н. И. Пикуров. 2-е изд., перераб. и доп. М., 2022. С. 184.

исключительно через мессенджеры, обмениваясь между собой сведениями о местах нахождения тайников с наркотическими средствами. Указанные действия конспирируют соучастников, позволяют им удаленно вести дела.

Однако, указанные лица выполняют совокупность действий, направленных на достижение единого умысла – сбыта наркотических средств приобретателям. Вместе с тем друг другу соучастники ничего не сбывают, а потому, по нашему мнению, само их взаимодействие через сеть «Интернет» не может свидетельствовать о наличии в их действиях квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228. 1 УК РФ. Напротив, указанное взаимодействие только усиливает позицию стороны обвинения в том, что такие лица действовали совместно и согласовано.

Кроме того, до настоящего времени не разрешена проблема квалификации действий лиц, разместивших несколько «закладок» с наркотическими средствами и (или) психотропными веществами, как совокупности преступлений, либо как продолжаемого преступления.

Так, 31.10.2023 Пленум Верховного Суда Российской Федерации рассмотрел проект постановления «О некоторых вопросах судебной практики по уголовным делам о длящихся и продолжаемых преступлениях», в котором предложил квалифицировать действия лиц, имеющих умысел на сбыт одного объема наркотиков нескольким потребителям, при отсутствии с последними предварительной договоренности об этом, как самостоятельное преступление, предусмотренное соответствующей частью ст. 228.1 УК РФ, поскольку действия лица, связанные с поиском приобретателей наркотиков, размещенных в тайниках, их оповещением о местах «закладок», получением оплаты, свидетельствуют в каждом случае об умысле лица на совершение самостоятельных преступлений, предусмотренных соответствующей частью ст. 228.1 УК РФ[1].

Однако, вопреки позиции Верховного Суда Российской Федерации, полагаем, что такая уголовно-правовая оценка действий лиц возможна только

[1] Пленум Верховного Суда России рассмотрел постановление о практике по длящимся и продолжаемым преступлениям // Верховный Суд Российской Федерации : офиц. сайт. URL: https://vsrf.ru/press_center/news/33051/ (дата обращения: 09.11.2023).

в случае квалификации их действий как оконченного преступления, поскольку в каждом случае будет свой потребитель и отличные признаки приобретенного «товара» (наименование, масса, цена) и обстоятельства его приобретения (время покупки, место нахождения «закладки»)

Полагаем, что в случае квалификации действий лиц как покушения на преступление, предусмотренное соответствующей частью ст. 228.1 УК РФ, их действия должны быть квалифицированы как единое преступление, поскольку при таких обстоятельствах договоренностей с приобретателями еще не существует, сведения, хотя и размещены на «витрине» интернет-магазина, однако, сами наркотические средства еще не проданы.

С учетом позиции Генеральной прокуратуры Российской Федерации проект указанного постановления Пленума Верховного Суда Российской Федерации направлен на доработку.

Исходя из изложенного, полагаем, что в целях правильного установления в действиях лиц, совершивших преступление, предусмотренное соответствующей частью ст. 228.1 УК РФ, квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228. 1 УК РФ, необходимо исходить из следующего:

1) размещение на «витрине» интернет-магазина сведений о тайниках с наркотическими средствами (их наименовании, внешнем виде, массе, координатах с точным описанием местонахождения) свидетельствует о том, что лицо предприняло все необходимые и зависящие от него действия, направленные на незаконный сбыт наркотических средств, а потому его действия должны быть квалифицированы как оконченное преступление;

2) взаимодействие соучастников преступления между собой через сеть «Интернет» по вопросам незаконного сбыта наркотических средств не свидетельствует о наличии в действиях последних квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ;

3) факт размещения на «витрине» интернет-магазина информации о ряде сделанных тайников с наркотическими средствами в рамках единого умысла свидетельствует о совершении лицом единого продолжаемого преступления, а не совокупности преступлений.

УДК 343

А. В. ЗАРУБИН

НЕКОТОРЫЕ ВОПРОСЫ ОТВЕТСТВЕННОСТИ ЗА ОРГАНИЗАЦИЮ И ПРОВЕДЕНИЕ АЗАРТНЫХ ИГР, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ»

Введенный Федеральным законом № 244-ФЗ от 29 декабря 2006 г. «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» запрет организации и проведения азартных игр вне специально отведенных для данной деятельности территорий привел к тому, что многие владельцы игорных заведений, не пожелавшие прекращать столь прибыльное занятие, приняли решение продолжить игорный бизнес нелегальными способами.

Такая деятельность наносит огромный ущерб экономике, поскольку сопровождается неуплатой налогов и других обязательных платежей в бюджеты. Исходя из объема поступлений в российский бюджет от легальной игорной деятельности, который в 2008 г. по оценкам специалистов составил около 24 млрд руб.[1], можно предположить, что после введения полных ограничений деятельности игорных заведений (с июля 2009 г.) государственная казна недополучает отчисления также в указанных пределах.

Федеральным законом от 20.07.2011 № 250-ФЗ в УК РФ введена ст. 171.2, предусматривающая ответственность за организацию и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны, либо с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной связи,

[1] Игорный бизнес в современной России // Смотрим глубже — Memoid.ru : сайт. URL: https://www.memoid.ru/node/Igornyj_biznes_v_sovremennoj_Rossii (дата обращения: 27.02.2012).

либо без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне[1].

По нашему мнению, данную статью необходимо признать специальной нормой по отношению к ст. 171 УК РФ, предусматривающей ответственность за незаконное предпринимательство.

При этом дискуссионным до настоящего времени является вопрос: является ли игорный бизнес видом предпринимательской деятельности? С одной стороны, проведение и организация азартных игр — это деятельность, которая напрямую, как и любая предпринимательская деятельность, направлена на получение дохода, прибыли (п. 1 ст. 2 ГК РФ), с другой Федеральным законом[2] предусмотрены игорные зоны, в связи с чем организация и проведение азартных игр вне обозначенных зон запрещено. Тем самым данный вид деятельности может быть осуществлен только на определенной территории.

Мы считаем оправданным расположение рассматриваемой нормы в главе 22 «Преступления в сфере экономической деятельности» в связи с тем, что незаконные организация и проведение азартных игр нарушают нормальное функционирование экономической сферы, препятствуют реализации законной предпринимательской деятельности, а также порождают многочисленные нарушения в разных отраслях права (налогового, трудового и т.д.), ущемляя при этом законные интересы государства, организаций и граждан.

Для оказания услуг, связанных с азартными играми, необходима организация предпринимательской деятельности, направленной на получение дохода, выраженная в подготовке помещения, его оборудования для проведения процесса игры, подборе кадров, участвующих в процессе проведения игорной деятельности.

---

[1] Лихолетов А. А. Уголовно-правовые и криминологические проблемы противодействия незаконному игорному бизнесу : автореф. дис. ... канд. юрид. наук. Саратов, 2013. С. 4.

[2] О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации : Федеральный закон от 29 декабря 2006 г. № 244-ФЗ : текст с изм. и доп. на 2 июля 2021 г. Ч. 1 ст. 3. Доступ из справ.-правовой системы «КонсультантПлюс».

Реализация деятельности, связанной с незаконными организацией и проведением азартных игр по данному шаблону становится источником совершения преступлений гражданами, ранее не привлекавшимися к уголовной ответственности, в силу либо их неосведомленности и наступлении ответственности за действия, квалифицируемые по ст. 171.2 УК РФ, либо определенных обстоятельств, совершающих иные преступления (кражи, разбой, мошенничество, убийство и т. д.).

Ущерб, наносимый государству от данного вида деятельности достаточно внушителен, в связи с чем, запрет на осуществление деятельности по организации и проведению азартных игр, за исключением определенных игорных зон, оправдан, а также выступает средством защиты не только граждан, но и государства, направлен на минимизацию последствий, связанных с незаконной предпринимательской деятельностью, отражающейся на здоровье и нравственности общества.

Таким образом, объектом преступления являются общественные отношения, складывающиеся по поводу законной организации и проведения азартных игр.

С нашей точки зрения, дополнительным объектом ст. 171.2 УК РФ являются общественные отношения, обеспечивающие права и законные интересы юридических лиц по организации и проведению азартных игр в игорной зоне, а также пополнение бюджета государства от рассматриваемой деятельности и ее налогообложение.

Объективная сторона незаконных организации и проведения азартных игр по своей конструкции характеризует формальный состав преступления, т. е. преступление признается оконченным с момента организации или проведения азартных игр.

А.И. Чучаев под организацией азартных игр понимает «действия, направленные на оборудование помещений необходимым инвентарем для проведения игорной деятельности, создания штата сотрудников и привлечение лиц, желающих принять участие в азартной игре, а также иные действия, обеспе-

чивающие возможность функционирования игорного заведения»[1]. Мы поддерживаем мнение А.И. Чучаева, и полагаем, что оборудование представляет собой неотъемлемую часть организации и проведения азартных игр.

Дискуссию вызывает вопрос, связанный с определением средств совершения преступлений, предусмотренных ст. 171.2 УК РФ. Под ним понимаются вещества, инструменты, иные средства, которые используются при реализации преступного умысла[2]. По нашему мнению, средством совершения преступлений, предусмотренных ст. 171.2 УК РФ, выступает игровое оборудование, с помощью которого осуществляется незаконные организация и проведение азартных игр. Усынин В. В. отмечает, что к перечню игрового оборудования не относится оборудование, которое используется при проведении букмекерских контор и тотализаторов (мониторы, системные блоки, телевизоры, системы видеонаблюдения)[3]. Мы в полной мере разделяем данную позицию.

М.Ф. Костюк под игровым оборудованием понимает «устройства или приспособления, используемые для проведения азартных игр»[4].

На сегодняшний день не выработано единого мнения относительно понятия «игровое оборудование», а имеющиеся формулировки не раскрывают полностью его содержание, обладая лишь субъективной оценкой.

Думается, что под игровым оборудованием следует понимать совокупность связанных между собой частей, устройств и приспособлений, конструктивно предназначенных для организации и проведения азартных игр.

Признание устройства или приспособления, которое задействовано в организации и проведении азартных игр, игровым оборудованием представляется сложным.

---

[1] Уголовное право. Особенная часть : учебник для бакалавров / [Ю. В. Грачева и др.] ; под ред. А. И. Чучаева. М., 2012. С. 181.

[2] Кустов А. М. Теоретические основы криминалистического учения о механизме преступления. М., 1997. С. 87.

[3] Усынин В. В. Средство совершения преступления — азартных игр // Тенденции науки и образования в современном мире. Самара, 2015. № 9. С. 65.

[4] Костюк М. Ф. Незаконные организация и проведение азартных игр (статья 171² Уголовного кодекса Российской Федерации) вопросы правовой оценки // Вестник Челябинского государственного университета. Серия: Право. 2015. № 4 (359), вып. 41. С. 111.

Важный аспект раскрывает Верховный Суд Российской Федерации в Постановлении от 28.08.2015, в котором отмечается проведение экспертизы сотрудниками ЭКЦ ГУ МВД России, перед которыми ставился вопрос о том, «имеется ли на представленном оборудовании программное обеспечение атрибутирующее себя как игровое?». Однако на данный вопрос не нашел однозначного отражения в проведенной экспертизе, что повлекло прекращение дела в связи с недоказанностью обстоятельств, на основании которых вынесены указанные судебные постановления. В рамках данного Постановления также отмечалось, что общество занималось производством игровых автоматов для организации азартных игр, т. е. были условия для разработки программ[1].

Необходимо отметить широкий спектр игровых платформ, используемых для реализации рассматриваемой деятельности. Например, программная платформа «TRADE BOX»; «Wintrade» («Гермес») (платформа доступна в двух видах: в виде программного обеспечения «Wintrade», устанавливаемого на конкретную ЭВМ, а также в виде интернет-ресурса с аналогичным функционалом); «Доминатор», «GMT» и т. д.[2]

По действующему законодательству к ответственности не может быть привлечено лицо, которое незаконно изготовило, модифицировало, хранило или реализовывало игровое оборудование. Таким образом, лица, осуществляющие вышеуказанные действия, избегают ответственности, а их действия представляют собой источник нарушения законодательства.

В соответствии с ФЗ № 244 п. 6 ст.4 под деятельностью по организации и проведению азартных игр понимают «деятельность по оказанию услуг по заключению с участниками азартных игр основанных на риске соглашений о выигрыше и (или) по организации заключения таких соглашений между двумя или несколькими участниками азартной игры». Исходя из данного определе-

[1] Постановление Верховного Суда Российской Федерации от 28 августа 2015 г. № 41-АД15-4. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Астахова Л. В., Волков А. В., Григорьев В. В., Роговский А. А. Современные программно-аппаратные средства организации и проведения азартных игр и их правовой статус // Наука, техника и образование. 2017. № 6. С. 33—34.

ния очевиден факт необходимости приложения определенных усилий для осуществления деятельности по организации и проведению азартных игр. Соответственно, можно сделать вывод о том, что преступления, уголовная ответственность за которые предусматривается ст. 171.2 УК РФ, совершаются путем действия.

Состав преступления, предусмотренного ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр», является формальным. Диспозиция статьи указывает на тот факт, что деяние совершается путем действия, чем характеризует объективную сторону преступления.

Исходя из формулировки диспозиции статьи 171.2 УК РФ, мы полагаем, что объективная сторона незаконных организации и проведения азартных игр выражается в формах:

1) организация и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны;

2) организация и (или) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной;

3) организация и (или) проведение азартных игр без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне[1].

Незаконные организация и проведение азартных игр в основном осуществляется «с использованием программно-аппаратного комплекса, Интернет-ресурсов, а также букмекерскими конторами без соответствующих лицензий»[2]. Отсюда рассмотрим следующую форму объективной стороны преступления, предусмотренного ст. 171.2 УК РФ, — организацию и проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной.

---

[1] Кормильцева С. О. Уголовная ответственность за незаконную организацию и проведение азартных игр // Вестник Казанского юридического института МВД России. 2016. № 1 (23). С. 120.

[2] Меркурьева В. В. Борьба с криминальными рынками в России : монография. М., 2015. С. 260.

В литературе выражено мнение, что сеть «Интернет» может быть признана «средством исполнения противоправных действий, и местом совершения деяния»[1]. В узком смысле «под местом совершения любых компьютерных преступлений понимается фактическое местоположение пользователя компьютера и самой ЭВМ, с помощью которой совершено общественно опасное деяние. Компьютер будет представлять собой средство совершения преступления, то есть фактическое средство доступа в сеть «Интернет». Орудием совершения подобных преступлений будут являться компьютерные программы»[2]. Данное мнение разделяют и другие исследователи, высказывающие точку зрения, согласно которой «при проведении азартных игр с использованием сети «Интернет» местом заключения соглашения о выигрыше следует признавать место нахождения игрока (физического лица, осуществляющего ставку), а не место регистрации организатора азартных игр (юридического лица) или место расположения игрового сервера. Это позволит реализовать уголовно-правовой запрет на проведение азартных игр с использованием сети «Интернет», предусмотренный ст. 171.2 УК РФ»[3].

В диспозиции ст. 171.2 УК РФ есть указание на то, что организация и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны либо с использованием информационно-телекоммуникационных сетей возможно с помощью сети «Интернет».

В литературе выделяется ряд теоретических проблем, возникающих при совершении преступлений в сети «Интернет». Одной из них является представляется проблема привлечения к юридической ответственности за нанесение реального ущерба правам физических и юридических лиц — пользователей сети «Интернет». Следующей проблемой выступает территориальность, поскольку

---

[1] Дашян М. С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет». М., 2007. С. 81.

[2] Актуальные проблемы уголовного права и криминологии : сборник научных трудов кафедры уголовного права / А. А. Арямов, А. В. Бриллиантов, М. А. Кауфман [и др.] ; Российская академия правосудия. М., 2013. Вып. 3. С. 198.

[3] Науменко О. П. Уголовная ответственность за незаконные организацию и проведение азартных игр : автореф. дис. ... канд. юрид. наук. М., 2016. С. 8.

совершенные преступления «могут попадать под несколько юрисдикций благодаря глобальной и межгосударственной природе сети «Интернет»[1].

Наконец не можем не назвать такую проблему как анонимность и зарождающееся чувство безнаказанности у лица, совершающего преступное деяние, в связи с реальной возможностью, обладая необходимыми специальными знаниями, скрыть следы совершенного общественно опасного деяния, свое фактическое место нахождения и данные о личности, тем самым лишая правоохранительные органы возможности раскрыть преступление.

Данную позицию поддерживает, в частности, О. М. Сафронов, который утверждает: «Сложность обнаружения действия компьютерного преступника и его возможности совершать преступления в киберпространстве, не имеющем государственных границ, многократно увеличивают степень общественной опасности таких деяний»[2].

Осуществление незаконной деятельности по организации и (или) проведению азартных игр без специального разрешения можно отметить в следующих случаях:

1. Организация и (или) проведение азартных игр осуществляются без специального разрешения;

2. Деятельность по организации и (или) проведению азартных игр осуществляется при наличии разрешения, но ранее даты, зафиксированной в нем, с которой организатору разрешено осуществлять деятельность;

3. Деятельность по организации и (или) проведению азартных игр реализуется при наличии разрешения, но на иной территории, указанной в разрешении;

4. Деятельность по организации и (или) проведению азартных игр ведется после аннулирования разрешения.

---

[1] Дремлюга Р. И. Интернет-преступность : дис. ... канд. юрид. наук. Владивосток, 2007. С. 49.

[2] Сафронов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования : автореф. дис. ... канд. юрид. наук. М., 2015. С. 3.

Субъект преступлений, предусмотренных ст. 171.2 УК РФ, общий, т. е. вменяемое физическое лицо, достигшее к моменту совершения преступления возраста шестнадцати лет.

В настоящее время высказываются точки зрения, согласно которым субъектами отдельных преступлений в сфере экономической деятельности, в частности игорной деятельности, могут быть лица, достигшие возраста 18 лет, данное мнение обосновывается тем, что согласно гражданскому законодательству, а именно ст. 21 Гражданского кодекса Российской Федерации, дееспособность возникает в полном объеме с наступлением совершеннолетия, то есть по достижении восемнадцатилетнего возраста[1].

На наш взгляд, данная позиция представляется недостаточно убедительной, на том основании, что гражданским законодательством предусмотрены условия получения полной дееспособности ранее достижения совершеннолетия (вступление в брак, решение органа опеки, попечительства, суда о признании лица полностью дееспособным[2]. Гражданское законодательство ст. 27 ГК РФ дает право заниматься предпринимательской деятельностью эмансипированному лицу.

Обобщая изложенное, полагаем, что увеличение возраста субъекта преступления, предусмотренного ст. 171.2 УК РФ до 18 лет, несмотря на имеющиеся справедливые в определенной мере позиции специалистов, по нашему мнению, нецелесообразно. Изменения возрастного ценза повлекут за собой новые факты совершения общественно опасных действий, предусмотренных ст. 171.2 УК РФ, уголовной ответственности за которые в силу возраста можно будет не опасаться. В качестве исполнителей возможно привлечение лиц, не достигших совершеннолетнего возраста, так и совершеннолетних лиц, которые способны в полной мере осознавать фактический характер и общественную опасность своих действий.

---

[1] Авдеева О. А. Незаконное предпринимательство: уголовно-правовая характеристика и ответственность : автореф. дис. … канд. юрид. наук. Иркутск, 2009. С. 9.

[2] Кормильцева С. О. Указ. соч. С. 122.

УДК 343

Н. Н. КАДЫРОВА

К ВОПРОСУ О ЗНАЧЕНИИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ

Значение научно-технического прогресса сложно переоценить, но в контексте уголовной политики его достижения не являются однозначными.

Согласно нормам Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Вопрос определения категории электронных или информационно-телекоммуникационных сетей в рамках уголовного судопроизводства до 2022 года не имел своего официального оформления, несмотря на объективную необходимость урегулирования данного вопроса с учетом значения использования электронных или информационно-телекоммуникационных сетей при совершении преступлений.

Законодательные конструкции составов общественно опасных деяний в действующем УК РФ учитывают рассматриваемую категорию не только в контексте главы 28, но и в других преступлениях, для которых нетипично использование электронных или информационно-телекоммуникационных сетей при совершении преступлений. К числу таких преступлений могут быть отнесены деяния, предусмотренные ст.ст. 110, 110.1, 128.1, 133, 137, 151.2 и другие нормы УК РФ, рассмотрение которых в совокупности позволяет данную категорию признать самостоятельным критерием криминализации.

Действительно, использование электронных или информационно-телекоммуникационных сетей при совершении преступлений не только формально повышает общественную опасность деяния, но и облегчает его совершение, существенно расширяя круг лиц — жертв преступлений.

Обращает на себя внимание то обстоятельство, что далеко не всегда при наличии формальных признаков совершения конкретных деяний с использованием электронных или информационно-телекоммуникационных сетей речь идет именно об уголовном преследовании. Например, такая ситуация имеет место в случаях вовлечения несовершеннолетнего в совершение действий, представляющих опасность для его жизни.

До настоящего времени в содержании Постановления Пленума Верховного Суда Российской Федерации от 01.02.2011 № 1 (ред. от 28.10.2021) «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних»[1] отсутствует легальное толкование положений ст. 151.2 УК РФ в части определения момента окончания данного преступления, что является очевидным пробелом и приводит к формированию неоднозначной судебной практики. Так, распространенными примерами в правоприменительной практике являются решения судов, принимаемые в интересах Российской Федерации и неопределенного круга лиц, о запрете распространения информации, содержащей материалы по обучению и пропаганде различных форм опасного для жизни девиантного поведения среди несовершеннолетних, в том числе «руфинга» (крышелазание) — хождения по самому краю крыши высотных зданий и сооружений с фиксацией происходящего на фото и видео[2].

Таким образом, значение электронных или информационно-телекоммуникационных сетей при квалификации преступлений возможно не только исключительно в случаях, прямо указанных в уголовном законе, но и при наличии официальных разъяснений по применению соответствующих норм.

Попытка решения данного вопроса была предпринята в 2022 году с принятием Постановления Пленума Верховного суда Российской Федерации

[1] О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : Постановление Пленума Верховного Суда Российской Федерации от 1 февраля 2011 г. № 1 : текст с изм. и доп. на 28 окт. 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Решение Калининского районного суда г. Тюмени от 29 июля 2020 г. по делу № 2А-3931/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/St5JLIdNPZo4 (дата обращения: 23.11.2023).

«О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[1].

Согласно п. 17 Постановления Пленума Верховного Суда Российской Федерации 2022 года «для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются», а сеть «Интернет» является одной из таких. Важность принятия данного документа сомнений не вызывает. Большое значение имеет унификация не только значения терминов, используемых в диспозициях соответствующих статей УК РФ, но и определении порядка разрешения вопросов в части оценки значения места совершения таких преступлений и института соучастия при их совершении.

Представляется, что остается неразрешенным вопрос общего характера: следует ли признавать использование электронных или информационно-телекоммуникационных сетей при совершении преступлений всегда в качестве обстоятельства, отягчающего уголовную ответственность. Анализ положений отечественного уголовного закона позволяет сделать вывод о его пробельности в этой части. Очевидно необходима ревизия отечественного уголовного закона на предмет включения данного признака не только в ряд статей Особенной части УК РФ, объективно обусловленную распространенностью их совершения с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», например, в стст.148, 296 УК РФ, но и в ч. 2 ст. 63 УК РФ.

Так, ученые в МГЮА имени О. Е. Кутафина в рамках юбилейной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» обсудили проблемы применения ст. 148 УК РФ. В частности, А. Г. Кибальник

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

отметил, что в качестве деяний, образующих оскорбление чувств верующих, судами признаются публикации в сети «Интернет», в том числе на религиозную тему, которые не носят научного характера, а также нецензурная брань на фоне религиозных символов и их публичное оскорбление[1].

Совершение общественно опасных деяний, выражающихся в высказывании угрозы в связи с осуществлением правосудия или производством предварительного расследования с использованием электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», латентны, но более опасны.

Так, Следственный комитет Российской Федерации возбудил уголовные дела в связи с опубликованием в сети «Интернет» угроз в адрес судьи Мосгорсуда[2]. Остается дискуссионной сама тема уголовной ответственности за лайки и репосты в сети «Интернет».

Существенное криминологическое значение имеет размещение в электронных или информационно-телекоммуникационных сетях, включая сеть «Интернет», информации, пропагандирующей насилие и жестокость, которая в большей степени оказывает негативное воздействие на формирование личности несовершеннолетних, а также способствует росту числа подражателей. Некоторые информационные ресурсы не только содержит информацию об обстоятельствах совершенных преступлений, но и фактически выступает «учебником» для отдельных субъектов, о чем свидетельствуют их показания во время следствия.

Так, Генеральная прокуратура Российской Федерации в рамках круглого стола в Совете Федерации по теме «Актуальные вопросы противодействия популяризации криминальной субкультуры среди несовершеннолетних» высту-

[1] Велимирова В. Ученые обсудили противоречия законодательства о защите чувств верующих // Адвокатская газета. 2018. 29 янв. URL: https://www.advgazeta.ru/novosti/uchenye-obsudili-protivorechiya-zakonodatelstva-o-zashchite-chuvstv-veruyushchikh/ (дата обращения: 25.11.2023).

[2] СК возбудил дело из-за поступивших судье Мосгорсуда угроз убийством // RBC : сайт. URL: https://www.rbc.ru/society/11/11/2019/5dc9bdf39a7947820cf2e04a?ysclid=lpqwk38ezi955632010 (дата обращения: 25.11.2023).

пила с инициативой запрета опубликования информации о преступлениях, совершенных несовершеннолетними, с целью недопущения формирования у других лиц, не достигших возраста уголовной ответственности, намерений на совершение аналогичных преступлений[1].

Еще одной, пока нереализованной инициативой, является предложение от депутатов партии «Единая Россия» на запрет на срок до 70 лет «публикации в СМИ, интервью, публичные выступления и ведение социальных сетей для лиц, осужденных за насильственные преступления». Данные ограничения должны распространяться на лиц, которые были осуждены по ст.ст. 105—125, 131-135 УК РФ[2]. Это предложение, безусловно, заслуживает внимания, учитывая его профилактический потенциал.

Подводя итог изложенному выше, важно указать на значительное влияние электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», на современное состояние уголовной политики и криминальной обстановки в Российской Федерации.

УДК 343

А. В. КАФИАТУЛИНА

ПОРЯДОК И ПРАКТИКА НАЗНАЧЕНИЯ ЛИШЕНИЯ ПРАВА ЗАНИМАТЬ ОПРЕДЕЛЕННЫЕ ДОЛЖНОСТИ ИЛИ ЗАНИМАТЬСЯ ОПРЕДЕЛЕННОЙ ДЕЯТЕЛЬНОСТЬЮ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Как представляется, назначение уголовного наказания — это исключительная прерогатива суда, осуществляемая в ходе уголовного судопроизводства на основании норм уголовного и уголовно-процессуального законодательства, результат которого отражается в итоговом процессуальном документе —

[1] Эксперты дали оценку идее запрета публикаций о преступлениях подростков // RG RU. Новости : сайт. URL: https://rg.ru/2019/10/31/eksperty-dali-ocenku-idee-zapreta-publikacij-o-prestupleniiah-podrostkov.html?ysclid=lpqvq8jfih956848828 (дата обращения: 25.11.2023).

[2] Солопова С. Запрет на интервью для убийц может составить до 70 лет // Радио Комсомольская правда. 97.2 : сайт. URL: https://radiokp.ru/obschestvo/zapret-na-intervyu-dlya-ubiyc-mozhet-sostavit-do-70-let_nid428144_au40439au?ysclid=lpqvu6zdmk996586765 (дата обращения: 25.11.2023).

приговоре. Вид и размер наказания должен соответствовать степени общественной опасности преступления, обстоятельствам его совершения и личности виновного. Сам приговор должен отвечать требованиям законности, обоснованности и справедливости.

Одним из видов наказаний, который может быть назначен виновному в совершении преступления, — лишение права занимать определенные должности или заниматься определенной деятельностью (ст. 47 УК РФ), для несовершеннолетних — лишение права заниматься определенной деятельностью (ст. 88 УК РФ).

Чаще всего названное наказание назначается в качестве дополнительного вида, причем даже при отсутствии его в санкции статьи Особенной части УК РФ, по которой квалифицировано деяние (с обязательной ссылкой на ч. 3 ст. 47 УК РФ).

Лишение права занимать определенные должности или заниматься определенной деятельностью как дополнительный вид наказания подлежит назначению, когда оно в таком качестве прямо предусмотрено в санкции соответствующей статьи Особенной части УК РФ как обязательное дополнительное наказание (ч. 3 ст. 272, ч. 1 ст. 281.1 УК РФ и др.) или факультативное дополнительное наказание (ч. 2 ст. 273, чч. 3 и 4 ст. 274.1 УК РФ и др.).

Решение вопроса о назначение обязательного дополнительного наказания является обязанностью суда. Неприменение такого вида наказания возможно лишь при наличии исключительных обстоятельств, связанных с целями и мотивами преступления, ролью виновного, его поведением во время или после совершения преступления, и других обстоятельств, существенно уменьшающих степень общественной опасности преступления.

Назначение факультативного дополнительного наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью — дискреционное полномочие суда, при этом вопрос и назначении или неназначении названного вида наказания должен быть мотивирован в описательно-мотивировочной части приговора.

Ранее мы отмечали, что рассматриваемый вид наказания используется преимущественно для охраны следующих объектов: «Преступления против личности» (раздел VII) — 27 %, «Преступления в сфере экономики (раздел VIII) — 16,2 %, «Преступления против общественной безопасности и общественного порядка» (раздел IX) — 32, 4 %, «Преступления против государственной власти» (раздел X) — 24.4 %[1].

Для более репрезентативной выборки, мы не стали ограничиваться лишь главой 18 УК РФ «Преступления в сфере компьютерной информации», а охватили составы, предусматривающие квалифицирующий признак — с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), размещенные в иных разделах и главах УК РФ.

Выборочный анализ судебных решений показал следующие результаты.

Н. осужден по ч. 1 ст. 205.2 УК РФ (в ред. Федерального закона от 07.12.2011 № 420-ФЗ), по ч. 2 ст. ст. 205.2 УК РФ, по ч. 2 ст. 280 УК РФ, ему назначено дополнительное наказание в виде лишения права занимать должности, связанные с администрированием сайтов. Верховный Суд Российской Федерации приговор изменил, лишив Н. права заниматься деятельностью, связанной с администрированием сайтов с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»[2]. Сформулированная Верховным Судом Российской Федерации правоограничительная мера в приведенной редакции устанавливает запрет на создание и ведение собственных страниц в сети «Интернет» и администрирование чужих ресурсов и не предполагает полный заперт на доступ в информационно-телекоммуникационной пространство.

---

[1] Кафиатулина А. В. Лишение права занимать определенные должности или заниматься определенной деятельностью: уголовно-правовой и уголовно-исполнительный аспекты : дис. ... канд. юрид. наук. М., 2019. С. 114.

[2] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 15 марта 2018 г. № 201-АПУ18-8. Доступ из справ.-правовой системы «КонсультантПлюс».

Приведенное решение высшего судебного органа стало ориентиром для судов, которые при назначении дополнительного наказания лицу, признанному виновным в размещении в открытом доступе запрещенных материалов, стали дословно использовать предложенную формулировку.

Назначение наказания, предусмотренного ст. 47 УК РФ, предполагает лишение права заниматься как профессиональной, так и иной деятельностью, вид которой должен быть конкретизирован в приговоре.

Верховный Суд Российской Федерации сформулировал позицию, согласно которой, к профессиональной деятельности относится деятельность, осуществляемая на постоянной основе за определенное вознаграждение или с целью извлечения прибыли[1].

Наказание, предусмотренное ст. 47 УК РФ, имеет ярко выраженный превентивный характер, лишая осужденного перспективы злоупотребления возможностями, вытекающими из занятия той или иной деятельностью, в целях предупреждения повторного совершения им аналогичного преступления, что предопределяет необходимость разумной конкретизации в приговоре — при условии его исполнимости — запрещаемой профессиональной или другой деятельности.

Однако зачастую правоприменитель допускает чрезмерную конкретизацию вида деятельности, подлежащего запрету, не использует понятия, раскрытые в нормах позитивного права, что может повлечь уменьшение потенциала превентивного воздействия.

Так, П., являясь учредителем информационного агентства, потребовала от потерпевшего передачи денежных средств, а также заключение сделки под угрозой распространения сведений, который могут причинить существенный вред последнему и членам его семьи. П. признана виновной в совершении преступлений, предусмотренных п. «г» ч. 2 ст. 163, ч. 1 ст. 179 УК РФ, ей назначено дополнительное наказание в виде лишения права заниматься трудовой

[1] О практике назначения судами Российской Федерации уголовного наказания : Постановление Пленума Верховного Суда Российской Федерации от 22 декабря 2015 г. № 58 : текст с изм. и доп. на 18 дек. 2018 г. Доступ из справ.-правовой системы «КонсультантПлюс».

деятельностью в средствах массовой информации: периодических печатных изданиях, сетевых изданиях, телеканалах, радиоканалах, телепрограммах, радиопрограммах, видеопрограммах, кинохроникальных программах, иных формах периодического распространения массовой информации под постоянным наименованием (названием). На наш взгляд, приведенная формулировка имеет чрезмерную конкретизацию. Используя понятия, которыми оперируют нормы позитивного права, в указанном случае — это Федеральный закон «О средствах массовой информации», мы предлагаем следующую формулировку - лишение права заниматься деятельностью, связанной с распространением продукции средств массовой информации, под которой понимается продажа, подписка, доставка, раздача периодического печатного издания, аудио- или видеозаписи программы, вещание телеканала, радиоканала (телевизионное вещание, радиовещание), вещание телепрограммы, радиопрограммы в составе соответственно телеканала, радиоканала, демонстрация кинохроникальной программы, предоставление доступа к сетевому изданию, иные способы распространения.

Д. разместил в сети «Интернет» собственную статью, признанное решением суда экстремистским материалом, за что осужден по ч. 1 ст. 205.2 УК РФ с назначением дополнительного наказания в виде лишения права заниматься публицистической деятельностью[1].

Руководитель отделения политической партии А. опубликовала в издании, учредителем которой она являлась, собственную статью, в которой содержалась негативная оценка социальной группы по признаку ее национальной принадлежности, языка и религии. А. осуждена по ч. 1 ст. 282 УК РФ, ей назначено дополнительное наказание в виде лишения права заниматься журналистикой и издательской деятельностью.

При осуждении виновных по ст. 272 УК РФ правоприменитель игнорирует недопустимость запрета занимать должности вне государственной

[1] Определение Верховного Суда Российской Федерации от 2 октября 2010 г. № 51-О10-94. Доступ из справ.-правовой системы «КонсультантПлюс».

службы и службы в органах местного самоуправления[1]. Так, сотруднику сотовой компании за копирование данных абонентов по ч. 3 ст. 272 УК РФ назначено наказание в виде лишения права занимать должности, связанные с доступом к охраняемой законом компьютерной информации.

Санкция ч. 3 ст. 272 УК РФ предусматривает обязательное дополнительное наказание в виде лишение права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Зачастую по ч. 3 ст. 272 УК РФ суды назначают наказание в виде лишения права заниматься деятельностью, связанной с доступом к персональным данным граждан[2].

Под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[3]. Правильной, на наш взгляд, представляется следующая формулировка — лишение права заниматься деятельностью, связанной со сбором и обработкой персональных данных.

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации. Под неправомерным доступом к компьютерной информации понимается получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа)[4]. Представляется возможным по ст. 272 УК РФ назначать

---

[1] Кафиатулина А. В., Хромов Е. В. Лишение права занимать определенные должности или заниматься определенной деятельностью как вид уголовного наказания : монография. М., 2024. С. 97.

[2] См., напр.: Приговор Междуреченского городского суда Кемеровской области от 18 октября 2017 г. № 1-8/2017, Приговор Кировского районного суда г. Томска Томской области от 7 сентября 2017 г. № 1-5/2017 (Государственная автоматизированная систем Российской Федерации «Правосудие» : интернет-портал. URL: https://sudrf.ru (дата обращения: 20.09.2023).)

[3] О персональных данных : Федеральный закон от 27 июля 2006 г. № 152-ФЗ : текст с изм. и доп. на 6 февр. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть

дополнительное наказание в виде лишения права заниматься деятельностью, связанной с системным администрированием охраняемой законом компьютерной информации.

Подводя итог сказанному, отметим, что наказание в виде лишения права занимать определенные должности или заниматься определенной деятельностью имеет ярко выраженный превентивный характер, лишая осужденного перспективы злоупотребления возможностями, вытекающими из занятия той или иной деятельностью, в целях предупреждения повторного совершения им аналогичного преступления, что предопределяет необходимость разумной конкретизации в приговоре — при условии его исполнимости — запрещаемой профессиональной или другой деятельности.

УДК 343

Я. М. КИРИЛЛОВА

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

В настоящее время использование и в науке уголовного права и в правоприменении обращается существенное внимание на значительное увеличение количества преступлений, совершаемых в сети «Интернет». При этом многие проблемы квалификации рассматриваемой группы преступлений не нашли единого решения.

Одна из проблем квалификации связана, по нашему мнению, с правовым статусом криптовалюты. Правовая определенность предмета преступления против собственности находится в плоскости гражданского права (в общих и специальных нормах). С введением в действие федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ, правовой статус криптовалюты остается неясным.

«Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

Несмотря на то, что российское законодательство (п. 10 ст. 8 Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции») и судебная практика признают биткоин и биткоин-кошельки имуществом[1], официальным средством платежа криптовалюта не является.

Вместе с тем, следует согласиться с мнением представителей науки уголовного права о том, что криптовалюта является иным имуществом, которое может быть предметом хищения[2] или вымогательства. При этом квалификация хищений, по нашему мнению, должна происходить по общей норме о мошенничестве (ст. 159 УК РФ) или краже (ст. 158 УК РФ), в зависимости от способа хищения. При наличии признаков мошенничества в отношении криптовалюты, безусловная квалификация такого хищения по статьям, предусматривающим ответственность за специальные мошенничества (ст. 159.3., ст. 159.6. УК РФ) являлась бы ошибочной.

Состав преступления, предусмотренный ст. 159.3. УК РФ (мошенничество с использованием электронных средств платежа) предполагает совершение хищения путем обмана или злоупотреблением доверием с использованием официально признанных средств платежа. Как было указано ранее, криптовалюта относится к иному имуществу и не является средством платежа.

В то же время, хищение криптовалюты в форме мошенничества, не всегда связано с теми способами, которые описаны в диспозиции ст. 159.6. УК РФ. Зачастую потерпевшего вводят в заблуждение относительно намерений «покупателя» криптовалюты, и он добровольно передает предмет хищения без встречного предоставления, либо виновный получает неправомерный доступ к криптокошельку или иному виртуальному хранилищу, и совершает

---

[1] Постановление Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП-16416/18, Определение Верховного Суда Российской Федерации от 2 февраля 2021 г. № 44-КГ20-17-К7. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Малыгин И. И., Русскевич Е. А. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 115—117.

незаконное изъятие и обращение в свою пользу или в пользу третьих лиц, что образует состав хищения в форме тайного хищения имущества — кражи по совокупности с ч. 2 ст. 272 УК РФ — неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности (при наличии признаков состава преступления).

К сожалению, на практике распространены случаи неполной квалификации преступлений в случае тайного хищения не только криптовалюты, но и других объектов «виртуального мира», когда виновный получает неправомерный доступ к криптокошелькам и (или) аккаунтам владельца имущества из корыстной заинтересованности (ч. 2 ст. 272 УК РФ) или создает, использует или распространяет вредоносные компьютерные программы для получения неправомерного доступа к имуществу из корыстной заинтересованности (ч. 2 ст. 273 УК РФ).

Очевидно, что при таких действиях виновного, квалификация по статьям, предусматривающим ответственность за хищение, является недостаточной и не учитывает причинение вреда иному объекту уголовно-правовой охраны – общественным отношениям, обеспечивающим безопасность компьютерной информации.

Хищение криптовалюты с использованием фишинговых сайтов также должно квалифицироваться по соответствующей части статьи 158 УК РФ, поскольку обман в тождестве сайта и правомерности ввода логина и пароля всего лишь облегчает доступ к имуществу – криптовалюте, а само хищение происходит тайно, владелец цифровой валюты или криптокошелька сам не отдает имущество под влиянием обмана.

Другой проблемой квалификации преступлений против собственности при неопределенности предмета посягательства, к которой бы хотелось обратиться, является проблема надлежащей оценки противоправных деяний, совершенных в виртуальном пространстве и (или) в отношении объектов виртуального мира.

Объекты виртуального мира, к которым приложен человеческий труд, в которые вложены такие ресурсы, как время и деньги, представляют ценность для правообладателя и являются объектами права собственности. Подобные объекты виртуального мира, особенно объекты онлайн игр (персонажи, «скины» и проч.), имеют стоимостную характеристику и часто являются предметом сделок между участниками (игроками) виртуального пространства.

Полагаем, что такие «виртуальные вещи» могут быть предметом, как хищений, так и вымогательства. Хищение таких предметов может совершаться путем кражи и (или) мошенничества, которые должны квалифицироваться по совокупности с ч. 2 ст. 272 УК РФ или ч. 2 ст. 273 УК РФ, при наличии признаков состава преступления. Итоговая квалификация по форме хищения будет зависеть от способа совершения преступления.

Один из способов преступления, используемый для совершения хищений — это использование служебного положения с целью модификации информации, а также получение неправомерного доступа к иной компьютерной информации. Такой способ модификации информации является незаконным и образует состав самостоятельного преступления, предусмотренного ст. 272 УК РФ (неправомерный доступ к компьютерной информации).

В случае, если модификация происходила в целях последующего совершения хищения или иного преступления против собственности, такие действия надлежит квалифицировать по совокупности по статьям, предусматривающим ответственности за преступление против собственности и по ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности).

Судебная практика по вопросу квалификации преступлений в случае совершения мошенничестве в сфере компьютерной информации (ст. 159.6. УК РФ) путем модификации информации или получения неправомерного доступа к компьютерной информации, изученная в пределах последних 5 лет, далека от единообразия. В одних случаях суды квалифицируют содеянное по

совокупности ст. 159.6. УК РФ (мошенничество в сфере компьютерной информации) и ч. 2 ст. 272 УК РФ[1], в других случаях — только по соответствующей части ст. 159.6. УК РФ[2].

Согласно позиции Верховного Суда Российской Федерации, выраженной в п. 20 Постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.

Полагаем, что подобную логику суды могут использовать и при квалификации действий виновных, связанных с намеренной модификацией компьютерной информации, путем внесения изменения в компьютерную информацию с целью хищения. Такой подход способен обеспечить единообразие практики применения норм о хищениях, совершаемых с использованием информационно-телекоммуникационных сетей.

Относительно новым способом хищения криптовалюты выступает мошенничество, совершенное путем злоупотребления доверием лиц, предоставляющих оборудование для «майнинга» и заключающих договоры оказания технологических услуг.

Фактически у виновного лица (исполнителя по договору) нет намерения исполнять договорные обязательства, более того, исполнитель может частично оказать услуги по технологическому присоединению, и перечислить часть криптовалюты на криптокошелек заказчика.

Далее, криптовалюта, полученная в результате майнинга на оборудовании заказчика (потерпевшего), поступает уже не в собственность заказчика,

[1] Приговор Центрального районного суда г. Тольятти от 14 мая 2020 г. по делу № 1-262/2020, Приговор Октябрьского городского суда Республики Башкортостан от 29 июля 2020 г. по делу № 1-243/2020. (Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 24.11.2023.)

[2] Приговор Советского районного суда г. Владивостока от 30 июля 2020 г. по делу № 1-277/2020 // Там же.

а на иные криптокошельки, а самого заказчика вводят в заблуждение относительно неисправности или утраты оборудования.

В некоторых случаях оборудование также становится предметом хищения. Такие противоправные действия следует квалифицировать как мошенничество по ст. 159.6. УК РФ и ч. 2 ст. 272 УК РФ, если вносятся изменения в компьютерную информацию, в результате чего меняется «путь» от оборудования, производящего криптовалюты на соответствующий криптокошелек, и как мошенничество по ст. 159 УК РФ, если согласно договоренности с заказчиком вся криптовалюта поступает на общий криптокошелек, и затем исполнитель перечисляет ее на криптокошелек заказчика индивидуально.

УДК 343

М. Б. КОСТРОВА

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»), В РОССИЙСКОМ УГОЛОВНОМ ПРАВЕ: ЯЗЫКОВОЙ АСПЕКТ

Закономерной реакцией российского государства на расширение масштабов преступной деятельности с использованием информационных ресурсов, доступ к которым имеет неограниченный круг лиц, стало столь же масштабное включение в разные составы преступлений признака «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)» в его различных вариациях.

Однако даже при беглом обзоре таких составов преступлений, содержащихся в настоящее время в УК РФ, обнаруживается несистемный подход законодателя к использованию языковых средств при формулировании данного признака и его вариаций.

Так, одной из его лексико-грамматических вариаций является введение в присоединительный оборот взамен скобочного уточнения «(включая сеть «Интернет»)» союза «в том числе».

При этом второй вариант является почти таким же распространенным (встречается 18 раз), как и первый (встречается 22 раза). Оба лексико-грамматических варианта — «(включая сеть «Интернет»)» и «в том числе сеть «Интернет» — семантически не различаются, они означают принадлежность сети «Интернет» к информационно-телекоммуникационным сетям.

Есть еще и третий вариант, тоже семантически тождественный, он встречается только трижды (в ч. ст. 128.1, в ч. 1 и ч. 2 ст. 282 УК РФ) — «включая сеть «Интернет», то есть без скобочного уточнения. На точность и ясность языкового выражения уголовно-правовых предписаний такая вариативность не влияет, но возникает большое сомнение в ее необходимости и целесообразности.

Язык уголовного закона, будучи функциональной разновидностью официально-документального стиля, в отличие от других функциональных стилей русского языка – художественной литературы, публицистики, разговорной речи, в принципе не требует подобного синонимического «украшательства», придающего речи выразительность и позволяющего избегать ее однообразия.

Если сеть «Интернет» является одним из видов информационно-телекоммуникационных сетей, о чем сейчас знают почти все люди, и что подтвердил Пленум Верховного Суда Российской Федерации в п. 17 Постановления от 15 декабря 2022 г. № 37[1], законодателю, возможно, следует задуматься вообще об отказе от ее выделения и обособления.

Перейдем к обсуждению второго недостатка языкового выражения признака «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)». При этом для сокращения объема текста статьи варианты «в том числе сеть «Интернет», «включая сеть «Интернет» как правило, упоминаться не будут.

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

Этот второй недостаток обусловлен, как видится, отсутствием должного внимания законодателя к номинации, то есть к процессу наименования, при котором языковые элементы соотносятся с обозначаемыми ими объектами. В результате в УК РФ встречаются три основные языковые формы, образованные за счет разницы в количестве и комбинациях, включенных в формулировку соответствующего признака состава преступления языковых элементов — словосочетаний «средства массовой информации», «электронные сети», «информационно-телекоммуникационные сети (включая сеть «Интернет»)».

Первая языковая форма — полная: «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)».

В УК РФ она содержится в шесть составах преступлений, два из которых являются основными и четыре — квалифицированными. В их числе: незаконные приобретение или продажа особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации, их частей и дериватов (производных) (ч. 1.1 ст. 258.1); незаконные приобретение или продажа особо ценных растений и грибов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации, их продуктов, частей и дериватов (производных) (ч. 2 ст. 260.1); публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ч. 2 ст. 205.2); сбыт наркотических средств, психотропных веществ или их аналогов (в п. «б» ч. 2 ст. 228.1); публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ч. 2 ст. 280.1); публичные призывы к осуществлению деятельности, направленной против безопасности государства (п. «в» ч. 2 ст. 280.4). Подчеркну, что кроме указанных статей словосочетание «электронные сети» в формулировках рассматриваемого признака в УК больше не обнаруживается.

Вторая языковая форма: «с использованием средств массовой информации либо информационно-телекоммуникационных сетей (включая сеть «Интернет»)», то есть без упоминания электронных сетей (как вариант в ней употребляется разделительный союз «или»).

Она встречается наиболее часто, а именно в 10 составах преступлений, из которых один является основным, а девять — квалифицированными или особо квалифицированными. В эту группу входят составы: возбуждения ненависти либо вражды, а равно унижения человеческого достоинства (ч. 1 и ч. 2 ст. 282); организации деятельности, направленной на побуждение к совершению самоубийства (ч. 2. ст. 110.2); понуждения к действиям сексуального характера (п. «б» ч. 3 ст. 133); обращения фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборота фальсифицированных биологически активных добавок (ч. 1.1 ст. 238.1); незаконных изготовления и оборота порнографических материалов или предметов (п. «б» ч. 3 ст. 242); изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних (п. «г» ч. 2 ст. 242.1); публичных призывов к осуществлению экстремистской деятельности (ч. 2 ст. 280); реабилитация нацизма (ч. 2 и ч. 4 ст. 354.1).

И еще в девяти составах преступлений (один — основной, остальные — квалифицированные) рассматриваемый признак обозначен в усеченной на треть языковой форме: «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)»[1].

К этой группе относятся такие составы как: незаконные организация и проведение азартных игр (ч. 1 ст. 171.2); клевета (ч. 2 ст. 128.1); незаконные приобретение, передача, хранение, перевозка, пересылка или ношение огнестрельного оружия, его основных частей и боеприпасов к нему (п. »в» ч. 3

[1] В этой группе преимущественно употребляется вариант «в том числе сети “Интернет”» по причине того, очевидно, что входящие в нее статьи 222, 222.1, 222.2 УК РФ, содержащие шесть из девяти рассматриваемых признаков, создавались (статья 222.2) и корректировались (статьи 222, 222.1) одним коллективом авторов-разработчиков Федерального закона от 1 июля 2021 г. № 281-ФЗ.

ст. 222); незаконный сбыт огнестрельного оружия, его основных частей, боеприпасов к нему (п. «в» ч. 5 ст. 222); незаконные приобретение, передача, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств (п. «в» ч. 3 ст. 222.1); незаконный сбыт взрывчатых веществ или взрывных устройств п. «в» ч. 5 ст. 222.1); незаконные приобретение, передача, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему п. «в» ч. 3 ст. 222.2); незаконный сбыт крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему (п. «в» ч. 5 ст. 222.2); склонение к потреблению наркотических средств, психотропных веществ или их аналогов (п. «д» ч. 2 ст. 230).

Во всех вышеперечисленных составах преступлений рассматриваемый признак, в какой бы из трех его языковых форм он не был представлен, выступает в качестве способа совершения преступления в силу включения в их формулировки термина «с использованием»[1].

Такой законодательный прием объединяет данные составы преступлений. Но, вместе с тем, как видим, они существенно различаются по количеству включенных языковых элементов – словосочетаний «средства массовой информации», «электронные сети», «информационно-телекоммуникационные сети (включая сеть «Интернет»)». В связи с этим встает вопрос об обоснованности неунифицированного подхода законодателя к языковым конструктам.

[1] Именно поэтому выше по тексту не упомянута часть 1 статьи 185.3 «Манипулирование рынком», текст которой не включает термин «с использованием»; соответственно, распространение заведомо ложных сведений через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»), в данном составе и есть манипулирование рынком, т. е. одно из общественно опасных действий, а не способ совершения преступления. Также в связи с заявленной темой настоящей статьи в ней не рассматриваются составы преступлений, при формулировании которых словосочетания «средства массовой информации» и «информационно-телекоммуникационные сети (включая сеть “Интернет”)» употребляются в уголовно-правовом значении места совершения преступления (хотя и своеобразного) за счет простановки перед ними предлога *в* (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, чч. 1 и 3 ст. 137, п. «г» ч. 2 ст. 245, п. «б» ч. 2 ст. 258.1, п. «б» ч. 3 ст. 260.1 УК РФ).

Решая этот вопрос, следует, очевидно, исходить из единой логико-языковой феноменологии законодательного текста, учитывая, что слово или словосочетание (компонент языка), обозначает понятие (форма мышления и, соответственно, компонент логики), которое, в свою очередь, отражает предметы и явления действительности в их существенных признаках.

Повторю уже написанное мной ранее: «Очевидное присутствие в тексте логического компонента, наряду с языковым, объясняется онтологическим статусом языка и мышления в общей картине мира и их соотношением… мышление и язык находятся в неразрывном органическом единстве, мышление не существует без языка, а язык не может существовать без мысли.

Он является способом существования мысли, ее материализацией, то есть формой выражения мысли. Природа мышления как обобщенного и опосредованного отражения действительности, а также природа языка как формы выражения мышления, важнейшего средства общения, обмена мыслями между людьми, не могут быть поняты, если мышление и язык рассматривать изолированно, в отрыве друг от друга»[1].

Базируясь на этой методологической основе объяснить «языковую чехарду» в российском УК в рассматриваемой части невозможно.

По мысли законодателя, выраженной в языковой форме, получается следующее. При совпадающей «физической» (не уголовно-правовой) сущности криминальных явлений одни из них могут совершаться с использованием всех трех информационных ресурсов — «средств массовой информации», «электронных сетей» «информационно-телекоммуникационных сетей (включая сеть «Интернет»)», другие – двух из них (первого и третьего), а третьи — только одного (третьего). Абсурдность такого допущения можно проиллюстрировать на ряде примеров.

Так, любой из трех информационных ресурсов может использоваться при публичных призывах к осуществлению террористической деятельности,

[1] Кострова М. Б. Теоретическая модель языковой формы нового Уголовного кодекса России. Часть 1. Теоретические подходы к пониманию онтологического статуса языка уголовного закона //R. 2015. № 12 (Том CIX). С. 99.

(ч. 2 ст. 205.2), к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ч. 2 ст. 280.1) и к осуществлению деятельности, направленной против безопасности государства (п. «в» ч. 2 ст. 280.4).

В то же время для публичных призывов к осуществлению экстремистской деятельности (ч. 2 ст. 280) использование электронных сетей не характерно, преступникам достаточно только средств массовой информации и информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Сбыт наркотических средств, психотропных веществ или их аналогов (в п. «б» ч. 2 ст. 228.1) может осуществляться с использованием любого из трех информационных ресурсов. Но незаконные сбыт огнестрельного оружия, в том числе крупнокалиберного, их основных частей и боеприпасов к ним (п. «в» ч. 5 ст. 222, п. «в» ч. 5 ст. 222.2), взрывчатых веществ или взрывных устройств (п. в» ч. 5 ст. 222.1) совершаются исключительно и только с использованием одного ресурса — информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Использование же при совершении этих преступлений средств массовой информации и электронных сетей не происходит. Наряду с этим, незаконные приобретение, передача, хранение, перевозка, пересылка или ношение[1] огнестрельного оружия, в том числе крупнокалиберного, их основных частей и боеприпасов к ним, взрывчатых веществ или взрывных устройств, становятся более общественно опасными, если они совершены с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (пункты «в» частей 3 ст. 222, 222.1, 222.2).

Однако аналогичные действия, криминализированные в ст. 228, а именно незаконные приобретение, хранение, перевозка наркотических

[1] Привожу дословно из указанных статей УК РФ, хотя трудно представить в реальности как минимум ношение данных предметов с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Сделано это намеренно, с целью высветить еще один недостаток законодательной деятельности в рассматриваемой сфере: формулируя квалифицирующий признак с использованием обобщенного понятия «то же деяние», законодатель не обращает внимание на его связь или отсутствие таковой с действиями, обозначенными в основном составе.

средств, психотропных веществ или их аналогов, растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» не совершаются, в связи с чем дифференциация уголовной ответственности и наказания не требуется.

Перечень подобных абсурдных примеров может быть продолжен, но в рамках настоящей публикации в этом нет нужды. Об отсутствии единого понятийного аппарата, системного подхода к использованию терминологии, о непоследовательном, никакой логикой необъяснимом избирательном подходе законодателя к включению рассматриваемого признака в целом и его вариантов в разные составы преступлений уже много написано в уголовно-правовой литературе[1].

Единственное, что абсолютно правильно сделано законодателем, — это отказ от включения словосочетания «электронные сети» в подавляющее большинство из вышеперечисленных составов преступлений. Оно в принципе не имеет права на существование в УК, так как создает видимость зависимости содержания уголовно-правового предписания от нормативных правовых предписаний информационного права при фактическом отсутствии такой зависимости.

Посредством включения в составы преступлений признака «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)» и его вариаций законодатель конструирует бланкетное уголовно-правовое предписание. И в нем, по логике межотраслевого согласования, должны употребляться

[1] Литвяк Л. Г., Пирогова Е. Н. К вопросу о понятии электронных или информационно-телекоммуникационных сетей для целей уголовного закона // Гуманитарные, социально-экономические и общественные науки. 2020. № 11, ч. 2. С. 93—96 ; Сабитов Т. Р. Об использовании терминов «средства массовой информации» и «Интернет» при формулировании признаков составов преступлений // Российское право: образование, практика, наука. 2020. № 6. С. 41—48.

только бланкетные термины — заимствованные словосочетания, обозначающие специальные понятия информационного права.

Два таких словосочетания, действительно, являются бланкетными терминами, причем имеющими легальные дефиниции. Так, Законом Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» (ст. 2) определено: «под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)».

В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в п. 4 ст. 2 понятие «информационно-телекоммуникационная сеть» определяется как «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники». Однако ни в одном нормативном правовом акте России словосочетание «электронные сети» не дефинируется, более того, именно в такой языковой форме оно не встречается.

Не случайно Пленум Верховного Суда Российской Федерации в Постановлении от 15 декабря 2022 г. № 37 воспроизведя в п. 17 данное в Федеральном законе от 27 июля 2006 г. № 149-ФЗ определение понятия «информационно-телекоммуникационная сеть», далее разъяснил: «Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются».

Выводы, которые следуют из всего вышеизложенного, такие.

Во-первых, необходимо исключить словосочетание «электронные сети» из всего УК РФ.

Во-вторых, целесообразно отказаться от упоминания во всех вышеперечисленных статьях УК сети «Интернет» в любых языковых вариантах.

В-третьих, во всех вышеперечисленных составах преступлений, а также во вновь включаемых в УК, следует использовать терминологию «с использованием средств массовой информации или информационно-телекоммуникационных сетей». Но последнее утверждение некатегорично, поскольку внедрять данную рекомендацию нужно осторожно, рассчитывая, с учетом механизма совершения конкретного преступления, как его в целом описал законодатель, может ли конкретное преступление быть совершено с использованием средств массовой информации.

УДК 343

Р. М. КРАВЧЕНКО

ВОПРОСЫ КВАЛИФИКАЦИИ ОБОРОТА ПОДДЕЛЬНЫХ ЭЛЕКТРОННЫХ ОФИЦИАЛЬНЫХ ДОКУМЕНТОВ

Элементы цифровой трансформации стали неотъемлемой частью жизни каждого члена общества. Покупка товаров, заказ услуг, оформление документов, получение образования, подача обращений в государственные органы могут быть осуществлены в электронной форме. Преступность как социальное явление также не отстает от такого общественного процесса как цифровизация.

Понятие электронного документа не является новеллой для отечественного законодателя. Так, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понимает электронный документ как документированную информацию, представленную в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» определяет электронный документ как информацию в электронной форме, подписанную квалифицированной электронной подписью.

Признавая юридическую силу и самостоятельность электронных документов, Трудовой кодекс Российской Федерации определяет электронный документооборот в сфере трудовых отношений как создание, подписание, использование и хранение работодателем, работником или лицом, поступающим на работу, документов, связанных с работой, оформленных в электронном виде без дублирования на бумажном носителе (электронные документы).

Пленум Верховного Суда Российской Федерации, в свою очередь, разъясняя наиболее важные вопросы квалификации преступлений в сфере документооборота, включил в понятие официального документа указание на возможность его изготовления в электронной форме[1].

Однако одно лишь признание электронных документов предметом преступления не решает всех квалификационных вопросов, так как цифровая форма создания и использования таких документов отражается на объективной стороне общественно опасных деяний.

Пленумом Верховного Суда Российской Федерации в п. 8 Постановления № 43 определены признаки подделки официального документа:

1) незаконное изменение отдельных частей подлинного официального документа путем подчистки, дописки, замены элементов и др., искажающее его действительное содержание;

2) изготовление нового официального документа, содержащего заведомо ложные сведения, в том числе с использованием подлинных бланка, печати, штампа.

Для привлечения лица к уголовной ответственности обязательным условием является установление факта подделки электронного официального документа. В связи с тем, что именно документ признается законом и Верховным Судом Российской Федерации предметом преступлений, предусмотренных

[1] О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324—327.1 Уголовного кодекса Российской Федерации : Постановление Пленума Верховного Суда Российской Федерации от 17 декабря 2020 г. № 43. П. 1. Доступ из справ.-правовой системы «КонсультантПлюс».

ст.ст. 324, 325, 327 УК РФ, можно сделать вывод, что подделка, хищение и использование поддельной копии официального документа не может быть квалифицировано по данным статьям.

Подобные ситуации связаны с использованием доверия либо необязательностью лица, которому предъявляются не оригиналы документа, а их копии. Правила делопроизводства требует от уполномоченных лиц учитывать либо оригиналы документов, либо заверенные в установленном порядке копии, либо принимать копии документов лишь после их сверки с оригиналами. Использование поддельных незаверенных копий документов не причиняет вреда общественным отношениям в сфере официального документооборота, так как не происходит воздействия на главное звено этих отношений – документ. Получение лицом прав или освобождение от обязанности происходит не в связи с его посягательством на порядок управления, а в связи с ненадлежащим отношением уполномоченного лица к инструкции о делопроизводстве и непрепятствием с его стороны попытке использования грубой подделки.

Таким образом, не может быть квалифицированы по ст. 327 УК РФ подделка и использование поддельных электронных копий официальных документов, если в оригиналы таких документов не взносились никакие ложные изменения либо если не создавалась заведомо ложная электронная копия официального документа.

Следуя данной логике, стоит согласиться с авторами, исключающими из числа предметов подделки официальных документов QR-коды, так как это всего лишь штрих-код, позволяющий быстро считать закодированную информацию, либо закодированная ссылка для быстрого перехода к электронному документу[1].

В случаях же, когда электронный документ не требует дополнительного заверения и может быть предъявлен самостоятельно (без сверки с бумажным

[1] Стяжкина А. А. Электронный документ как предмет уголовно-правовой охраны // Вестник Удмуртского университета. 2022. Т. 32, вып. 1. С. 181.

носителем), использование электронного файла, в который были внесены изменения, могут быть квалифицированы по ч. 3-5 ст. 327 УК РФ (в зависимости от статуса документа, который используется виновным).

Так, Правилами оказания услуг по перевозкам на железнодорожном транспорте пассажиров, а также грузов, багажа и грузобагажа для личных, семейных, домашних и иных нужд, не связанных с осуществлением предпринимательской деятельности, утвержденными Постановлением Правительства Российской Федерации от 27.05.2021 № 810, установлено, что гражданином может быть предъявлен электронный билет. Такой документ подтверждает факт договорных отношений между пассажиром и перевозчиком и предоставляет гражданину право воспользоваться транспортной услугой без предъявления проездного документа на бумаге. Видится, что ввиду самостоятельности такого электронного документа и нормативной включенности его документооборот, предъявление такого поддельного билета может быть квалифицировано по ч. 5 ст. 327 УК РФ[1].

Указом Президента Российской Федерации от 18.09.2023 г. № 695 представление гражданами сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации, либо иных документах, выданных гражданам государственными органами, в электронной форме с использованием мобильного приложения федеральной государственной информационной системы «Единый портал государственных и муниципальных

[1] Этими же Правилами определено, что для идентификации и аутентификации пассажира используются федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», что поможет легко выявить факт подделки проездного документа. Однако в силу разъяснений Верховного Суда Российской Федерации использование заведомо поддельного (подложного) документа, указанного в частях 3 и 5 ст. 327 УК РФ, квалифицируется как оконченное преступление с момента его представления с целью получения прав или освобождения от обязанностей независимо от достижения данной цели. (О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324—327.1 Уголовного кодекса Российской Федерации : Постановление Пленума Верховного Суда Российской Федерации от 17 декабря 2020 г. № 43. П. 11. Доступ из справ.-правовой системы «КонсультантПлюс».)

услуг (функций)» в определенных случаях приравнено к предъявлению указанных документов. Таким образом, паспорт гражданина РФ получил официально признанную электронную копию. Однако подделка электронного паспорта в силу природы электронного документа возможна лишь путем внесения ложных сведений в базу данных портала Госуслуг, следовательно, такое деяние немыслимо без совершения преступлений, предусмотренных ст.ст. 272 и (или) 273 УК РФ.

Преступник, внося изменения в компьютерную информацию, являющуюся официальным документом, посягает на два объекта преступления и, соответственно, на два предмета. В данном случае информация имеет две составляющие – это форма ее представления и содержание. По форме она будет являться компьютерной, так как представлена в виде электрических сигналов, а по содержанию – она будет являться официальным документом[1]. Видится, что данная позиция будет верной и в случаях незаконного приобретения электронного официального документа путем его неправомерного копирования[2].

В то же время, уничтожение электронного документа, который является хоть и самостоятельным, но, дубликатом, потерпевший не лишается возможности пользоваться теми правами и свободами, который продолжает или порождает удостоверять официальный документ на бумажном носителе. Подобные деяния видится правильным квалифицировать лишь по статьям 272 и (или) 273 УК РФ, так как вреда отношениям в сфере документооборота не причиняется.

Подделка же электронных документов, не дублирующих бумажные аналоги, в принципе невозможна без противоправного воздействия на компьютерную информацию. Если электронный официальный документ представлен только в форме электрических сигналов, то в лучшем случае преступник может приобрести или сбыть материальный носитель данной информации, либо электронную версию документа[3].

---

[1] Стяжкина А. А. Указ. соч. С. 182.

[2] Сабитова Е. Ю. Как квалифицировать подделку, изготовление и сбыт компьютерных (электронных) документов // Вестник Челябинского государственного университета. 2002. № 1 (3). С. 141.

[3] Стяжкина А. А. Указ. соч. С. 181.

Так, Ч. осуждена за совершение преступлений, предусмотренных ч. 4 ст. 159, ч. 1 ст. 187, ч. 1 ст. 159 УК РФ, при следующих обстоятельствах.

Осуществляя свою трудовую деятельность в должности бухгалтера, Ч. пользовалась доверием руководства организации, в связи с чем, при осуществлении своих трудовых обязанностей для изготовления электронных платежных поручений, использовала переданные ей руководством логины и пароли для дистанционной работы с кредитными учреждениями, в частности в системе «Альфа-клиент онлайн».

Ч. решила систематически совершать неправомерное перечисление денежных средств по фиктивным основаниям с расчетного счета организациям в свою пользу. При этом Ч. получала от неосведомленного о ее преступных намерениях руководства пароль, посредством ввода которого в программе заверяла изготовленные ею поддельные платежные поручения криптоподписью, оформленной на имя директора, направляя таким образом неправомерные распоряжения о переводе денежных средств с расчетного счета организации[1].

В приведенной ситуации виновная осуществляла интеллектуальную подделку платежных документов, являющихся основанием для осуществления расчетов, в целях совершения хищения. Однако видится необходимой дополнительная квалификация ее деяния по ст. 272 УК РФ.

По мнению Пленума Верховного Суда Российской Федерации, изложенной в п. 5 Постановления № 37 от 15.12.2022 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» под неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка

[1] Приговор Пролетарского районного суда г. Твери от 15 января 2020 г. по делу № 1-1/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru/regular/doc/FPIJYwDERp6j/ (дата обращения: 17.10.2023).

независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

Несмотря на предоставление Ч. фактического доступа к программному обеспечению предприятия, она использовала его как возможность совершения преступления, что, как видится, исключает правомерность доступа к компьютерной информации.

УДК 343

Д. Ю. КРАЕВ

КВАЛИФИКАЦИЯ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ, НАПРАВЛЕННОЙ НА ПОБУЖДЕНИЕ К СОВЕРШЕНИЮ САМОУБИЙСТВА, СОПРЯЖЕННОЕ С ПУБЛИЧНЫМ ВЫСТУПЛЕНИЕМ, ИСПОЛЬЗОВАНИЕМ ПУБЛИЧНО ДЕМОНСТРИРУЮЩЕГОСЯ ПРОИЗВЕДЕНИЯ, СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ») (ч. 2 ст. 110.2 УК РФ)

Статья 110.2 — новелла уголовного законодательства: она введена в УК РФ Федеральным законом от 7 июня 2017 г. № 120-ФЗ и устанавливает ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства.

Как отмечают разработчики статьи 110.2 УК РФ, «в частности, речь идет об ответственности для администраторов так называемых «групп смерти» и организаторов любых неформальных сообществ, деятельность которых сопряжена с побуждением, прежде всего детей, к совершению самоубийства…

Своевременное пресечение преступной деятельности организаторов имеет причинно-следственную связь с возможностью упреждения и недопущения гибели несовершеннолетних, которые находятся под влиянием преступного воздействия организаторов.

В этой связи в целях превентивного реагирования законопроектом предлагается установить дополнительную уголовную ответственность в отношении организаторов такой опасной для граждан деятельности с возможностью их привлечения к ответственности, когда еще отсутствует конкретная жертва преступления, но имеются все признаки склонения лица к совершению самоубийства.

Например, созданы сайты с соответствующей суицидальной тематикой либо «игра», предполагающая вовлечение ребенка в суицидальную модель поведения... Анализ правоприменительной практики свидетельствует, что зачастую с детьми работают лица, знающие подростковую психологию.

Закрытый и ритуальный характер вступления в указанные сообщества, методично разработанный набор заданий (путь инициации) привлекает внимание детей и, в конечном счете, доводит ребенка до суицида или попытки совершения самоубийства. Предлагаемый законопроектом подход согласуется с международным и зарубежным опытом правового регулирования противодействия суицидам.

В частности, учитывался опыт ряда уголовных законодательств зарубежных государств в части криминализации содействия совершения суицида и пропаганды самоубийства[1]… Данный законопроект носит комплексный характер и подготовлен с учетом негативных общемировых тенденций, свидетельствующих о динамике роста суицидов среди несовершеннолетних, широком распространении в сети «Интернет» информации, побуждающей детей и подростков к совершению самоубийств или иной деструктивной деятельности, формировании ложных смыслов и популяризации преждевременной смерти…Защита детей от информации, побуждающей к суициду и опасному для жизни поведению, относится к одной из задач национальной безопасности»[2].

---

[1] Нормы о пропаганде самоубийства и публичном оправдании самоубийства содержатся, например, в уголовных кодексах Республики Беларусь (ст. 342-1) и Республики Молдовы (ст. 150-1).

[2] Пояснительная записка к проекту федерального закона № 118634-7 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов

Согласно ст. 5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»:

— к информации, запрещенной для распространения среди детей, относится информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

— к информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация, вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий.

В части 2 ст. 110.2 УК РФ установлена повышенная ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, сопряженную с публичным выступлением, использованием публично демонстрирующегося произведения, средств массовой информации или информационно-телекоммуникационных сетей (включая сеть «Интернет»)»[1].

Учитывая разъяснения, содержащиеся в пунктах 18-22 Постановления Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1

противодействия деятельности, направленной на побуждение детей к суицидальному поведению». (Доступ из справ.-правовой системы «КонсультантПлюс».)

[1] Приговор Пятигорского городского суда Ставропольского края от 30 августа 2021 г. № 1-611/2021, которым А. был осужден за совершение преступления, предусмотренного ч. 2 ст. 110.2 УК РФ и признан виновным в организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства, сопряженной с использованием информационно-телекоммуникационной сети «Интернет». (Пятигорский городской суд Ставропольского края : офиц. сайт. URL: https://piatigorsky.stv.sudrf.ru (дата обращения: 19.10.2023).)

«О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» и в пунктах 4-6.1 Постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности», можно сделать вывод о том, что:

1) вопрос о публичности выступления, использовании публично демонстрирующегося произведения при совершении преступления, предусмотренного ч. 2 ст. 110.2 УК РФ, должен разрешаться с учетом места, способа, обстановки и других обстоятельств дела (например, обращения к группе людей в общественных местах, на собраниях, распространение листовок, вывешивание плакатов, распространение обращений путем массовой рассылки сообщений абонентам мобильной связи и т.п.);

2) организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, сопряженную:

— с использованием сайтов в информационно-телекоммуникационных сетях (включая сеть «Интернет»), зарегистрированных в качестве средства массовой информации в установленном порядке, следует квалифицировать по ч. 2 ст. 110.2 УК РФ по признаку «сопряженная с использованием средств массовой информации»;

— с использованием же сайтов в информационно-телекоммуникационных сетях (включая сеть «Интернет»), не зарегистрированных в качестве средства массовой информации в установленном порядке - по ч. 2 ст. 110.2 УК РФ по признаку «сопряженная с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)»[1];

[1] Приговор Вуктыльского городского суда Республики Коми от 27 января 2021 г. по делу № 1-1/2021, которым Е. была осуждена за совершение преступления, предусмотренного ч. 2 ст. 110.2 УК РФ, за организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства, сопряженную с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). (Вуктыльский городской суд Республики Коми : офиц. сайт. URL: https://vuktyl--komi.sudrf.ru (дата обращения: 15.10.2023).)

3) при квалификации организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, по ч. 2 ст. 110.2 УК РФ как сопряженной с использованием средств массовой информации (газет, журналов и т. д.) или информационно-телекоммуникационных сетей, включая сеть «Интернет» (например, сайтов, форумов, блогов), следует учитывать, в частности, положения Закона Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» и Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В соответствии со ст. 2 Закона Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», под средством массовой информации понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием).

Согласно Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

— информационно-телекоммуникационная сеть – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (ст. 2);

— владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распростра-

няться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более пятисот тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, обязан соблюдать требования законодательства Российской Федерации, в частности, осуществлять мониторинг социальной сети в целях выявления информации о способах совершения самоубийства, а также призывов к совершению самоубийства (ст. 10.6).

В соответствии с разъяснениями постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»:

1) указанная в ч. 2 ст. 110.2 УК РФ сеть «Интернет» является одним из видов информационно-телекоммуникационных сетей (п. 17);

2) для признания наличия в содеянном признака сопряженности организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, с использованием информационно-телекоммуникационных сетей (ч. 2 ст. 110.2 УК РФ) не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики (таковыми могут признаваться, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между компьютерными устройствами) (п. 17);

3) при квалификации организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, по ч. 2 ст. 110.2 УК РФ как сопряженной с использованием сети «Интернет», следует иметь в виду, что под сайтом в сети «Интернет» понимается совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты; страница сайта в сети «Интернет» — это часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет» (п. 18);

4) организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, квалифицируется по ч. 2 ст. 110.2 УК РФ как сопряженная с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), независимо от стадии совершения данного преступления, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения указанного преступления или входящих в его объективную сторону, виновный использовал такие сети (например, если лицо, используя сеть «Интернет» подыскивало соучастников организации деятельности, направленной на побуждение к совершению самоубийства, размещало информацию о способах совершения самоубийства или призывы к совершению самоубийства). По указанному признаку ч. 2 ст. 110.2 УК РФ квалифицируется и совершенная в соучастии организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, если связь между соучастниками в ходе подготовки и совершения данного преступления обеспечивалась

с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» (п. 20);

5) доступ к информационно-телекоммуникационным сетям, в том числе сети «Интернет», может осуществляться с различных компьютерных устройств, технологически предназначенных для этого, с использованием программ, имеющих разнообразные функции (браузеров, программ, предназначенных для обмена сообщениями, - мессенджеров, специальных приложений социальных сетей, онлайн-игр, других программ и приложений). При квалификации организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, по ч. 2 ст. 110.2 УК РФ как сопряженной с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), необходимо установить:

— какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью (п. 21);

— осуществляло ли лицо такие деяния умышленно, осознавало ли содержание и общественную опасность соответствующих действий, включая характер распространяемой информации о способах совершения самоубийства или призывов к совершению самоубийства;

— а также другие обстоятельства, имеющие значение для юридической оценки содеянного (п. 23).

Так, приговором суда Есипова была признана виновной в совершении преступления, предусмотренного ч. 2 ст. 110.2 УК РФ и выразившегося, по оценке суда, в организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к его совершению, сопряженной с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет».

Как установил суд, виновная разместила указанную информацию в социальной сети в созданной и администрируемой ею группе, в которой состояло

несколько тысяч пользователей. Кассационный суд общей юрисдикции согласился с выводом приговора о том, что Есипова осуществляла непосредственное руководство группой в социальной сети, поддерживала ее функционирование, популяризируя информацию суицидальной направленности, доступную к получению неопределенным кругом лиц[1].

Единичное преступление, предусмотренное ч. 2 ст. 110.2 УК РФ, необходимо отграничивать от совокупности данных преступлений, что нередко вызывает затруднения у правоприменителя[2].

Так, приговором Люберецкого городского суда Московской области от 6 марта 2019 г. Г. был осужден по ч. 2 ст. 110.2 УК РФ и признан виновным в организации деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства, сопряженной с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

У находящегося в неустановленном месте на территории Московской области Г. возник преступный умысел на доведение до самоубийства неопределенного круга лиц путем вовлечения пользователей общедоступной сети «ВКонтакте» в коммуникацию с ним и последующего побуждения их в ходе диалога к выполнению ими ряда заданий, необходимых для подготовки их к совершению самоубийства.

Будучи пользователем общедоступной социальной сети «ВКонтакте», Г., достоверно зная о повышенном интересе значительной части пользователей

---

[1] Об отказе в принятии к рассмотрению жалобы гражданки Есиповой Полины Дмитриевны на нарушение ее конституционных прав положениями статьи 110.2 Уголовного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 30 мая 2023 г. № 1104-О. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Например, приговором Абаканского городского суда Республики Хакасия от 31 мая 2021 г. по делу № 1-346/2021 А. был осужден за совершение преступления, предусмотренного ч. 2 ст. 110.2 и ч. 2 ст. 110.2 УК РФ, за то, что дважды организовал деятельность, направленную на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства и призывов к совершению самоубийства, сопряженную с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), однако Верховным судом Республики Хакасия данный приговор был изменен, а действия А. квалифицированы как одно преступление, предусмотренное ч. 2 ст. 110.2 УК РФ. (Апелляционное определение Верховного суда Республики Хакасия от 28 июля 2021 г. по делу № 22-1046/2021. Доступ из справ.-правовой системы «КонсультантПлюс».)

указанной социальной сети к темам самоубийства, депрессии и иного деструктивного контента (информации), используя свой мобильный телефон, имеющий доступ к сети «Интернет», а также имевшиеся в его распоряжении персональные электронные страницы «Г.», «А. Глазик», «Аннубис Кит», «К.», систематически размещал на указанных страницах общедоступную информацию суицидального характера, в том числе с использованием гиперссылок, объединяющих публичные сообщения определенной тематики, размещенные в информационно-телекоммуникационной сети «Интернет» (хештег), тем самым завлекал на свои страницы лиц, имеющих намерения совершить суицид, с целью дальнейшего склонения данных лиц к совершению самоубийства.

Реализуя свой преступный умысел, Г. организовал деятельность, направленную на побуждение к совершению самоубийства и распространение информации о способах совершения самоубийства, выражавшуюся в упорядочении и оптимизации процессов ежедневного обмена текстовыми сообщениями, изображениями, аудио, видео файлами в созданной им конференц-беседе под названием «На грани жизни» в социальной сети «ВКонтакте» с использованием своего мобильного телефона, вступил в электронную переписку посредством информационно-телекоммуникационной сети «Интернет» с Б.Е.А., Н.А.Д., Б.А.В., Ф.М.А., К.Е.А.

В ходе переписки с указанными лицами Г. разъяснял правила участия в данной беседе и давал различные задания, в том числе причинять себе членовредительство, подниматься на крыши высотных зданий, стрелы строительных кранов и там себя фотографировать, перебежать железнодорожное полотно перед близко идущим поездом, давал обязательные для выполнения задания о необходимости просмотра и прослушивания аудио и видеоматериалов, содержащих откровенные сцены насилия и осуществления людьми самоубийства различными способами, формирующие у указанных лиц депрессивную направленность сознания, тем самым снимая у них психологический барьер, препятствующий совершению суицида выбранным ими способом.

В вышеуказанный период времени, Г. в ходе переписки с Б.А.В. выяснил у последней причины, по которым она намеревалась совершить самоубийство,

разъяснил правила участия в данной беседе, дал первое задание порезать лезвием руку и убедился в выполнении ею первого задания.

В созданной Г. конференц-беседе под названием «На грани жизни» в социальной сети «ВКонтакте» с участником данной беседы Б.А.В. он совершенствовал методы психологического воздействия, тем самым, желая наиболее эффективным способом достичь своей цели — самоубийства Б.А.В., осуществлял ежедневный контроль за полученной от участника беседы Б.А.В. информацией о возрасте, личности, увлечениях проблемах и жизненных трудностях, предполагаемом способе совершения самоубийства, учитывая индивидуально-психологические особенности потерпевшей предвидя возможность лишения ею себя жизни и желая наступления этих последствий, умышленно распространил информацию о способе самоубийства, в частности призывал Б.А.В. покончить жизнь самоубийством путем падения с высотного здания.

Обвиняемый Г. в социальной сети «ВКонтакте» путем систематического устойчивого целенаправленного психологического воздействия на Б.А.В. посредством сети «Интернет» неоднократно призывал Б.А.В. к совершению последовательных действий, при которых Б.А.В. должна совершать активные аутогрессивные действия: ежедневно резать различные части своего тела, проникать и фотографироваться в различных местах, опасных для жизни: сидеть на краю крыши высотного дома, забираться на строительный кран, находится вблизи движущихся поездов; совершать иные действия, имитирующие распространенные способы самоубийств. Г. вел с Б.А.В. переписку в ночные и ранние часы, то есть во время, предназначенное для отдыха и сна, что являлось дополнительной психотравмирующей нагрузкой для Б.А.В., давал обязательные для выполнения задания о необходимости просмотра и прослушивания аудио и видеоматериалов, содержащих откровенные сцены насилия и осуществления людьми самоубийства различными способами, формирующие у потерпевшей депрессивную направленность сознание, тем самым, снимая психологический барьер Б.А.В., препятствующий совершению суицида выбранным ею способом.

По мнению суда, действия подсудимого органами предварительного следствия были ошибочно квалифицированы как два преступления (первое в отношении неопределенного круга лиц и второе — в отношении Б.А.В.). Как видно из предъявленного обвинения, и установлено в судебном заседании, реализуя свой преступный умысел, подсудимый по обоим преступлениям для посещения общедоступной сети «ВКонтакте» каждый раз использовал один и тот же мобильный телефон, использовал одни и те же учетные записи «А. Глазик», «К.», «А. Кит», «Г.», разъяснение правил и публикацию заданий для всех участников, включая Б.А.В., осуществлял в созданной им беседе в общедоступной сети «ВКонтакте».

Г. пояснил суду, что стать участником созданной им «беседы» мог стать любой человек, ее посетивший; никого лично из участников созданной им беседы он лично не знал, относился ко всем одинаково, задания для всех участников были типовыми; какой-либо предвзятости, особого отношения, либо неприязни он ни к кому из участников беседы не испытывал, в том числе и к Б.А.В. Все это свидетельствует о едином умысле подсудимого и совершении преступления одним способом.

Суд считает, что органом предварительного расследования без достаточных оснований действия Г. квалифицированы несколькими эпизодами. Противозаконные действия Г. осуществлялись в одной обстановке, подсудимый не выделял участников из конференц-беседы, в данном случае налицо продолжаемое[1] преступление, все совершенные действия входят в один незаконный замысел и имеют одну конечную цель.

Суд квалифицировал действия Г. как одно преступление, предусмотренное ч. 2 ст. 110.2 УК РФ, как организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации

[1] О признаках продолжаемого преступления см.: Краев Д. Ю. Основные признаки продолжаемого преступления // Законность. 2021. № 4. С. 44—52.

о способах совершения самоубийства и призывов к совершению самоубийства, сопряженное с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)[1].

Как отмечает Конституционный Суд Российской Федерации, ст. 110.2 УК РФ согласуется с требованиями Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который, определяя особенности распространения информации в социальных сетях, предполагает недопустимость (запрет) распространения в сети «Интернет» информации[2] о способах совершения самоубийства, а также призывов к его совершению (подп. «в» п. 5 ч. 1 ст. 10.6 и подп. «в» п. 5 ч. 1 ст. 15.1).

Дополнительно Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» относит к информации, запрещенной для распространения среди детей, в частности информацию, побуждающую к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо направленную на склонение или иное вовлечение детей в совершение таких действий (п. 1 ч. 2 ст. 5).

---

[1] Приговор Люберецкого городского суда Московской области от 6 марта 2019 г. по делу № 1-74/2019 // Люберецкий городской суд Московской области : офиц. сайт. URL: https://luberetzy--mo.sudrf.ru (дата обращения: 25.09.2023).

[2] Об утверждении критериев оценки информации, необходимой для принятия Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено», в отношении информации о способах совершения самоубийства, а также призывов к совершению самоубийства : Приказ Роспотребнадзора от 27 февраля 2023 г. № 79. Доступ из справ.-правовой системы «КонсультантПлюс».

В отношении распространяемой посредством сети «Интернет» информации о способах совершения самоубийства, а также призывов к его совершению может приниматься решение уполномоченных федеральных органов исполнительной власти, служащее основанием для включения в единый реестр доменных имен и (или) указателей страниц сайтов в сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию (Постановление Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»).

Действуя с учетом ограничений, установленных для распространения отдельных видов информации, ст. 110.2 УК РФ направлена на охрану неопределенного круга лиц (в число которых могут входить и несовершеннолетние, отличающиеся — вследствие незавершенности формирования их личности - незрелостью и внушаемостью) от вредного (негативного) побуждающего воздействия на их психику, способного при неблагоприятном стечении обстоятельств подтолкнуть их к самоубийству или помочь им в этом.

Тем самым данная норма косвенно направлена и на защиту жизни человека как высшего блага и как особой конституционной ценности, что соответствует конституционным обязанностям государства в вопросах обеспечения прав и свобод граждан и принятия адекватных мер их охраны[1].

[1] Об отказе в принятии к рассмотрению жалобы гражданки Есиповой Полины Дмитриевны на нарушение ее конституционных прав положениями статьи 110.2 Уголовного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 30 мая 2023 г. № 1104-О. Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 343

А. В. КУРСАЕВ

НЕЗАКОННОЕ РАСПРОСТРАНЕНИЕ ПОРНОГРАФИЧЕСКИХ МАТЕРИАЛОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»

В настоящее время рынок сексуальных услуг активно информатизируется. Одним из проявлений данной тенденции является появление многочисленных интернет-сайтов и иных сервисов в информационно-телекоммуникационных сетях. Они позволяют удовлетворять свои половые потребности без непосредственного контакта с другим лицом.

Однако данная деятельность может являться и уголовно-наказуемой. В УК РФ существуют специальные нормы об ответственности за незаконное изготовление или оборот порнографических материалов или предметов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (п. «б» ч. 3 ст. 242 УК РФ), а также изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (п. «г» ч. 2 статьи 242.1 УК РФ).

В первоначальной редакции УК РФ подобные квалифицирующие признаки не содержал.

Полагаем, что закрепление данного способа распространения информации порнографического характера в качестве криминобразующего является вполне обоснованным и обусловлено тремя причинами.

Во-первых, данный способ позволяет довести порнографические материалы до массового потребителя, что значительно увеличивает оборот порнографических материалов. Это позволяет причинять ущерб не одному, а сразу нескольким потерпевшим.

Во-вторых, поскольку в информационно-телекоммуникационных сетях количество граждан, которые получают доступ к информации порнографического характера, определить сложно и невозможно обеспечить какие-либо ограничения по доступу к такой информации в зависимости от статуса граждан, потерпевшими могут выступать и дети, что еще более увеличивает общественную опасность содеянного. Обращение несовершеннолетних к подобного рода информации может отрицательно сказаться на их нравственном развитии.

В-третьих, он связан с фактической бесконтрольностью контента, который можно распространить в информационно-телекоммуникационных сетях. Информация эта не всегда полезна для пользователя, однако последний в силу того, что он в целях надлежащей социализации вынужден пользоваться такими сетями, в первую очередь Интернетом, может стать невольным потребителем порнографического материала. Особенно это актуально в случае, если пользователями Интернета выступают дети, которые в силу возраста не могут критически осмысливать содержание интернет-страниц.

Анализ судебной практики показывает, что к информационно-телекоммуникационным сетям для целей статей 242 и 242.1 УК РФ помимо сети «Интернет»[1] относятся социальные сети «ВКонтакте»[2] и «Одноклассники»[3], мессенджер «WhatsApp»[4], интернет-мессенджер «Telegram»[5], локальные сети организации[6].

---

[1] Определение Первого кассационного суда общей юрисдикции от 20 июля 2023 г. № 77-3485/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Кассационные определения Второго кассационного суда общей юрисдикции от 24 февраля 2021 г. № 77-463/2021 и от 2 марта 2021 г. № 77-566/2021. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Определение Первого кассационного суда общей юрисдикции от 11 ноября 2021 г. № 77-4361/2021. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Приговор Тигильского районного суда Камчатского края от 20 июля 2023 г. по делу № 1-1-27/2023 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[5] Приговор Ленинского районного суда города Севастополя от 5 июня 2023 г. по делу № 1-217/2023 // Там же.

[6] Приговор Петропавловск-Камчатского городского суда Камчатского края от 11 февраля 2020 г. по делу № 1-158/2020 // Там же ; Приговор Петропавловск-Камчатского городского суда Камчатского края от 5 марта 2020 г. по делу № 1-226/2020 // Там же.

Уголовный закон не требует, чтобы указанные в статьях 242 и 242.1 УК РФ информационно-телекоммуникационные сети являлись только сетями общего пользования. Так, судебная практика признает возможным осуждение по п. «б» ч. 3 ст. 242 УК РФ и в том случае, если распространение порнографического материала имело место в электронной группе в рамках мобильного приложения «WhatsApp»[1].

По нашим подсчетам, в 95,3 % в качестве информационно-телекоммуникационной сети, где распространялись порнографические материалы, выступала социальная сеть «ВКонтакте».

Применение указанных норм может вызывать определенные сложности.

Первая из имеющихся проблем касается отсутствия в законодательстве общего понятия порнографии. Вместо него раскрываются понятия, тесно связанные с этим явлением. Так, в пункте 8 статьи 8 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» используется термин информация порнографического характера, под которой понимается информация, представляемая в виде натуралистических изображения или описания половых органов человека и (или) полового сношения либо сопоставимого с половым сношением действия сексуального характера, в том числе такого действия, совершаемого в отношении животного.

В примечании 1 к статье 242.1 УК РФ дано понятие материалов и предметов с порнографическими изображениями несовершеннолетних для целей уголовного права.

Правоприменительная практика в целях установления того, относится ли размещенный материал к порнографическим, обращаются к заключению эксперта. По некоторым категориям материала (например, фильмам) это может являться оправданным. В некоторых фильмах присутствует изображения обнаженных человеческих тел, половых сношений.

[1] Приговор Елизовского районного суда Камчатского края от 20 ноября 2019 г. по делу № 1-460/2019 // Там же.

Законодательство не исключает возможности выпуска таких фильмов в гражданский оборот. В частности, возможна выдача прокатных удостоверений на фильмы, но предназначенные для зрителей, достигших возраста 18 лет, и которые содержат изображение или описание половых отношений, в том числе действий сексуального характера, сцен сексуального насилия или принуждения, но только при условии, если это оправдано жанром и (или) сюжетом фильма[1].

Поэтому не потеряла своей актуальности рекомендация, сформулированная Верховным Судом РСФСР по конкретному делу, о том, что отнесение видеофильмов к порнографическим изделиям должно производиться искусствоведческой экспертизой с обязательным участием специалистов в области киноискусства, имеющих специальное образование и опыт работы[2].

Необходимость проведения экспертизы в подобных примерах обусловлена неочевидностью того, что сюжет видеофильма носит допустимый или явно аморальный, противозаконный, порнографический характер.

Однако вызывает вопросы необходимость проведения такой экспертизы, когда порнографический характер размещенного видеоролика является очевидным. В отличие от видеофильмов, в размещаемых в информационно-телекоммуникационных сетях порнороликах отсутствует художественный сюжет, оправдывающий обнажение. В связи с этим «подстраховка» судебно-следственных органов, требующих наличие заключения эксперта во всех случаях, касающихся незаконного распространения порнографии, вызывает обоснованные сомнения.

Это суждение актуально и в том контексте, что для виновного, как и для любого человека, не обладающего специальными познаниями, в целях соблю-

[1] Административный регламент Министерства культуры Российской Федерации по предоставлению государственной услуги по выдаче прокатных удостоверений на фильмы, созданные в Российской Федерации или приобретенные за рубежом для проката на ее территории, и по ведению Государственного регистра фильмов : утв. Приказом Минкультуры России от 20 июля 2012 г. № 787 : текст с изм. и доп. на 28 дек. 2015 г. Подп. 20.4.3.6. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Бюллетень Верховного Суда РСФСР. 1989. № 5. С. 9.

дения принципа субъективного вменения должен быть очевиден порнографический характер распространяемых материалов. Актуальность такого вывода основывается и на том, что по статьям 242 и 242.1 УК РФ могут квалифицироваться и деяния, носящие «бытовой» характер.

Так, к ответственности по статье 242 УК РФ был привлечен гражданин, который посредством интернет-мессенджера «WhatsApp» направил фотографию, являющуюся порнографическим материалом, на абонентский номер сотовой связи, находящийся в пользовании потерпевший, получившего отмеченный выше порнографический материал[1].

Во-вторых, весьма сложен вопрос о субъективной стороне рассматриваемых преступлений.

Большинство исследователей сходятся во мнении, то рассматриваемые преступления совершаются с прямым умыслом. Такой точки зрения придерживаются С.В. Маликов и А.И. Чучаев[2], А.В. Наумов[3], Е.В. Миллеров и Е.А. Миллерова[4], В.Н. Бурлаков, Л.В. Готчина, Л.Н. Плоткина и В.В. Семенова[5].

В целом это суждение не вызывает вопросов, поскольку то, что рассматриваемые статьи 242 и 242.1 УК РФ совершаются именно с прямым умыслом, следует из того, что они сконструированы в качестве формальных составов, то есть считаются оконченными с момента распространения информации порнографического характера.

---

[1] Приговор Марксовского городского суда Саратовской области от 10 февраля 2023 г. по делу № 1-18/2023 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[2] Полный курс уголовного права. В 10 т. Т. VII. Преступления против общественной безопасности и общественного порядка / под ред. А. И. Коробеева. СПб., 2021. С. 506, 509.

[3] Наумов А. В. Российское уголовное право. Курс лекций. В 3 т. Т. 3. Особенная часть (главы XI—XXI). М., 2016. С. 177, 178.

[4] Энциклопедия уголовного права. В 35 т. Т. 22. Преступления против здоровья населения и общественной нравственности / [М. А. Любавина и др.]. СПб., 2014. С. 702.

[5] Бурлаков В. Н., Готчина Л. В., Плоткина Л. Н., Семенова В. В. Защита здоровья населения и общественной нравственности в уголовном праве / под ред. В. Н. Бурлакова. СПб., 2023. С. 138, 142.

Для формальных составов в большей степени характер прямой умысел. Кроме того, сам характер преступлений, связанный с распространением порнографических материалов, предполагает, что субъект преступления осознает характер того, что распространяемые им материалы содержат информацию порнографического характера и такие действия приведут к причинению вреда охраняемым общественным отношениям в виде общественной нравственности.

О наличии в статьях 242 и 242.1 УК РФ только прямого умысла отмечают и суды в своих постановлениях[1].

Однако некоторые авторы отмечают сложности в определении вида умысла в составах распространения порнографических материалов с использованием информационно-телекоммуникационных сетей. Проблема здесь состоит в том, что пользователи могут сделать свой профиль в этих сетях открытым, что дает возможность другим гражданам ознакомиться с их содержимым.

В данном случае распространение состоит не в направлении другим адресатам порнографических материалов, а в возможности ознакомления с ними других лиц. Так, по одному из уголовных дел осужденный по статье 242.1 УК РФ пояснил, что специального намерения распространять файлы порнографического характера не имел, скачивал их ради любопытства, загружаемые файлы автоматически сохранялись в папке, созданной по умолчанию самой программой, он просто не обращал внимания на то, что к этой папке открыт общий доступ[2].

На возможность совершения рассматриваемых преступлений указанным способом обращает внимание и Верховный Суд Российской Федерации.

[1] Определение Верховного Суда Российской Федерации от 6 июля 2021 г. № 89-УД21-8-К7, Определение Восьмого кассационного суда общей юрисдикции от 17 февраля 2021 г. № 77-517/2021. (Доступ из справ.-правовой системы «КонсультантПлюс».)

[2] Приговор Кушвинского городского суда Свердловской области от 9 февраля 2015 г. по делу № 1-3/2015 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

В частности, высшей судебной инстанцией разъяснено, что под распространением порнографических материалов в статьях 242 и 242.1 УК РФ понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Оно может совершаться в том числе путем размещения на личных страницах и на страницах групп пользователей, в том числе в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания[1].

С учетом этого некоторые криминалисты приходят к выводу, что в такой ситуации размещения информации порнографического характера на личной странице, к которой открыт общей доступ, у виновного имеется не прямой, а косвенный умысел[2].

Однако следует учитывать, что в настоящее время личные страницы в социальных сетях имеют соответствующие программы, направленные на ограничение доступа к определенному контенту посторонних лиц. Их невыполнение свидетельствует о том, что лицо выражает намерение распространить какую-либо информацию, сделать ее достоянием неопределенного круга лиц. Соответственно, лицо понимало неизбежность распространения этой информации и желало этого, что вполне охватывается формулой прямого умысла.

На эту техническую особенность доступа к личным страницам в социальных сетях обращают внимание и суды. Так, по одному из дел суд в приговоре отметил, что виновный Л. умышленно не воспользовался ограничениями в допуске пользователей социальной сети «ВКонтакте» к загруженным в

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. П. 22. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Ширяев А. Ю. О возможности косвенного умысла в преступлениях с формальным составом // Российский юридический журнал. 2016. № 5. С. 154 ; Альфимов Н. Г. Современные аспекты распространения порнографии в сети «Интернет» // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 86.

каталог файлам, тем самым умышленно предоставил хранящиеся в указанном каталоге файлы на всеобщее обозрение и для копирования, то есть сделал указанный видеофайл общедоступным[1]. По другому уголовному делу суд указал, что виновный умышленно не выполнил условия правил регистрации на сайте и не ограничил доступ к посещению своей страницы другим пользователям, тем самым оставил размещенные им файлы на всеобщее обозрение и копирование любому желающему пользователю социальной сети «ВКонтакте», предоставив возможность просматривать и копировать их[2].

В то же время следует учитывать, что сохранение скачанных на компьютер файлов порнографического характера в программе, позволяющей другим пользователям скачивать эти файлы, само по себе не может свидетельствовать об умысле виновного на их распространение[3].

Вменение ст. 242 УК РФ предполагает, что умысел направлен на причинение вреда именно общественной нравственности, а не другому объекту. Исходя из этого полагаем, что пересылка интимных фотографий между близкими людьми не является уголовно наказуемым.

Мотивация распространения порнографических материалов с использованием информационно-телекоммуникационных сетей юридического значения не имеет. Такие мотивы могут быть различными и заключаться в корысти, хулиганских побуждениях, удовлетворении половой потребности, мести[4], ревности[5] и прочее.

---

[1] Приговор Измайловского районного суда города Москвы от 2 марта 2023 г. по делу № 1-84/2023 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[2] Приговор Клинцовского городского суда Брянской области от 14 февраля 2023 г. по делу № 1-11/2023 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[3] Определение Первого кассационного суда общей юрисдикции от 22 апреля 2021 г. № 77-1239/2021. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Соловьев В. С. Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. 2017. № 6. С. 60—64.

[5] Приговор Воткинского районного суда Удмуртской Республики от 8 июня 2018 г. по делу № 1-188/2018 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Отдельный вопрос образует ситуация, когда виновный распространял материалы порнографического характера таким образом, что доступ к ним получают несовершеннолетние в возрасте от 12 до 16 лет. Указанное может представлять собой интеллектуальный способ совершения развратных действий.

Преступление по п. «б» ч. 3 ст. 242 УК РФ и развратные действия являются деяниями, которые отличаются между собой признаками как объективной (характеризующими материалы или предметы как порнографические), так и субъективной стороны (не предполагающими обязательное наличие мотивов и целей, характерных для развратных действий)[1].

В связи с этим совершение развратных действий посредством распространения порнографических материалов в информационно-телекоммуникационных сетях, включая сеть «Интернет», требует дополнительной квалификации по статье 242 или 242.1 УК РФ. Данные действия образуют идеальную совокупность преступлений, что подтверждается и материалами судебной практики[2]. Впрочем, такой подход критикуется отдельными авторами[3].

Совершение же указанных действий в отношении потерпевшего, не достигшего возраста 12 лет, исходя из примечания к ст. 131 УК РФ, является уже не развратными действиями, а изнасилованием или насильственными действиями сексуального характера, и по совокупности вменяются именно эти уголовно-правовые нормы.

---

[1] Об отказе в принятии к рассмотрению жалобы гражданина Королева Дмитрия Ивановича на нарушение его конституционных прав частью второй статьи 242 Уголовного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 20 декабря 2016 г. № 2775-О. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Приговор Невского районного суда города Санкт-Петербурга от 24 июля 2018 г. по делу № 1-1017/2018 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[3] Бурлаков В. Н., Готчина Л. В., Плоткина Л. Н., Семенова В. В. Указ. соч. С. 297.

Например, по п. «б» ч. 4 ст. 132 и п. «б» ч. 3 ст. 242 УК РФ были квалифицированы действия виновного, который в процессе общения в сети «Интернет» с несовершеннолетним, не достигшим возраста 12 лет, направил последнему порнографические фото- и видеоматериалы[1].

При квалификации распространения порнографических материалов с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», может возникнуть ситуация, когда предметом преступления являются материалы порнографического характера, содержащие изображения как взрослых, так и несовершеннолетних, не достигших возраста 18 лет. Такие действия образуют идеальную совокупность преступлений и подлежат квалификации по п. «б» ч. 3 ст. 242 и п. «г» ч. 2 ст. 242.1 УК РФ[2].

В практической деятельности также встречаются ситуации, когда виновный распространяет с использованием информационно-телекоммуникационных сетей порнографические материалы, на которых изображен известный ему человек, к которым он получил доступ в результате личного знакомства и общения.

Подобные деяния в последнее время получают все большее распространение. Целью действий виновного при указанных обстоятельствах выступает распространение не любых, порнографических материалов с неизвестными ему лицами, а порнографических изображений конкретного человека, то есть распространение сведений о частной жизни индивида. В силу этого данные действия помимо п. «б» ч. 3 ст. 242 УК РФ также свидетельствуют о нарушении частной жизни и потому влекут ответственность и по ст. 137 УК РФ[3].

---

[1] Приговор Московского городского суда от 18 февраля 2014 г. по делу № 2-0011/2014 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[2] Приговор Промышленного районного суда города Курска от 17 августа 2023 г. по делу № 1-215/2023 // Там же.

[3] Приговор Ленинского районного суда города Уфы от 20 января 2015 г. по делу № 1-30/2015 // Там же ; Приговор Первомайского районного суда города Краснодара от 21 апреля 2023 г. по делу № 1-139/2023 // Там же.

Однако следует учитывать, что вменение ст. 137 УК РФ возможно лишь в том случае, если информация порнографического характера собрана виновным незаконно. Если же она была получена от самого потерпевшего и с его согласия, то вменение ст. 137 УК РФ исключается.

В Особенной части УК РФ криминообразующий признак совершения преступления в информационно-телекоммуникационных сетях, в том числе сети «Интернет», используется в 36 составах. При этом его юридико-техническое изложение не отличается единообразием. Так, в п. «в» ч. 2 ст. 280.4 УК РФ указано об электронных или информационно-телекоммуникационных сетях.

Поскольку информатизация современного общества будет продолжаться и дальше, считаем необходимым унификацию терминологического изложения данного признака в уголовном законе. Кроме того, следует задуматься и о том, чтобы закрепить признак совершения преступления с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», в Общей части УК РФ в качестве обстоятельства, отягчающего наказание.

УДК 343

С. М. МЕДУНЦОВА

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СВЯЗАННЫЕ С БЛАНКЕТНЫМИ ПРИЗНАКАМИ СОСТАВОВ ЭТИХ ПРЕСТУПЛЕНИЙ

Диспозиции норм главы 28 УК РФ носят бланкетный характер. В связи с этим при квалификации преступлений в сфере компьютерной информации возникает ряд проблем, связанных с определением понятий, являющихся обязательными признаками составов рассматриваемых преступлений.

Так, в частности, вызывает трудности при квалификации деяний, предусмотренных статьи 272 УК РФ такой признак предмета преступления, как «охраняемая законом компьютерная информация». Его неопределенность в ряде случаев приводит к неверной квалификации. Несмотря на то, что в примечании к данной статье раскрывается понятие компьютерной информации,

не совсем ясно идет ли речь о любой охраняемой законом информации либо об информации, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная, коммерческая тайна, персональные данные).

Анализ судебной практики показал, что наиболее распространенной является позиция, согласно которой под такого рода информацией понимается информация, доступ к которой ограничен.

Так, Р. была признана виновной в совершении преступления, предусмотренного частью 3 статьи 272 УК РФ.

Третье лицо обратилось к Р. с просьбой передать за вознаграждение персональные данные абонентов ПАО «ВымпелКом», а также информацию с детализацией по абонентским номерам. Находясь на своем рабочем месте в офисе ПАО «ВымпелКом», Р. осуществила вход в систему управления взаимоотношениями с клиентами (ACR) ПАО «ВымпелКом» и произвела поиск информации о детализации по нескольким абонентским номерам. После чего Р. скопировала информацию с детализацией по абонентскому номеру в созданный ею файл «1.xls» на рабочем столе служебного компьютера и затем посредством USB соединения скопировала указанный файл в свой персональный мобильный телефон. Затем Р. посредством программы обмена сообщениями «Telegram» отправила файл «1.xls» третьему лицу[1].

Другой подход подразумевает, что действие ст. 272 УК РФ распространяется на любую охраняемую законом информацию, в том числе и находящуюся в свободном доступе, поскольку согласно статье 6 Федерального закона от 27.07.2006 № 149-ФЗ (в ред. от 2.11.2023) «Об информации, информационных технологиях и о защите информации» обладатель информации устанавливает режим доступа к этой информации.

[1] Приговор Центрального районного суда города Тулы от 15 апреля 2020 г. по делу № 1-101/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Соответственно, неправомерным в таком случае будет являться любой доступ к данной информации, если он нарушает режим, установленный ее обладателем, а также установленные федеральными законами ограничения для такого рода информации.

Кроме того, ст. 7 Федерального закона от 27.07.2006 № 149-ФЗ (в ред. от (в ред. от 2.11.2023) «Об информации, информационных технологиях и о защите информации» предусматривает такой формат общедоступной информации как открытые данные, для которого приказом Министерства связи и массовых коммуникаций Российской Федерации от 27.06.2013 № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования» предусмотрена защита от уничтожения, модификации, блокирования, а также от иных неправомерных действий.

Пленум Верховного Суда Российской Федерации в своем Постановлении от 15.11.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» разъяснил, что в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

Кроме того, отсутствует легальное определение таких относящихся к способу совершения рассматриваемых преступлений понятий, как «уничтожение», «блокирование», «модификация», «копирование» (по отношению к компьютерной информации), что позволяет правоприменителю неоднозначно толковать данные понятия.

Например, анализ судебной практики показал, что под копированием компьютерной информации правоприменитель понимает как непосредственное копирование компьютерной информации из файла одного формата в файл другого формата, с одного цифрового носителя на другой цифровой носитель, так и фотографирование соответствующей компьютерной информации, пересылка файла с такой информацией по электронной почте и распечатка данной информации на бумажном носителе.

Во избежание ошибок квалификации, Пленум Верховного Суда Российской Федерации в пункте 4 вышеуказанного Постановления разъяснил что следует понимать под рассматриваемыми понятиями. Однако указанный документ имеет ограниченный круг действия, что препятствует его применению в целом ряде случаев.

Ввиду этого представляется более целесообразным закрепить понятия «уничтожение», «блокирование», «модификация», «копирование» компьютерной информации на законодательном уровне, в частности в профильном Законе об информации.

Для целей толкования статьи 273 УК РФ в пункте 8, 9 Постановления Пленума Верховного Суда Российской Федерации от 15.11.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» указано, что уголовная ответственность наступает за распространение или использо-

вание только вредоносных компьютерных программ либо иной компьютерной информации, то есть заведомо для лица предназначенной для несанкционированных действий с компьютерной информацией.

Однако при таком толковании содержания понятия вредоносной компьютерной программы из него исключается случаи использования для совершения преступлений легального программного обеспечения.

Например, программы для записи информации на CD-диски нередко используются для изготовления контрафактной продукции, то есть неправомерного копирования информации.

При этом само программное обеспечение никаким изменениям не подвергается, сохраняя полный набор оригинальных настроек, заложенных разработчиком. Квалификация таких деяний по ст. 273 УК РФ весьма затруднительна, поскольку изначально они не являются компьютерными программами, заведомо предназначенными для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Однако в случае приспособления легальной компьютерной программы для совершения конкретных преступлений, для чего соответствующим образом изменяется ее интерфейс, можно вести речь об изготовлении вредоносного программного обеспечения, поскольку происходит модификация исходного функционала программы, что обеспечивает возможность совершения противоправного деяния.

Чаще всего таким образом используют компьютерные программы, предназначенные для записи информации в целях пополнения баланса проездного документа.

Пункт 8 Постановления Пленума Верховного Суда Российской Федерации от 15.11.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информаци-

онно-телекоммуникационных сетей, включая сеть «Интернет» к иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, отнес любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в ч. 1 ст. 273 УК РФ, например, ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

При этом если создается только часть (фрагмент) кода вредоносной компьютерной программы, то такие действия квалифицируются как создание иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Не менее спорным является вопрос о том, что следует понимать под созданием, распространением или использованием таких компьютерных программ.

Например, суд признал К. виновным в распространении вредоносной программы путем продажи за денежное вознаграждение в сумме 500 р. Ф. оптического диска, содержащего программный продукт, в которых имеются инструкции и исполняемые файлы, предназначенные для запуска программного обеспечения без сообщения об ознакомительном периоде или необходимости активации, то есть нейтрализации технической системы защиты, предусмотренной правообладателями от несанкционированного воспроизведения программного обеспечения[1].

Анализ судебной практики позволяет говорить о том, что как правило под распространением вредоносных программ правоприменитель

[1] Приговор Кировского районного суд города Самары от 28.05.2020 по делу № 1-336/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

понимает предоставление доступа к воспроизведенной в любой материальной форме компьютерной программе, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы для любой из этих целей. Одним из типичных способов распространения вредоносных программ является их размещение на различных сайтах в сети «Интернет». Из этого вытекает, что лицо должно либо разместить вредоносную программу в общем доступе, либо непосредственно передать ее другому лицу. Таким образом, виновным лицом должны совершаться непосредственные действия с таким программным обеспечением.

Вместе с тем в пункте 11 Постановления Пленума Верховного Суда Российской Федерации от 15.11.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» среди видов распространения вредоносных программ такие его разновидности, как прокат, сдача в наем и предоставление взаймы не упоминаются, однако они имеют весьма распространенный характер.

Нередко вызывает затруднения при квалификации деяний, предусмотренных ст. 274 УК РФ, отсутствие легального определения понятия «средства хранения, обработки или передачи компьютерной информации».

Представляется целесообразным внести изменения в законодательство Российской Федерации, дополнив его разъяснением содержания указанного понятия. Также не совсем ясно какого рода охраняемая компьютерная информация имеется в виду в диспозиции ч. 1 ст. 274 УК РФ, поскольку, в отличие от диспозиции ч. 1 ст. 272 УК РФ, в ней не указано, что она охраняется законом.

Отдельно следует упомянуть, что проблемы квалификации преступлений, предусмотренных ст. 274 УК РФ, нередко связаны с тем, что по смыслу диспозиции ч. 1 ст. 274 УК РФ субъект данного преступления яв-

ляется специальным, но указание на это в рассматриваемой норме отсутствует, что позволяет правоприменителю неверно расширительно толковать указанное положение уголовного закона, распространяя его действие на общий субъект.

Однако для нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, лицу в силу своих должностных обязанностей необходимо иметь к ним санкционированный доступ и обязанность соблюдать установленные для них правила эксплуатации.

Так, Б., М. и О. признаны виновными в совершении преступлений, предусмотренных статьями 272 и 274 УК РФ. Эти лица, являясь сотрудниками федерального государственного унитарного предприятия, договорились об использовании вычислительных мощностей находящегося на рабочем месте неиспользуемого компьютерного оборудования и его возможностей, предназначенных для обработки конфиденциальной информации уровня конфиденциальности «для служебного пользования», «персональные данные» и «коммерческая тайна», для вычисления (майнинга) криптовалюты и ее последующего обращения в свою пользу, вопреки служебным интересам.

Таким образом, Б., М. и О. неправомерно и с превышением предоставленных им полномочий пользователей указанной системы внесли изменения в состав, конструкцию, конфигурацию, условия размещения компьютерной информации, тем самым существенно снизившие уровень защищенности данной автоматизированной системы. При этом был осуществлен неправомерный доступ к охраняемой законом компьютерной информации, обрабатываемой и передаваемой в указанной сети, что повлекло модификацию компьютерной информации, которая выразилась

в изменении служебной информации, используемой активным сетевым оборудованием данной системы[1].

Тем не менее, на практике встречаются примеры ошибочной квалификации деяний по ст. 274 УК РФ, когда обвинительные приговоры выносятся в отношении лица, не являющегося сотрудником организации, работе информационно-телекоммуникационных сетей которой был нанесен ущерб вследствие его неправомерных действий.

Во избежание неправильной квалификации рассматриваемых деяний, представляется необходимым уточнить данный законодательный пробел путем указания в примечании к ст. 274 УК РФ на специальный субъект.

В настоящее время данные разъяснения приведены в пункте 12 Постановления Пленума Верховного Суда Российской Федерации от 15.11.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» закреплено в качестве обязательного условия доведение до сведения лица, которому вменяется совершение соответствующего преступления, обязанность соблюдения указанных правил в письменном виде.

Проблемы квалификации по статье 274.1 УК РФ, устанавливающей уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в основном связаны с отграничением деяний, предусмотренных этой статьей, от преступлений, предусмотренных другими статьями главы 28 УК РФ, поскольку особенностью данной статьи является то, что она в своей конструкции предусматривает преступные действия, охватываемые статьей 272-274 УК РФ, только совершенные в отношении компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации.

[1] Приговор Саровского городского суда Нижегородской области от 17 сентября 2019 г. по делу № 1-149/2019 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Таким образом, нормы рассматриваемой статьи являются специальными по отношению к другим преступлениям этой главы (по предмету преступления). И при квалификации необходимо учитывать положения ч. 3 ст. 17 УК РФ о том, что если преступление предусмотрено общей и специальной нормами, то ответственность наступает по специальной норме.

Причем нормами статьи 274.1 УК РФ полностью охватываются использование вредоносных компьютерных программ для совершения данных деяний, и дополнительная квалификация по статье 273 УК РФ не требуется.

Суд признал Л., М. и О. виновными в совершении преступления, предусмотренного статьей 274.1 УК РФ. Л., М. и О. осуществили неправомерный доступ к компьютерной информации, содержащейся в критической информационной структуре Российской Федерации – АО «Восточная верфь», путем использования вредоносной программы, что повлекло причинение вреда критической информационной структуре Российской Федерации, выразившегося в модификации компьютерной информации и воздействиях на компьютерную информацию и технику, вследствие чего стало невозможно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, и повлекло за собой нарушение рабочего и производственного процесса АО «Восточная верфь»[1].

Однако для верной квалификации деяний по статье 274.1 УК РФ необходимо обязательное причинение вреда критической информационной структуре Российской Федерации, совершенное умышленно. В противном случае такие деяния должны быть квалифицированы по другим статьям главы 28 УК РФ.

[1] Приговор Первомайского районного суда города Владивостока от 25 сентября 2019 г. по делу № 1-376/2019 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Так, А., находясь на своем рабочем месте в здании предприятия, относящегося к объектам критической информационной структуры, после обращения к нему сотрудницы с просьбой о предоставлении ей компьютерной программы «Microsoft Office Word» для другой сотрудницы с целью использования указанной программы по месту жительства на период действия режима самоизоляции, скачал из информационно-телекоммуникационной сети «Интернет» на закрепленный за ним служебный компьютер указанную программу и передал через просившую его сотрудницу указанного предприятия твердотельный накопитель, содержащий экземпляр программного продукта «Microsoft Office», другой сотруднице, которая осуществила копирование данной компьютерной программы на свой личный персональный компьютер, находящийся по месту жительства.

В результате действий А. вместе с программой «Microsoft Office Word» совместно с программой-активатором на служебный компьютер А. была скачана вредоносная программа, которая с его рабочего компьютера два раза в день (при включении и выключении) передавала данные в малом объеме в американский сегмент сети «Интернет». При этом во время скачивания и открытия программы «Microsoft Office Word» совместно с программой-активатором каких-либо уведомлений от антивируса, установленного на его служебном компьютере, не поступало. Сам А. антивирус не отключал, в исключение скаченные им программы не вносил.

Идентифицировать какие именно данные были отправлены в зарубежный сегмент сети «Интернет» не представлялось возможным. В ходе проверки выяснилось, что дальше компьютера А. вредоносная программа не распространилась, сеть предприятия не пострадала, так как был установлен небольшой трафик с очень маленьким объемом информации. На служебном компьютере А. какой-либо информации с ограниченным доступом не содержалось. Умысла на причинение вреда предприятию у А. не имелось.

А. был оправдан за отсутствием в его действиях состава преступления, обосновав это тем, что согласно предъявленному А. обвинению по ч. 4

ст. 274.1 УК РФ в качестве вреда, причиненного критической информационной инфраструктуре Российской Федерации, указана утечка информационных массивов из объектов критической информационной структуры Российской Федерации, принадлежащих предприятию, из-за использования нелицензированных программных продуктов, что создало угрозу информационной безопасности предприятия, связанную с последующей утечкой конфиденциальной информации из критической информационной инфраструктуры предприятия третьим лицам, однако при этом не было установлено какая конкретно информация была передана вследствие скачивания А. вредоносной программы.

Таким образом, факт передачи неустановленной по содержанию и характеру информации сам по себе не свидетельствует о причинении существенного ущерба безопасности информации на предприятии, а также причинения какого-либо иного значимого ущерба интересам потерпевшего.

Кроме того, инкриминируемое А. по ч. 4 ст. 274.1 УК РФ преступление относится к категории умышленных. Вместе с тем субъективное отношение А. к последствиям является неосторожным: он не имел умысла на причинение в результате своих действий вредоносных последствий критической информационной инфраструктуре Российской Федерации, а лишь желал помочь своей знакомой и не предполагал, что это повлечет утечку информации.

Тем же приговором суда А. был признан виновным в совершении преступления, предусмотренного частью 1 статьи 273 УК РФ[1].

Таким образом, учитывая изложенное, можно сделать вывод, что несмотря на появление официальных разъяснений Пленума Верхов-

[1] Приговор Кировского районного суда города Перми 7 июля 2021 г. по делу № 1-18/2021 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

ного Суда Российской Федерации по ключевым проблемам квалификации преступлений, предусмотренных главой 28 УК РФ, в настоящее время остается довольно много неразрешенных вопросов в силу специфики и ограниченного характера применения постановлений Пленума Верховного Суда Российской Федерации.

В связи с этим целый ряд бланкетных понятий, содержащихся в диспозициях рассматриваемых норм, следует закрепить на законодательном уровне.

УДК 343

Ю. В. МОРОЗОВА

НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В докладе ООН по вопросу о торговле детьми, детской проституции и детской порнографии в России отмечается, что сексуальная эксплуатация детей в Российской Федерации является более серьезной проблемой, чем торговля детьми, и основными причинами были названы очень тяжелое экономическое положение и сексуальное надругательство в семье.

Сексуальная эксплуатация несовершеннолетних происходит в нелегальных публичных домах, гостиницах, развлекательных заведениях. Этот бизнес тесно связан с интернетом.

Сексуальная эксплуатация несовершеннолетних осуществляется в том числе, путем привлечения детей к проституции и порнографии. Факт массовости сексуальной эксплуатации детей в данных сферах подтверждается не только увеличением числа выявленных преступлений по всему миру, но и растущим количеством онлайн-ресурсов, распространяющих детскую порнографию[1].

[1] Силуянова Ю. А. Борьба с торговлей детьми в России: поиски решения проблемы // Государственное управление. Электронный вестник. 2020. Вып. № 81. С. 273.

Одной из мер противодействия распространению детской порнографии явилось установление уголовной ответственности за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ).

Появление данной статьи связано с ратификацией Конвенции о правах ребенка, обязывающей государства - участники принимать все необходимые меры для предотвращения использования в целях эксплуатации детей в порнографии и порнографических материалах.

Пунктом «г» ч. 2 ст. 242. 1 УК РФ предусмотрена повышенная уголовная ответственность за совершение деяний, предусмотренных анализируемой нормой с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Следует отметить, что данное преступление чаще всего и совершается с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»), что увеличивает общественную опасность анализируемых деяний и вызывает сложности при выявлении и расследовании дел данной категории. Кроме того, возникают проблемные вопросы при квалификации данного состава преступления.

Действующая редакция пункта явилась поводом для обращения в Конституционный Суд Российской Федерации по сколько по мнению заявителя позволяет — вследствие своей неопределенности — относить действия, совершенные в сети «Интернет», к использованию средств массовой информации, квалифицировать такие, адресованные несовершеннолетнему, действия с порнографическими материалами как преступление, а также поскольку допускает смешение понятий «распространение информации» и «предоставление информации», разделенных в Федеральном законе от 27 июля 2006 года № 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации».

Согласно позиции Конституционного Суда Российской Федерации уголовно-правовой запрет, установленный в пункте «б» части третьей статьи 242 УК РФ, согласуется с соответствующими законоположениями, при

этом используемые в них определения не предрешают содержание и, следовательно, истолкование этого запрета, в том числе потому, что он прямо установлен применительно к соответствующим материалам или предметам, которые по своим признакам не идентичны понятиям «информация» и «информационная продукция». Нормы же имеющего самостоятельный предмет регулирования (часть 1 статьи 1) Федерального закона «Об информации, информационных технологиях и о защите информации», разделяя понятия «распространение информации» и «предоставление информации», относятся именно к информации и не предопределяют содержание и объем названного уголовно-правового запрета[1].

Вместе с тем, при квалификации по данному признаку в судебной практике встречаются ошибки.

Так, К. признан виновным в приобретении, хранении в целях распространения, распространение материалов с порнографическими изображениями несовершеннолетних, в том числе, не достигших четырнадцатилетнего возраста, с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Как следует из приговора, К., находясь в своем жилище, используя принадлежащий ему системный блок компьютера, имея доступ к международной информационно-телекоммуникационной сети «Интернет», посредством установленной на его компьютере пиринговой программы, позволяющей загружать и распространять любые типы файлов, в том числе видеофайлы в пиринговых сетях, загрузил, с целью хранения и последующего распространения на принадлежащий ему системный блок, 37 видеофайлов, относящиеся к порнографическим материалам, содержащим порнографическое изображение несовершеннолетних, в том числе лиц, не достигших четырнадцатилетнего возраста. Затем, хранил данные видеофайлы в целях их распространения, в памяти своего компьютера. В дальнейшем К. с целью распространения порно-

[1] Определение Конституционного Суда Российской Федерации от 19 июля 2016 г. № 1746-О. Доступ из справ.-правовой системы «КонсультантПлюс».

графических материалов, содержащихся на 37 видеофайлов порнографические изображения, предоставил свободный доступ к данным файлам для неограниченного числа пользователей сети «Интернет», у которых на компьютере установлена соответствующая программа.

При этом суд не учел, что по смыслу закона квалифицирующий признак, а именно: с использованием средств массовой информации, в том числе информационно-телекоммуникационных сетей (включая сеть «Интернет») распространяется только на интернет-ресурсы, которые зарегистрированы в качестве средств массовой информации.

Однако из фабулы предъявленного обвинения и описательной части приговора не следует, что К., используя принадлежащий ему компьютер, был зарегистрирован в качестве представителя средств массовой информации[1].

Следует отметить, что изготовление или приобретение материалов или предметов с порнографическими изображениями несовершеннолетних для личных целей состава анализируемого преступления не образует. Связано это с тем, что Россия при ратификации «Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений» сделала несколько существенных оговорок. В связи с этим, рассматриваемый состав значительно отличается от большинства схожих составов содержащихся в уголовных кодексах стран Европы[2].

В судебной практике действия пользователей информационно-телекоммуникационных сетей (в том числе сети «Интернет»), связанные с размещением порнографических материалов на общедоступных ресурсах для личного просмотра (в файлообменных программах, на страницах социальных сетей и т. п.), если при этом не совершались другие действия, направленные на передачу указанных материалов неограниченному кругу лиц, не расцениваются как распространение порнографических материалов,

[1] О передаче кассационной жалобы для рассмотрения в судебном заседании суда кассационной инстанции : Постановление Московского городского суда от 13 ноября 2017 г. по делу № 4у/11-5600/17. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Пачулия Г. Т. Уголовно-правовые средства противодействия сексуальной эксплуатации человека : дис. ... канд. юрид. наук. М., 2020. С. 136.

в том числе тогда, когда пользователи осознают факт общедоступности размещенных порноматериалов[1].

По приговору Дзержинского районного суда Калужской области от 20 июня 2019 г. П. признан виновным в распространении материалов с порнографическими изображениями несовершеннолетних.

Судом установлено, что П., отбывая наказание в местах лишения свободы, используя мобильный телефон с выходом в информационно-телекоммуникационную сеть «Интернет», зарегистрировал в социальной сети «ВКонтакте» персональную страницу под ником (псевдонимом), где в разделе «мои фотографии» разместил не менее четырех фотографий с порнографическими изображениями несовершеннолетней С., с предоставлением возможности общего доступа и копирования неограниченному количеству пользователей указанной сети к информации, содержащейся на данной странице.

Эти действия П. были квалифицированы судом по ч. 1 ст. 242.1 УК РФ, как распространение материалов с порнографическими изображениями несовершеннолетних, с чем согласилась апелляционная инстанция Калужского областного суда.

Статья 242.1 УК РФ прямо определяет, какие действия составляют объективную сторону предусмотренного этой статьей преступления, а также указывает на наличие прямого умысла, направленного на незаконное распространение порнографических материалов или предметов, как обязательного условия привлечения правонарушителя к ответственности.

При этом, распространение порнографических материалов или предметов заключается в выпуске в обращение указанных предметов, передаче их на любых основаниях хотя бы одному лицу.

Как распространение порнографических материалов или предметов также следует оценивать и действия, направленные на доведение до сведения других лиц путем их показа, демонстрации видеофильмов, чтения литературных порнографических изданий, организации порнографических шоу и т. д.

---

[1] Определение Первого кассационного суда общей юрисдикции от 24 марта 2020 г. № 77-291/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

Хранение материалов или предметов с порнографическими изображениями несовершеннолетних может быть уголовно-наказуемым деянием лишь при условии доказанности совершения с целью их последующего распространения, публичной демонстрации или рекламирования. Если указанные материалы приобретаются и хранятся для личного просмотра, то состав преступления отсутствует.

Вместе с тем, сославшись в приговоре на наличие у П. прямого умысла на распространение материалов с порнографическими изображениями несовершеннолетних по данному эпизоду, суд не дал оценки тому обстоятельству, что с данной страницы в социальных сетях П. никому указанные фотографии не рассылал и не сообщал об их наличии.

Распространение материалов с порнографическими изображениями несовершеннолетней потерпевшей совершалось осужденным со страницы под другим ником в социальной сети «ВКонтакте» и с его страницы в социальных сетях «Одноклассники».

Достоверные данные о том, что на странице осужденный разместил фотографии с порнографическими изображениями несовершеннолетней потерпевшей именно с целью их распространения, что они были распространены осужденным, то есть получены другими лицами в результате его целенаправленных действий, в материалах дела не содержатся и в приговоре не приведены.

То обстоятельство, что эта страница в соцсетях была доступна для всеобщего обозрения и копирования, не свидетельствует о том, что этими действиями осужденный распространил порнографические изображения несовершеннолетней. При этом квалифицирующий признак ст. 242.1 УК РФ, вмененный осужденному органами следствия, «публичная демонстрация материалов с порнографическими изображениями несовершеннолетних» судом первой инстанции исключен из обвинения П.

Судебная коллегия по уголовным делам Первого кассационного суда общей юрисдикции приговор и апелляционное определение в части осуждения

П. по эпизоду распространения материалов с порнографическим изображением несовершеннолетней путем помещения фотографий потерпевшей на своей странице под ником в социальной сети «ВКонтакте» отменила с прекращением уголовного преследования П. в этой части в связи с отсутствием в деянии состава преступления, предусмотренного ч. 1 ст. 242.1 УК РФ, с признанием за ним права на реабилитацию[1].

В практике распространены случаи совершения развратных действий, сопряженных с изготовлением и распространением материалов или предметов с порнографическими изображениями несовершеннолетних.

В соответствии с п. 17 Постановления Пленума Верховного Суда Российской Федерации от 4 декабря 2014 г. № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» к развратным действиям применительно к статье 135 УК РФ следует относить любые действия, кроме полового сношения, мужеложства и лесбиянства, совершенные в отношении лиц, достигших двенадцатилетнего возраста, но не достигших шестнадцатилетнего возраста, которые были направлены на удовлетворение сексуального влечения виновного, или на вызывание сексуального возбуждения у потерпевшего лица, или на пробуждение у него интереса к сексуальным отношениям.

Также согласно данному Постановлению Пленума Верховного Суда Российской Федерации развратными могут признаваться и такие действия, при которых непосредственный физический контакт с телом потерпевшего лица отсутствовал, включая действия, совершенные с использованием сети «Интернет», иных информационно-телекоммуникационных сетей.

Факты совершения развратных действий, сопряженных с изготовлением и распространением порнографических материалов, можно разделить на две группы, а именно, когда порнографические материалы являются лишь средством

[1] Обобщение кассационной практики судебной коллегии по уголовным делам Первого кассационного суда общей юрисдикции за второй квартал 2020 г. (типичные ошибки, допускаемые судами, входящими в кассационный округ) : утв. Президиумом Первого кассационного суда общей юрисдикции 3 сентября 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс».

данного преступления и когда, наоборот, сами развратные действия являются средством (предметом) фото- и видеосъемок порнографического характера[1].

Примером, когда использование порнографии является одним из средств совершения развратных действий, может служить приговор в отношении Ф., который, находясь в квартире с двумя лицами, не достигшими 16-летнего возраста, вел с ними разговоры на сексуальные темы, демонстрировал им фотоснимки обнаженных половых органов, а также видеофильмы сексуально непристойного характера, включая соответствующие диски в DVD-проигрывателе, вместе с тем демонстрируя несовершеннолетним и свои половые органы.

Поскольку согласно назначенной и проведенной в ходе предварительного следствия комиссионной искусствоведческой экспертизе указанные фильмы были признаны порнографическими, действия виновного как на предварительном следствии, так и в суде были квалифицированы по совокупности ст. 135 и ст. 242 УК РФ[2].

Примеров, когда развратные действия являются материалом для изготовления фото- или видеопродукции порнографического характера, тоже встречается немало. Так, по совокупности преступлений, предусмотренных ст. 135 и ст. 242.1 УК РФ, осужден гражданин, который совершал развратные действия в отношении своего пасынка, фотографируя их на свой мобильный телефон, а затем распространяя в сети «Интернет»[3].

На практике данные действия, как правило, квалифицируются по совокупности преступлений. Представляется, что данная практика является правильной.

---

[1] Миллерова Е. А. О некоторых проблемах квалификации развратных действий, сопряженных с изготовлением и распространением порнографических материалов // Уголовное право. 2015. № 2. С. 36—39.

[2] Приговор Кингисеппского городского суда Ленинградской области от 18 мая 2011 г. по делу № 1-167/2011 // Кингисеппский городской суд Ленинградской области : офиц. сайт. URL: https://kingisepp--lo.sudrf.ru (дата обращения: 19.09.2023).

[3] В Свердловской области местный житель признан виновным в совершении преступлений сексуального характера в отношении своего пасынка // Следственный комитет Российской Федерации : офиц. сайт. URL: https://sledcom.ru (дата обращения: 30.09.2023).

УДК 343

Т. М. ПЕТРОВА

НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ И ЗАКОНОДАТЕЛЬНОЙ РЕГЛАМЕНТАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ», ПРОТИВ ОСОБО ОХРАНЯЕМЫХ БИОРЕСУРСОВ

В современном мире все большую распространенность получает совершение преступлений с помощью цифровых технологий. Мессенджеры, социальные сети, компьютерная техника, средства массовой информации, сама сеть «Интернет» используются преступниками во всем мире. По данным МВД РФ с использованием информационно-коммуникационных технологий совершается каждое третье преступление. За период январь-сентябрь 2023 года в этой сфере зарегистрировано на 29,2 % преступлений больше, чем за аналогичный период прошлого года[1].

Ответом законодателя на проникновение информационных цифровых технологий в преступную сфере является установление уголовной ответственности с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», за совершение тех деяний, которые ранее им были криминализированы, то есть, в уголовном законе конструируются новые квалифицированные составы.

В сфере охраны дикой флоры и фауны стремительное развитие глобализации и информатизации оказывает огромное влияние на международный рынок по торговле редкими и исчезающими видами животных и растений.

При этом незаконный оборот биоресурсов, находящихся под угрозой исчезновения, уже давно считается одним из наиболее прибыльных видов нелегального бизнеса. Собственно, с вовлеченностью редких животных и растений в торговый оборот в основном и связана интенсивность их изъятия из природной среды. Еще в 2016 году министр природных ресурсов и экологии Рос-

[1] Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/dejatelnost/statistics (дата обращения 23.11.2023).

сийской Федерации Сергей Донской озвучил данные о том, что оборот незаконной торговли дикими животными оценивается в 19 миллиардов долларов в год. В России браконьерский рынок оценивается в сумму свыше 10 миллиардов рублей[1].

В последние десятилетия широкие возможности для онлайн-торговли особо охраняемыми видами биоресурсов предоставляют именно интернет-технологии. Через сеть реализуется преступный умысел лиц, осуществляющих незаконную торговлю особо охраняемыми животными и растениями.

С использованием таких средств связи виновные лица ведут поиск предложений о приобретении или продаже предмета преступления путем размещения соответствующих объявлений, договариваются о способах и видах оплаты по сделке, передаче предмета сделки. С помощью сети «Интернет» возможно существенным образом расширить аудиторию совершаемого преступления, сохранив при этом анонимность самого преступника. По данным Минприроды Российской Федерации, только за год было обнаружено более 30 тысяч объявлений в интернете о продаже занесенных в Красную книгу Российской Федерации диких животных, либо изготовленных из них товаров.

Уголовное законодательство Российской Федерации в ответ на распространение влияния интернет-технологий пополнилось новыми составами в части установления ответственности за совершение экологических преступлений, а именно, за посягательства на краснокнижные виды животных и растений.

Так, в 2018 году ст. 258.1 УК РФ была дополнена ч. 1.1, предусматривающей ответственность за незаконные действия в виде приобретения и продажи особо ценных диких животных и водных биологических ресурсов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Введение в уголовное законодательство данной нормы было связано с массовыми случаями продажи шкур, костей и прочих дериватов особо ценных диких животных и водных биологических ресурсов в сети «Интернет»;

[1] Березина Е. Зверье выдернут из сети // Российская газета. 2016. 19 окт. (№ 237).

отсутствием постоянного государственного мониторинга торговых площадок в сети «Интернет».

Предложение о торговле с использованием средств массовой информации и сети «Интернет» распространяется на широкий круг лиц, что ведет к массовому сбыту и уничтожению особо ценных животных[1].

В апреле 2023 года УК РФ был дополнен ст. 260.1 «Умышленные уничтожение или повреждение, а равно незаконные добыча, сбор и оборот особо ценных растений и грибов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации».

По аналогии со ст. 258.1 УК РФ в структуре ст. 260.1 УК РФ имеется часть вторая, предусматривающая ответственность за незаконные приобретение или продажу особо ценных растений и грибов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации, их продуктов, частей и деривативов (производных) с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Таким образом, всемирная сеть может выступать как способ и средство совершения преступления – незаконного приобретения или продажи особо ценных видов диких животных, водных биологических ресурсов, растений и грибов[2].

---

[1] Паспорт проекта федерального закона № 356397-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (по вопросу совершенствования уголовного законодательства Российской Федерации в сфере противодействия преступлениям, связанным с незаконной добычей и оборотом водных биологических ресурсов, диких животных, в том числе занесенных в Красную книгу Российской Федерации)» // СОЗД : сайт. URL: https://sozd.duma.gov.ru/bill/356397-7 (дата обращения: 25.10.2023).

[2] Скачко А. В. Сеть «Интернет» как способ и средство для незаконного приобретения или продажи особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации // Право и политика. 2019. № 1. С. 104—107.

Сам Перечень особо ценных видов диких животных и водных биологических ресурсов утвержден постановлением Правительства Российской Федерации от 31 октября 2013 года № 9783. В октябре 2023 года в него были внесены дополнения в части отнесения к ценным видам также растений и грибов. Помимо ранее указанных 22 видов млекопитающих, рыб и птиц Перечень дополнен такими особо ценными видами растений и грибов, как женьшень настоящий, родиола розовая и рядовка мацутакэ.

То есть, далеко не за каждого представителя животного и растительного мира, внесенного в Красную книгу, виновное лицо может понести наказание. В отношении редких и исчезающих животных, занесенных в Красную книгу, но не внесенных в указанный выше Перечень, такой ответственности на сегодняшний день не предусмотрено и их использование в нелегальном обороте уголовно не наказуемо.

При этом, научно обоснованные критерии определения особой ценности диких животных и водных биологических ресурсов, за посягательство на которые наступает уголовная ответственность по ст. 258.1 УК РФ, в законе на сегодняшний день отсутствуют. В качестве таковых в литературе выделяют, в совокупности, следующие: количество посягательств на такие объекты, экологическую, культурную и экономическую ценности[1].

При совершении экологических преступлений в отношении редких видов биоресурсов не всегда возможно определить видовую принадлежность животного — в объявлениях, размещенных в сети «Интернет», подобная информация преступными лицами намеренно скрывается.

При необходимости следователям следует использовать специальные знания экспертов и ставить вопрос о проведении экспертизы объектов дикой флоры и фауны на предмет отнесения их к числу особо ценных. Экспертиза проводится лицами, имеющими специальные знания в области ботаники, микологии, зоологии, генетики, экологии, ветеринарии, криминалистики.

[1] Гусаренко Д. М. Относительная распространенность посягательств на особо ценных диких животных // Российский следователь. 2017. № 17. С. 36—39.

При квалификации деяний, совершенных посредством сети «Интернет» либо иных информационных ресурсов, когда они совершаются путем приобретения либо продажи предмета преступления, могут возникнуть трудности относительно того, какая норма подлежит применению — п. «б» ч. 2 ст. 258.1 УК РФ (незаконные добыча и оборот особо ценных видов биоресурсов с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетей, в том числе сети «Интернет») либо ч. 1.1, а также 2.1 и 3.1 ст. 258.1 УК РФ.

Каких-либо четких критериев ни наука, ни практика на этот счет до сих пор не выработали. Мы придерживаемся той позиции, что преступное деяние квалифицируется по части 1.1, 2.1 и 3.1 статьи 258.1 УК РФ в случаях, если средства массовой информации либо электронные или информационно-телекоммуникационные сети, в том числе сеть «Интернет», используются для обеспечения совершения общественно опасного деяния.

К примеру, с их помощью достигается соглашение на совершение сделки, посредством электронных средств осуществляются платежи, размещается реклама в средствах массовой информации или в информационно-телекоммуникационных сетях, в том числе, в сети «Интернет».

В тех случаях же, когда путем средств массовой информации или информационно-телекоммуникационных сетей, включая сеть «Интернет», публично демонстрируется процесс или результат приобретения или продажи предмета преступления, предусмотренного ст. 258.1 УК РФ, содеянное следует квалифицировать по п. «б» ч. 2 или по ч. 3 ст. 258.1 УК РФ. Аналогичным образом, на наш взгляд, следует квалифицировать посягательства по введенной в уголовное законодательство ст. 260.1 УК РФ.

Однако примеры из судебной практики иллюстрируют разные подходы к квалификации деяний в каждом конкретном случае. Так, например, П. обвинялся в совершении преступления, предусмотренного п. «б» ч. 2 ст. 258.1 УК РФ. Из корыстных побуждений П. посредством сети «Интернет» у неустановленного лица приобрел черную икру дикой рыбы «калуга» весом не менее

523 грамм, добытую незаконным способом, перевез ее до места своего проживания, после чего с целью ее реализации посредством сети «Интернет» разместил в публичной группе «Камчатский берег v.2» объявление о ее продаже[1].

Согласно материалам дела № 1-39/2020 от 19.05.2020 Ц. обвиняется в совершении преступления, предусмотренного ч. 1.1. ст. 258.1 УК РФ, а именно Ц. посредством интернет ресурса в социальной сети «ВКонтакте», в группе «Барахолка Ейск», под ником «Иван Макаренко» разместил объявление о продаже Азовского осетра стоимостью 1 300 рублей за 1 кг. Впоследствии с целью извлечения материальной выгоды незаконно продал два экземпляра рыбы Русский осетр, которые были изъяты в ходе оперативно-розыскного мероприятия[2].

В диспозициях ч. 1.1 ст. 258.1 УК РФ и ч. 2 ст. 260.1 УК РФ содержится указание на совершение лишь двух преступных действий — приобретения и продажи. Однако в отношении особо ценных видов биоресурсов с помощью сети «Интернет» возможно совершение и иных действий, к примеру, их пересылка.

В таком случае, в целях недопущения уклонения от уголовной ответственности виновных лиц, данное действия следует квалифицировать по ч. 1 ст. 258.1 УК РФ либо ч. 1 ст. 260.1 УК РФ.

Помимо законодательной регламентации действий о недопустимости преступных посягательств в отношении редкой флоры и фауны, включая использование средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», следует ответственно и со всей долей серьезности подойти к разработке механизма их практического исполнения.

---

[1] Приговор Ново-Савиновского районного суда города Казани Республики Татарстан от 21 мая 2020 г. по делу № 1-28/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

[2] Приговор Ейского районного суда Краснодарского края от 19 мая 2020 г. по делу № 1-39/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Необходимо усиление взаимодействия правоохранительных и контролирующих органов, в лице прокуратуры, органов внутренних дел, таможенных органов, Росприроднадзора, а также специалистов в области редкой флоры и фауны в лице биологов, зоологов, экологов, ботаников. Любая правовая норма будет действовать лишь тогда, когда отлажен механизм ее применения на практике.

УДК 343

С В. ПИКАЛОВ

ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ИСПОЛЬЗОВАНИЯ СЛУЖЕБНОГО ПОЛОЖЕНИЯ ПРИ КВАЛИФИКАЦИИ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПЛЕНИЙ

Уголовный закон не раскрывает понятие служебного положения, равно как не раскрывает виды и способы его использования, при этом Особенная часть Уголовного кодекса Российской Федерации содержит значительное количество составов преступлений, где факт использования служебного положения при совершении преступления является квалифицирующим признаком.

Сам по себе квалифицирующий признак использования служебного положения достаточно широко освещен в научной литературе, посвященной конкретным видам преступлений, особенно мошенничеству, присвоению и растрате, сбыту наркотиков.

В целях формирования единства судебной практики в разное время были приняты постановления Пленума Верховного Суда Российской Федерации, которые раскрывают содержание признака «использование служебного положения», применительно к конкретным составам преступлений, но по-разному. Применительно к ст. 272 УК РФ (неправомерным доступом к компьютерной информации) и ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ) такие разъяснения отсутствуют.

В обозначенных документах Верховный Суд Российской Федерации использует статусный и функциональный критерии, через которые раскрывается

признак «использование служебного положения», но в зависимости от вида преступления.

Статусный определяется через принадлежность преступника к категории должностного лица или лица, обладающего признаками, предусмотренными п. 1 прим. к ст. 285 УК РФ, государственным или муниципальным служащим, а также иным лицам, отвечающим требованиям, предусмотренным п. 1 прим. к ст. 201 УК РФ. Функциональный — через профессиональные функции, исполнение которых облегчает совершение преступления[1].

Генеральная прокуратура Российской Федерации, давая рекомендации по осуществлению надзорной деятельности (далее по тексту — Рекомендации), под использованием служебного положения применительно к ч. 3 ст. 272 УК РФ, предлагает понимать или фактический доступ к компьютерной информации, возникший из исполнения профессиональных обязанностей (на основании трудового и гражданско-правового договора), или влияния по службе на лиц, имеющих такой доступ[2].

То есть речь идет о функциональном критерии. Согласно данным разъяснениям, специальным субъектом может быть не только должностное лицо, но и рядовые сотрудники частной организации: программисты, пользователи программ, администраторы баз данных, инженеры, ремонтники и прочие.

При всем при этом во всех Постановлениях Пленума Верховного Суда Российской Федерации после 2007 года использование при совершении преступления служебного положения трактуется через статусный критерий.

Анализ 83 судебных актов первой, апелляционной и кассационной инстанций, где лица привлекались к уголовной ответственности по ч. 3 ст. 272 УК РФ (неправомерным доступом к компьютерной информации с использованием служебного положения) и по ч. 2 ст. 273 УК РФ (создание, использование

[1] Щепельков В. Ф. Субъектный состав преступления, совершаемого с использованием своего служебного положения, в разъяснениях Верховного Суда Российской Федерации // Криминалистъ. 2023. № 2 (43). С. 65—70.

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации / Генеральная прокуратура Российской Федерации // Законы. Кодексы и нормативно-правовые акты Российской Федерации : сайт. URL: https://legalacts.ru (дата обращения: 09.11.2023).

и распространение вредоносных компьютерных программ с использованием служебного положения) показал, что суды руководствуются именно функциональным критерием.

Сложившуюся ситуацию нельзя назвать приемлемой. Необходим единый подход к прочтению уголовного закона, на что неоднократно обращал внимание Конституционный Суд Российской Федерации.

Принцип правовой определенности обязывает законодателя формулировать уголовно-правовые нормы с достаточной ясностью, чтобы каждый мог осознавать, что является разрешенным или запрещенным поведением и предвидеть последствия своих действий[1].

Недопустимо, чтобы существовало несколько взаимоисключающих варианта толкования одной и той же уголовно-правовой нормы в отношении одного вопроса при правоприменении[2].

Возвращаясь к проведенному анализу судебной практики было установлено, что суды по этой категории дел, в отличие от мошенничества, присвоения и растраты, сбыта наркотиков, вменение признака «с использованием служебного положения» не мотивируют. Однако из содержания предъявленных подсудимым обвинений видно, что фактически суды руководствуются вышеприведенными Рекомендациями[3].

Квалифицирующий признак вменяется преимущественно рядовым сотрудникам организаций, которые не обладают признаками должностного лица и не наделены организационно-распорядительными или административно-хозяйственными полномочиями, за нарушения, допущенные при исполнении профессиональных обязанностей (функциональный критерий), а именно: специалисты офисов операторов связи (преимущественно «Билайн»), клиентские менеджеры банков, продавцы-консультанты, кассиры АЗС, специалисты многофункциональных центров.

---

[1] Постановление Конституционного Суда Российской Федерации от 16 июля 2015 г. № 22-П/2015. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Постановление Конституционного Суда Российской Федерации от 8 декабря 2022 г. № 53-П/2022. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Методические рекомендации по осуществлению прокурорского надзора …

Так, по одному из дел, подсудимый на основании трудового договора являясь специалистом офиса ПАО «Вымпел – Коммуникации», находясь на своем рабочем месте, используя служебный персональный компьютер, подключенный к корпоративной сети с открытой программой информационной системы «Амдокс Энсембл», используя свою учетную запись и конфиденциальный пароль, предоставленные ему для выполнения служебных обязанностей, но без письменного заявления клиента и его идентификации произвел регистрацию на вымышленные данные SIM-карт, что повлекло модификацию компьютерной информации[1].

По другому делу подсудимая, являясь сотрудником АО «Почта России», получила право доступа к базе данных АО «Почта Банк», содержащей персональные данные клиентов, информацию об операциях, о счетах и вкладах клиентов и корреспондентов и внесла в указанную базу данных полученные неустановленным способом персональные данные ранее ей незнакомой И., без ведома и согласия последней, необходимые для открытия банковского счета, тем самым модифицировав охраняемую законом компьютерную информацию[2].

Если бы, к примеру, кто-либо из указанной категории совершил присвоение или растрату, признак использования служебного положения ему нельзя было бы вменить, хотя формулировки данного квалифицирующего признака идентичны.

Анализируя положения вышеприведенных Рекомендаций В.Ф. Щепельков приходит к выводу, что отсутствие упоминания статуса субъекта восполняется указанием на содержание этого статуса, на особенности совершения преступления, характерные только для статусных лиц (должностных лиц и лиц, выполняющих управленческие функции в коммерческих и иных организациях)[3].

---

[1] Приговор Железнодорожного районного суда города Хабаровска от 25 июля 2023 г. по делу № 1-580/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Приговор Псковского городского суда Псковской области от 8 августа 2023 г. по делу № 1-512/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Щепельков В. Ф. Указ. соч.

Однако как показано выше, суды на местах не стали идти по пути системного толковая закона в связи с чем, по мнению автора настоящей статьи, пришли к неверному выводу.

Критикуя позицию судов по делам о сбыте наркотических средств, ставящих во главе исключительно функциональный критерий, М. А. Любавина справедливо обращает внимание, что в Уголовном кодексе Российской Федерации речь идет об использовании служебного положения, а не о выполнении в целом трудовых функций.

В соответствии с доктринальными определениями, отмечает ученый, служба — профессиональная деятельность определенного контингента лиц — служащих — по организации исполнения и практической реализации полномочий, государственных, общественных и иных социальных структур. Поскольку речь идет об использовании служебного, а не должностного или иного управленческого положения, специальным субъектом может выступать любой служащий, но именно служащий, а не лицо, таковым не являющееся[1].

Однако, если речь идет о служащих в негосударственном секторе, даже в доктрине возникают споры о признаках, которыми они должны обладать.

Так, А.В. Шнитенков под службой предлагает понимать «элемент организации деятельности, представляющий собой правовое отношение гражданина с физическим или юридическим лицом, на основе которого гражданин наделяется полномочиями по выполнению функций управленческого или профессионального характера»[2].

В.М. Манохин выделял два критерия отграничения службы от иной профессиональной деятельности: процесс труда и объект воздействия в процессе труда[3]. Ученый понимает под службой профессиональную деятельность опре-

[1] Любавина М. А. Квалификация преступлений, предусмотренных ст.ст. 228 и 228.1 УК РФ : учебное пособие. СПб., 2016. С. 160—162.

[2] Шнитенков А. В. Ответственность за преступления против интересов государственной службы и интересов службы в коммерческих и иных организациях. СПб., 2006. С. 15.

[3] Манохин В. М. Служба и служащий в Российской Федерации: правовое регулирование. М., 1997. С. 5–6.

деленного контингента лиц – служащих по организации исполнения и практической реализации полномочий государственных, общественных и иных социальных структур[1].

Из приведенных подходов сложно выделить какие-либо признаки служащего в негосударственном секторе, отличающего его от работника, занятого в сфере оказания услуг, и, как следствие, влекущего необходимость введения более строгой ответственности. Для решения о привлечении к уголовной ответственности — это главное условие: отсутствие четких условий должно расцениваться как невозможность уголовного преследования.

Нет никаких оснований привлекать к разной ответственности за нарушение профессиональных функций сотрудника отдела кадров, менеджера по продажам, юриста, инженера, IT-специалиста, водителя-экспедитора, маляра, поскольку сама по себе их деятельность не влияет на характер и степень общественной опасности деяния.

В связи с изложенным, следует прийти к выводу, что применительно к ст.ст. 272, 273 УК РФ в настоящее время судами допускаются ошибки при вменении квалифицирующего признака «с использованием служебного положения», поскольку субъект данных преступлений должен быть наделен организационно-распорядительными или административно-хозяйственными полномочиями, или подпадать под признаки должностного лица.

Помимо этого, анализ судебной практики показал, что преступления, подпадающие под ст. 272 или ст. 273 УК РФ идеальную совокупность со ст. 285 УК РФ не образуют, что нельзя сказать про ст. 286 УК РФ.

Так, подсудимая, являясь оперуполномоченной полиции, находясь на рабочем месте, лично, посредством автоматизированного рабочего места (компьютера), подключенного к ИБД ИЦ УМВД России по Новгородской области, ввела выделенный ей логин и пароль доступа, ввела запросы о субъектах персональных данных, получив на экране монитора компьютера информацию о персональных данных нескольких лиц, которую передала третьим лицам для

[1] Там же. С. 9.

ознакомления и копирования. Действия оперуполномоченной были квалифицированы по ч. 5 ст. 33, ч. 3 ст. 272 УК РФ[1].

Однако, в правоприменении встречается и другой подход к квалификации. Например, Василеостровский районный суд г. Санкт-Петербурга, рассмотрев резонансное дело о предоставлении служебной информации, установил, что Голубев, занимая должность оперуполномоченного, с помощью своего сослуживца, неосведомленного о преступном умысле и будучи уверенным, что Голубев действует в интересах службы, получил доступ к системе «Розыск-Магистраль». Таким образом, Голубев заполучил персональные данные пассажиров двух авиарейсов, а затем передал их третьему лицу. Действия Голубева были квалифицированы по ч. 1 ст. 285 УК РФ[2].

При превышении должностных полномочий подход к квалификации иной. Так, осужденный, используя свою должность государственного инспектора дорожного надзора, незаконно внес в электронную карточку административного материала в отношении Н, ложные сведения о начале течения срока лишения специального права, не сдавшего водительское удостоверение и не обращавшегося с заявлением о его утрате в установленном законом порядке. Подобные действия были квалифицированы по ч. 3 ст. 272 УК РФ и ч. 1 ст. 286 УК РФ[3].

Таким образом, действующее правовое регулирование требует единого подхода при трактовке квалифицирующего признака использование служебного положения;

Если отсутствуют разъяснения Пленума Верховного Суда Российской Федерации нижестоящие суды отдают предпочтение функциональному критерию, через который раскрывается использование служебного положения, забывая о статусном, что, по мнению автора работы, приводит к неверной квалификации.

---

[1] Приговор Новгородского районного суда Новгородской области от 27 февраля 2023 г. по делу № 1-66/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Петербургский полицейский отправится в колонию за слив личных данных граждан // Санкт-Петербург : сайт. URL: https://tvspb.ru/news/2023/03/2/peterburgskij-policzejskij-otpravitsya-v-koloniyu-za-sliv-lichnyh-dannyh-grazhdan (дата обращения: 23.11.2023).

[3] Приговор Россошанского районного суда Воронежской области от 23 января 2023 г. по делу № 1-7/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

Преступления, совершаемые с использованием служебного положения, могут совершаться путем должностного злоупотребления, что не требует дополнительной квалификации по ст. 285 УК РФ. Если в действиях должностного лица будут содержаться признаки превышения полномочий, то имеет место совокупность преступлений ч. 2 ст. 272 УК РФ или ч. 2 ст. 273 УК РФ и ст. 286 УК РФ.

УДК 343

А. Э. ПОБЕГАЙЛО

УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, РАСПРОСТРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Понятие «вредоносное компьютерная программа» известно российскому уголовному праву достаточно давно. Статья 273 УК РФ была включена еще в первую редакцию УК РФ (от 13.06.1996 г). В первоначальной редакции название статьи звучало как: «Создание, использование и распространение вредоносных программ для ЭВМ». Редакция от 13.06.1996 г. включала в себя основной и квалифицированный составы.

Основной состав включал в себя несколько альтернативных действий: создание программ для ЭВМ, внесение изменений в существующие программы, а равно за распространение таких программ или машинных носителей с такими программами, при условии, что их основной функцией являлось несанкционированное уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Указанный функционал должен был быть заведомо известен субъекту преступления.

Квалифицированный состав, в отличии от основного, являвшейся формальной, была материальной, и предусматривала более суровое наказание за вышеуказанные деяния, совершение которых повлекло за собой тяжкие последствия. При этом норма предусматривала ответственность только за неосторожную форму вины, в рамках формулировки ч. 2 ст. 273 УК РФ: «Те же

деяния, повлекшие по неосторожности тяжкие последствия». Такая формулировка подвергалась обоснованной критике научного сообщества.

Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» внес существенные изменения в текст статьи и сущность самой нормы.

В кодекс было введено понятие предмета преступлений, предусмотренных главой 28 УК РФ — компьютерной информации. Под данным понятием понимались «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Также было определено понятие крупного ущерба в рамках данной главы — ущерб, сумма которого превышает один миллион рублей.

В рамках диспозиции ст. 273 УК РФ появилось также описание такого средства совершения преступления, как «иная компьютерная информация», которую законодатель не конкретизировал.

Претерпел некоторые изменения признак «заведомости», представляющий собой особый технический прием, применяемый для характеристики субъективной стороны преступления. В рамках него презюмировалось, что противоправные действия, совершаемые посредством вредоносных компьютерных программ, совершаются умышленно, и должны быть направленны на определенные преступные цели – а именно уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализации средств защиты компьютерной информации. Из перечисленных целей, нейтрализация была введена законодателем впервые.

Несмотря на данные изменения, правоприменители продолжали сталкиваться с рядом трудностей. Так, например, понятия «вредоносная компьютерная программа» и «иная компьютерная информация» не были закреплены ни в рамках примечания к ст. 273 УК РФ, ни в рамках Постановления Пленума Верховного Суда Российской Федерации.

Кроме того, на практике возникали вопросы квалификации ряда однородных действий с использованием вредоносных компьютерных программ как отдельных эпизодов, или же единого продолжаемого преступления. Не урегулированными оставались вопросы квалификации формального выполнения объективной стороны данного состава в рамках образовательной деятельности, трудовой деятельности по защите информации и иных общественно-полезных видах деятельности.

Проблемами, не решенными в рамках изменений, внесенных в Уголовный кодекс Российской Федерации, Федеральным законом 07.12.2011 № 420-ФЗ оставались:

1. Отсутствие закрепления понятий «вредоносная компьютерная программа» и «иная компьютерная информация» как в самой норме, так и в рамках примечания к УК РФ.

2. Не были решены возникающие на практике вопросы квалификации ряда однородных действий с использованием вредоносных компьютерных программ (например, нескольких эпизодов неправомерного доступа к охраняемой законом компьютерной информации, даже объединенных общим умыслом и местом совершения преступления) как отдельных эпизодов, или же как единого продолжаемого преступления.

3. Не были урегулированы вопросы квалификации формального выполнения объективной стороны ст. 273 УК РФ в рамках образовательной деятельности, трудовой деятельности по защите информации и иных общественно-полезных видах деятельности.

4. Вопросы, связанные с квалификацией малозначительности деяний, предусмотренных гл. 28 УК РФ также не были разрешены.

15 декабря 2022 г. Пленум Верховного Суда Российской Федерации принял Постановление «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», разъяснившее

ряд проблемных вопросов квалификации преступлений в сфере компьютерной информации.

Положительно оценивая разъяснения ряда спорных и неясных аспектов, предложенные Верховным Судом, необходимо при этом отметить, что далеко не все из данных аспектов были разрешены, а равно сами разъяснения не свободны от дискуссионных положений.

Например, понятие компьютерного устройства, вынесенное по аналогии с понятием «компьютерная информация» было определено как «любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов», что, на наш взгляд, является чрезмерным расширением понятия.

Уточнено понятие охраняемой законом компьютерной информации, в качестве ее признаков закреплены: а) установление специального режима правовой защиты; б) ограничение доступа; в) отнесения ее к сведениям, составляющим различные виды тайн (личную, семейную, служебную, и др.). При этом эти признаки не раскрыты, что составляет определенные трудности квалификации таких преступлений, особенно касающиеся «ограничения доступа к информации».

Определено понятие компьютерной программы, приведенное в соответствие положениями ст. 1261 ГК РФ, как: «представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения».

Данное определение не учитывает разницу в общественной опасности между исполняемой программой и ее исходным кодом, а равно уравнивает приготовление к совершению преступления, предусмотренного ст. 273 УК РФ (написание исходного кода) и приведение ее в исполняемый вид (собственно создание).

Были конкретизированы преступные последствия в отношении охраняемой законом компьютерной информации, предусмотренные ст.ст. 272, 274, 274.1 и преступные цели ст. 273 УК РФ, а именно: а) уничтожение, б) блокирование, в) модификация, г) копирование и д) нейтрализация средств защиты.

Безусловно положительно оценивая попытку такой дефиниции, необходимо отметить, что она не лишена проблемных аспектов. Так, например, копирование компьютерной информации указанное Постановление Пленума трактует чрезмерно широко, при этом само определение выбивается при этом из остальных преступных последствий.

Согласно этой дефиниции, простая зарисовка изображения, находящегося на экране компьютерного устройства от руки, или же его фотографирование уже составляет преступление, предусмотренное ст. 272 УК РФ. На наш взгляд, данное преступление может быть совершено только цифровыми средствами, а копирование информации аналоговым способом должно быть квалифицированно по иным статьям (например, ст.ст. 137, 138, 183, 275, 276 УК РФ и др.).

В рамках определения средства нейтрализации защиты компьютерной информации Пленум предусматривает любое воздействие на средства защиты информации от несанкционированного доступа, но при этом не рассматривает подробно ни понятие санкционированного доступа, ни характер такой информации. Между тем в рамках использования компьютерных устройств многие программы, не являющиеся вредоносными, могут подпасть под данное определение (например, эмуляторы игровых консолей, HEX-редакторы, и многие другие программы).

Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» определяет как

иную компьютерную информацию, заведомо предназначенную для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в ч. 1 ст. 273 УК РФ.

По нашему мнению, определение иных сведений как «любых сведений» является чрезмерно расширительным, так как под него подпадают не только, например, ключи доступа, но и, например, последовательность действий, выполняя которую лицо может обойти защиту компьютерной информации, включая, например, как сведения по использованию программатора, так и сведения по нажатию определенных клавиш при загрузке программы, для, например, установки Root-прав на смартфон.

Полагаем, что такая информация должна содержаться в цифровом виде, как, например, эксплойты, скрипты и т. д., а иные действия следует квалифицировать по другим составам.

Момент окончания преступления, предусмотренного ст. 273 УК РФ действующим Постановлением Пленума определено как: «создание части (фрагмента) кода вредоносной компьютерной программы, позволяющего осуществить неправомерный доступ к компьютерной информации. В таком случае, если еще не было завершено создание вредоносной компьютерной программы, действия лица подлежат квалификации как создание иной вредоносной компьютерной информации».

Таким образом, даже если лицо еще не закончило создание вредоносной программы, а лишь написало несколько строк кода, который при этом еще даже не является исполняемым, преступление уже считается оконченным.

В данном случае, в рамках создания вредоносных компьютерных программ, исследуемое Постановление Пленума фактически трактует состав в части создания вредоносных программ и иной компьютерной информации как усеченный, что, на наш взгляд, уравнивает общественную опасность от работающей вирусной программы и нескольких строк исходного кода, что не соответствует ни принципу справедливости, ни гуманизма.

Распространение вредоносных компьютерных программ Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» определяет как: «предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом».

При этом в данном Постановлении Пленума Российской Федерации не разграничивается умышленное, неосторожное и невиновное распространение таких программ, которое, учитывая их свойства, может происходить без ведома пользователя, и, таким образом, повлечь за собой объективное вменение, поскольку ст. 273 УК РФ предусматривает умышленную форму вины.

В данном Постановлении Пленума Российской Федерации разъяснено, что создание, использование или распространение вредоносных компьютерных программы, использующихся в образовательных и иных общественно-полезных целях не образует состава преступления. Это является большим шагом вперед по противодействию объективному вменению в данной сфере, но при этом вопросы малозначительности таких деяний, так и не были Постановлением Пленума решены.

Необходимо обратить внимание, что общее количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации за период 2019— сентябрь 2023 года увеличилось с 294 409 до 489 044 преступлений.

При этом темпы прироста преступлений данной группы за рассматриваемый период времени снизились с +68,5 в 2019 году до +29,2 за девять месяцев 2023 года.

Общее количество зарегистрированных преступлений, предусмотренных ст. 273 УК РФ период 2019—сентябрь 2023 года снизилось с 455 (−37,9 %) в 2019 году до 109 (−36,6 %) за девять месяцев 2023 года.

При этом доля преступлений, предусмотренных ст. 273 УК РФ в общей структуре преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации за рассматриваемый период времени снизилось с 0,15 % в 2019 году до 0,02 % за девять месяцев 2023 года.

Оценку латентности создания, распространения и использования вредоносных компьютерных программ и иной компьютерной информации дать достаточно сложно, исследователям приходится сопоставлять для этого ряд независимых характеристик.

Так, например, ведущим производителем антивирусного программного обеспечения в Российской Федерации является Лаборатория Касперского, которая ежегодно выпускает доклады, касающиеся инцидентов компьютерной безопасности и общего состояния в данной сфере.

В своем докладе за 2022 год, в частности, компания приводила данные, согласно которым антивирусом компании было зафиксировано 101 612 333 уникальных вредоносных URL, 109 183 489 уникальных вредоносных объектов было заблокировано[1].

Согласно тому же отчету, Россия находилась на пятом месте в мире по числу атакованных пользователей[2]. Компания CyberProof, официальный член Ассоциации информационной безопасности Майкрософт, в своем отчете за 2022 год приводила данные, согласно которым Россия являлась источником 2,4% кибератак в мире[3].

При этом необходимо учитывать, что атаки могли вестись через VPN, с использованием VPS и иных способов обфускации точки выхода, а равно оценки иностранных компаний достаточно давно могут являться политически мотивированными.

---

[1] Kaspersky Security Bulletin 2022. Статистика // SECURELIST : сайт. URL: https://securelist.com (дата обращения: 11.11.2023).

[2] Там же.

[3] Which Countries are Most Dangerous? Cyber Attack Origin — by Country // CyberProof : сайт. URL: https://blog.cyberproof.com/blog/which-countries-are-most-dangerous (дата обращения: 11.11.2023).

Но даже учитывая эти факторы, видна существенная разница между количеством зарегистрированных преступлений, предусмотренных ст. 273 УК РФ, и количеством зарегистрированных киберугроз.

По мнению А.Н. Попова, компьютерная преступность практически не находит своего отражения в официальной статистике, мы полностью согласны с данной научной позицией[1].

И.М. Рассолов оценивает латентность киберпреступлений в России в 90 %[2]. Данная оценка представляется нам, по отношению к ст. 273 УК РФ, несколько заниженной. Тем не менее, большинство исследователей сходятся во мнении, что латентность киберпреступности в России крайне высока.

Таким образом, представляется, что противодействие киберпреступности в настоящее время связано с рядом трудностей, как уголовно-правового, так и криминологического характера. На наш взгляд, основным проблемным аспектом, так и не решенным ни Постановлением Пленума Верховного Суда Российской Федерации, ни законодателем — является вопрос малозначительности деяния, предусмотренного ст. 273 УК РФ.

В частности, в условиях наложенных на нашу страну санкций, представляется, что использование средств модификации или нейтрализации средств защиты компьютерной информации в отношении иностранного ПО, ушедшего с Российского рынка, не соответствует ни принципу справедливости, ни здравому смыслу.

Официальная статистика показывает высокие темпы роста преступлений, связанных с использованием информационно-телекоммуникационных технологий, но при этом количество дел, возбужденных по ст. 273 УК РФ остается весьма небольшим. Большинство экспертов и ученых в качестве причины такого небольшого, и при этом уменьшающегося, процента выявленных преступных деяний, указывают как на естественную, так и на искус-

[1] Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб., 2018. С. 12.

[2] Рассолов И. М. Право и Интернет. Теория кибернетического права : монография. 3-е изд., доп. М., 2022. 304 с.

ственную латентность. К факторам, влияющим на нее, являются и недостаточное финансирование структур МВД, занимающихся борьбой с киберпреступлениями, что не позволяет набрать достаточное число квалифицированных специалистов в области информационно-телекоммуникационных технологий, и правовой нигилизм населения, неверие в деятельность правоохранительных органов, а равно объективные технические сложности с выявлением таких преступлений и фиксацией цифровых доказательств.

Важнейшим (и нерешенным) вопросом остается общесоциальная и специальная криминологическая профилактика.

Просвещение населения, сотрудничество правоохранительных органов с производителями антивирусного программного обеспечения, повышение доверия населения по отношению к сотрудникам полиции, Следственного комитета и прокуратуры, эффективное межведомственное взаимодействие, а равно решительные действия по нейтрализации детерминантов киберпреступности и ее латентности является первоочередной задачей для России на современном этапе.

УДК 343

А. А. РАДЧЕНКО

НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ ОСНОВ КОНСТИТУЦИОННОГО СТРОЯ И БЕЗОПАСНОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В современных условиях обострения геополитической обстановки вопросы уголовной ответственности за преступления против основ конституционного строя и безопасности государства, приобретают важное прикладное значение.

Так, необходимо констатировать, что вектор уголовно-правовой политики противодействия преступности в условиях СВО в кратчайшие сроки был изменен в направлении учета текущей ситуации.

Следует отметить, что законодатель оперативно решил вопросы криминализации и пенализации новых преступных деяний, которые можно разделить на несколько групп: связанных с ведением самих военных действий; с совершением других преступлений, связанных с обеспечением условий осуществления СВО; а также объявленной 21.09.2022 частичной мобилизацией[1].

В частности, одним из проявлений указанной тенденции является установление федеральным законом от 14 июля 2022 г. № 260-ФЗ уголовной ответственности за «сотрудничество на конфиденциальной основе с иностранным государством, международной либо иностранной организацией» (ст. 275.1 УК РФ).

Включение в уголовный закон указанного состава преступления в некоторой степени разрешило имеющеюся дискуссию по поводу момента окончания государственной измены в форме «иного оказания помощи»[2], который трактовался некоторыми специалистами как вступление в «контакт (сговор) с представителем иностранной стороны»[3]. Однако указанная новелла породила новые проблемы, обусловленные неоднозначным толкованием конструктивных признаков указанного состава преступления.

Общественная опасность рассматриваемого преступного деяния заключается в том, что оно делает возможным создание подпольной сети конфидентов иностранных разведок, в том числе так называемых «спящих ячеек», готовых оказать всестороннюю помощь враждебным странам в подрыве безопасности

---

[1] Репецкая А. Л. Специфика политики противодействия преступности в условиях осуществления СВО // Актуальные проблемы политики противодействия преступности : материалы Всероссийской научно-практической конференции (г. Иркутск, 27 сентября 2022 г.). Иркутск, 2023. С. 59—63.

[2] Дьяков С. В. Преступления против основ конституционного строя и безопасности государства : уголовно-правовое и криминологическое исследование. СПб., 2009. С. 44 ; Преступления против основ конституционного строя и безопасности государства. Комментарий к главе 29 УК РФ : с постатейным приложением нормативных актов и документов / [А. Ю. Шумилов]. М., 2001. С. 19 ; Энциклопедия уголовного права. В 35 т. Т. 26. Преступления против основ конституционного строя и безопасности государства / Е. Пономоренко, А. Кулев, И. Яцута [и др]. СПб., 2015. С. 140—142.

[3] Рябчук В. Н. Государственная измена и шпионаж : уголовно-правовое и криминологическое исследование. СПб., 2007. С. 727, 855—858 ; Царев В. Д. Общее понятие и признаки преступлений против основ конституционного строя и безопасности государства России : дис. … канд. юрид. наук. Иваново, 2005. С. 168.

России[1]. Фактические указанное деяние можно рассматривать как приготовление к государственной измене, которое законодателем в настоящее время «возведено» в самостоятельный состав преступления[2].

При этом иностранными специальными службами проводиться активная и фактически открытая работа по привлечению граждан России к сотрудничеству в ущерб национальной безопасности, в т. ч. с использованием дистанционных способов через информационно-телекоммуникационные сети.

Так, в мае 2023 года ЦРУ США создало Telegram-канал для вербовки россиян и разместило в нем пропагандистский видеоролик. В частности, в материале содержится инструкция по связи с ЦРУ через скрытые сервисы в браузере «Tor».

Подчеркивается, что американское разведывательное ведомство интересует информация «об экономике или высшем руководстве Российской Федерации»[3]. Также эксперты в области информационных технологий и отмечают, что «основная вербовка россиян самых разных возрастов сегодня идет через соцсети, где для этого есть все условия»[4].

В этой связи встает комплекс вопросов об уголовно-правовой оценке действий как лиц, размещающих указанную информацию в информационно-телекоммуникационных сетях, так и лиц, откликающихся на указанные призывы, а также так называемых инициативников — лиц, самостоятельно проявляющих инициативу к вступлению в контакт с иностранными спецслужбами с использованием современных информационных технологий.

Для начала необходимо рассмотреть объективные признаки состава преступления, предусмотренного ст. 275.1 УК РФ. В соответствии с диспозицией

---

[1] Власенко В. В. Конфиденциальное сотрудничество с иностранным государством: условия привлечения к ответственности // Уголовный процесс. 2023. № 7. С. 49.

[2] Пономаренко Е. В., Копшева К. О. Обоснованность изменений уголовного законодательства, касающихся отдельных составов преступлений против основ конституционного строя и безопасности государства // Правовая политика и правовая жизнь. 2023. № 1. С. 124—125.

[3] ЦРУ создало Telegram-канал для вербовки россиян // LENTA.RU : сайт. URL: https://lenta.ru/news/2023/05/16/cia/ (дата обращения: 29.10.2023).

[4] LIFE : сайт. URL: https://life.ru/p/1471891 (дата обращения: 11.11.2023).

уголовно-правовой нормы преступление является сложносоставным, т. к. деяния состоит из двух обязательных и взаимосвязанных действий: установления и поддержания гражданином Российской Федерации отношений сотрудничества на конфиденциальной основе с представителем иностранного государства, международной либо иностранной организации в целях оказания им содействия в деятельности, заведомо направленной против безопасности Российской Федерации.

При этом диспозиция имеет также отсылочный характер за счет указания на отсутствие в указанных действиях признаков преступления, предусмотренного ст. 275 УК РФ.

Рассматриваемое деяние следует признать оконченным лишь при совершении обоих указанных в диспозиции действий. При этом как установление сотрудничества на конфиденциальной основе, так и поддержание конфиденциальных отношений, может происходить с использованием информационно-телекоммуникационных сетей.

С учетом рассмотренных особенностей состава преступления, предусмотренного ст. 275.1 УК РФ, проведем анализ некоторых возможных ситуаций и соответствующих вариантов квалификации преступных деяний.

Так, российский гражданин откликается на обращение иностранных спецслужб в сети «Интернет» и с использованием предложенных алгоритмов конфиденциальности направляет информацию о своем желании сотрудничать с представителями зарубежных организаций, но ответа не получает.

Представляет, что в данном случае действия гражданин России возможно квалифицировать как покушение на сотрудничество на конфиденциальной основе (ч. 3 ст. 30 и ст. 275.1 УК РФ), т. к. лицо непосредственно приступило к выполнению объективной стороны указанного состава, но не смогло его довести до конца по независящим от него обстоятельствам.

При этом не имеет значения по каким причинам не получен ответ иностранной стороны: предложение от российского гражданина не дошло до ад-

ресата из-за технических проблем или сбоев, личность россиянина или предлагаемая им помощь не представили интереса или иностранная спецслужба заподозрила «подставу» с российской стороны.

Основными моментами является направленность умысла на установление и поддержание конфиденциального сотрудничества в деятельности, заведомо направленной против безопасности Российской Федерации, и совершение конкретных действий по реализации указанного намерения.

Представляется, что аналогичная уголовно-правовая оценка должна применяться и в случае получения гражданином России отказа от иностранной стороны, т.к. в данном случае виновный принял все зависящие от себя меры по совершению преступления, которое не было доведено до конца по не зависящим от этого лица обстоятельствам.

Особый интерес и сложность вызывает квалификация деяния при получении российским гражданином положительного ответа от иностранной стороны с использованием информационно-телекоммуникационных сетей.

В данном случае возникает целый ряд взаимосвязанных вопросов: «С какого момента считать конфиденциальное сотрудничество установленным?»; «Что включает поддержание таких отношений, необходимое для признания оконченным преступления, предусмотренного ст. 275.1 УК РФ?»; «Как соотноситься поддержание конфиденциального сотрудничества и непосредственное выполнение заданий иностранной стороны?».

Представляется, что установление сотрудничества предполагает не просто выражение желания обоих сторон, но включает определение и закрепление его основных параметров (например, возмездная или безвозмездная основа, направления и сферы предполагаемого осуществления деятельности, направленной против безопасности России, определение дальнейших конспиративных способов связи, в т. ч. с использованием информационно-телекоммуникационных сетей).

В свою очередь, поддержание отношений сотрудничества охватывает дальнейшие развитие конспиративных контактов (т. н. «поддержание связи») в целях проведения деятельности в ущерб безопасности России (например,

прохождения российским гражданином, в т. ч. дистанционным способом, инструктажей и обучения, получение шпионских заданий и рекомендаций по сокрытию своей преступной деятельности и т. д.).

Очевидно, что в силу отсылочной конструкции диспозиции ст. 275.1 УК РФ, если в рамках поддержания сотрудничества с использованием информационно-телекоммуникационных сетей происходит передача иностранной стороне секретной информации или иных сведений, которые могут использоваться против безопасности России, а также оказании помощи в деятельности, направленной против безопасности Российской Федерации (например, подбор через сеть «Интернет» квартир для размещения агентуры или мест для проведения «акций по связи», осуществляются переводы собранных денежных средств и т. д.), указанные действия подпадают под состав государственной измены (ст. 275 УК РФ) и полностью ей охватываются, и не подлежат дополнительной квалификации по ст. 275.1 УК РФ[1].

Таким образом, происходит «перерастание» установление и поддержания конфиденциального сотрудничества (как фактическое приготовительной деятельности) в непосредственное совершение конкретных форм государственной измены.

При этом требуют уголовно-правовой оценки и действия представителей иностранной стороны по установлению и поддержанию конфиденциального сотрудничества с российскими гражданами в целях деятельности, заведомо направленной против безопасности Российской Федерации.

В этой связи необходимо поддержать концептуальную мысль о том, что государственная измена является «своеобразной формой соучастия гражданина нашей страны с внешним противником в проведении деятельности против собственного государства»[2].

---

[1] Власенко В. В. Указ. соч. С. 52. Однако некоторые специалисты указывают на наличие в данном случае идеальной совокупности и возможности одновременного вменения ст. 275 и ст. 275.1 УК РФ (Пономаренко О. В., Копшева К. О. Указ. соч. С. 125).

[2] Энциклопедия уголовного права ... Т. 26. С. 139—140.

Следовательно, для правильной квалификации необходимо четко установить взаимосвязи и взаимообусловленность деятельности российских граждан и представителей иностранной стороны в ущерб безопасности Российской Федерации.

Поэтому установление и поддержание сотрудничества с российским гражданином, с одной стороны, можно расценивать как приготовление (ч. 1 ст. 30 УК РФ) к шпионажу (ст. 276 УК РФ) или иным преступлениям против безопасности (например, диверсии ст. 281 УК РФ), а, с другой стороны, как деятельность организатора или подстрекателя российского гражданина к совершению деяния, предусмотренного ст. 275.1 УК РФ.

Представляется, что ключевым моментом для квалификации деяний представителей иностранной стороны должна выступать направленность умысла, т.к. фактически установление и поддержание сотрудничества выступает для зарубежных спецслужб лишь способом проведения деятельности в ущерб безопасности России, которая подлежат конкретной уголовно-правовой оценке.

В этой связи, представляется, что размещение в информационно-телекоммуникационных сетях абстрактных призывов к сотрудничеству и оказанию помощи иностранным спецслужбам не подпадает под признаки уголовно-наказуемый деяний, запрещенных действующим УК РФ, и лишь в случае перехода в форму действий по использованию россиян в определенных формах «враждебной деятельности» может быть оценено сквозь призму конкретного состава преступления, в т. ч. формате организатора или подстрекателя.

Кроме того, представляется, что предупредительно-профилактическая функция ст. 275.1 УК РФ направлена именно на граждан России (в частности, исходя из субъекта преступления), т.к. иностранные спецслужбы независимо от геополитических условий всегда проводили и будут проводить разведывательную деятельность, в т. ч. с привлечением конфидентов.

УДК 343

А. В. РЕЗЦОВ

ПРОТИВОДЕЙСТВИЕ ДИСТАНЦИОННОМУ ХИЩЕНИЮ ДЕНЕЖНЫХ СРЕДСТВ: ОБМЕН ОПЫТОМ, ОЦЕНКИ И ТЕНДЕНЦИИ

Общественная жизнь сегодня характеризуется ускорением процессов во всех ее сферах, в первую очередь — в сфере обмена информацией. Активно развиваются новые формы такого обмена — цифровые средства и электронные ресурсы. Данные процессы несут в себе риск потери информации, утраты доступа к ней или, напротив, получения несанкционированного доступа лицами с противоправными установками поведения, которыми совершаются преступления с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Для координации деятельности правоохранительных органов и повышения эффективности работы в указанной сфере Генеральным прокурором Российской Федерации поддержана инициатива Северо-Западного банка ПАО Сбербанк, дано поручение о проведении на площадке управления Генеральной прокуратуры Российской Федерации по Северо-Западному федеральному округу форума «Противодействие и профилактика несанкционированных операций по переводу денежных средств с банковских счетов, совершенных с использованием электронных средств платежа», который состоялся 08.11.2023 в Санкт-Петербурге[1]. Этот форум не являлся единственным, ранее аналогичное мероприятие прошло в Дальневосточном федеральном округе[2].

Актуальность обсуждаемой темы отметила во вступительном слове начальник управления Генеральной прокуратуры Российской Федерации по Северо-Западному федеральному округу Н.Е. Солнышкина, указав на рост в течение нескольких лет преступлений ИТТ в России (2018 г. – 174 674;

[1] Управление Генеральной прокуратуры Российской Федерации по Северо-Западному федеральному округу : сайт. URL: https://epp.genproc.gov.ru/web/proc_szfo/mass-media/news?item=91385579 (дата обращения: 28.10.2023).

[2] Там же. URL: https://epp.genproc.gov.ru/web/proc_dvfo/mass-media/news?item=87034500 (дата обращения: 28.10.2023).

2022 г. – 522 065), большую часть из которых составляют преступления, предусмотренные статьей 159 УК РФ (2018 г. – 90 664 или 51,9 % от общего количества преступлений ИТТ; 2022 г. – 249 984 или 47,8 %).

По итогам января-октября 2023 г. количество зарегистрированных в России преступлений ИТТ по сравнению с аналогичным периодом прошлого года возросло на 30,7 % и составило 561 203, в том числе на 44,1 % до 291 889 возросло количество преступлений, предусмотренных статьей 159 УК РФ; в Северо-Западном федеральном округе зарегистрировано на 27,5 % больше преступлений ИТТ (60 437), в том числе на 42,2 % больше (33 688) преступлений, предусмотренных статьей 159 УК РФ.

Иная динамика характерна для входящих в преступления с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации краж (ст. 158 УК РФ) и мошенничеств с использованием электронных средств платежа (ст. 159.3 УК РФ).

Их рост на территории Российской Федерации имел место в 2018-2020 гг. и достиг показателя в 173 416 и 25 820 преступлений, соответственно. Далее отмечается последовательное снижение зарегистрированных в Российской Федерации краж с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации с 156 792 в 2021 г. до 100 600 – за 10 месяцев 2023 г., мошенничеств с использованием электронных средств платежа с 10 258 в 2021 г. до 3 656 – за 10 месяцев 2023 г.

Несмотря на внесение 15.12.2022 изменений в постановление Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» о квалификации по статье 158 УК РФ хищений с банковских карт с использованием конфиденциальной информации, полученной от владельца путем обмана или злоупотребления доверием, роста таких преступлений не отмечается.

Увеличение количества одних преступлений и одновременное уменьшении других указывают на сложную структуру преступлений с использованием

информационно-телекоммуникационных технологий или в сфере компьютерной информации, наличие различных, не связанных между собой факторов, обуславливающих такую динамику.

Советник заместителя Председателя Центрального Банка Российской Федерации Д.В. Корякин привел данные о предотвращении в первом полугодии 2023 г. свыше 9,3 млн попыток банковских операций без согласия клиентов на сумму свыше 1,6 трлн руб. (1 623,13 млрд руб.). Он указал на увеличение количества и сумм таких операций, в том числе среднего чека хищения. Об усилении противодействия растущей криминальной активности свидетельствует увеличение за указанный период количества ходатайств о блокировке доменов в сети «Интернет» до 16 355 и телефонных номеров – до 373 691.

Им сообщено о внесении изменений в Федеральные законы «О банках и банковской деятельности» (от 02.12.1990 № 395-1) и «О национальной платежной системе» (от 27.06.2011 № 161-ФЗ).

С 21.10.2023 вступили в силу положения об информационном обмене между МВД России и Банком России посредством технологической инфраструктуры последнего – автоматизированной системы обработки инцидентов ФинЦЕРТ.

Вводится так называемый «период охлаждения», снижающий оперативность банковских операций, осуществленных без добровольного согласия клиентов. Банк России устанавливает признаки, формирует и ведет базу данных таких операций. На основании этой информации операторы по переводу денежных средств уполномочены приостанавливать действие электронных средств платежа.

Возобновление операций возможно после исключения сведений из базы данных на основании заявления лица или оператора по переводу денежных средств, предусмотрена судебная процедура обжалования отказа в удовлетворении заявления.

Кроме того, при наличии признаков совершения операции без согласия клиента оператор по переводу денежных средств обязан осуществить проверку до их списания, для чего операция приостанавливается на срок до

2 дней, а от клиента получается дополнительное подтверждение на ее совершение. Указанные изменения вступают в силу с 25.07.2024.

Начальник Центра расследования киберпреступлений Департамента по мошенничествам ПАО Сбербанк Д.Д. Савенкова привела сведения об опыте противодействия дистанционным хищениям средств клиентов.

По ее данным, ситуационными центрами информационной безопасности в день регистрируются 400 млрд событий кибербезопасности, 40 атак в день на финансовые сервисы банка, более 60 атак на банковскую инфраструктуру, около 20 тысяч попыток мошенничества (за 2022 г. — 5 млрд), фиксируется отправка свыше 60 тысяч фишинговых писем, анализируется более 4 тысяч сообщений о продаже банковской информации.

Для противодействия клиентам, принимающим на свои счета похищенные денежные средства, на контроль взяты 580 тыс. реквизитов банковских карт, отклонено 119 тыс. попыток их выпуска или выдачи, в результате предотвращен вывод средств на сумму 2 млрд руб., а доля карт клиентов, вовлеченных в принятие похищенных денежных средств, снизилась с 55 % в 2021 г. до 15 % — в 2023 г.

На фоне увеличения объема операций с денежными средствами одновременно изменились способы совершения указанных преступлений: возросло количество преступлений, совершенных методами «социальной инженерии», при этом с 22 % до 1 % сократилось количество преступлений, совершенных с применением вирусного программного обеспечения (данные тенденции соотносятся с результатами анализа основных показателей уголовно-правовой статистики, приведенными в начале настоящей работы).

В 2020 г. похищались сбережения граждан, в 2021 г. к ним добавились кредитные денежные средства, которые составили 25 % от похищенного, в 2022 г. – жилые помещения, каждая сотая жертва лишилась единственного жилья, в 2023 г. – граждане оказались вовлечены в совершение актов терроризма.

Отметим, что данные представителей банковского сообщества существенно расходятся между собой и явно превосходят статистику регистриру-

емых преступлений ИТТ. Оценки ПАО Сбербанк противоречивы – при совершении в день 20 тыс. попыток банковских операций без согласия клиентов за год их число должно составить около 7,3 млн; если же взять за основу 5 млрд таких операций за 2022 г., то в день должно совершаться около 13,6 млн попыток операций без согласия клиента.

В этой связи преждевременно утверждать, что приведенные показатели объективно характеризуют латентную составляющую экономической преступности. Они существенно больше результатов, например, надзорной деятельности прокуроров, которыми в 2022 г. поставлено на учет 136 048 преступлений всех категорий, ранее известных, но по разным причинам не учтенных[1], из них к мошенничествам в сфере информационно-телекоммуникационных технологий или в сфере компьютерной информации относится примерно каждое десятое (см.: Информационное письмо Генеральной прокуратуры Российской Федерации от 3 ноября 2023 г. № 69-09-2023/Иф11745-23).

Вряд ли правоохранительные органы с учетом численности сотрудников справятся с анализом указанных 5 млрд инцидентов традиционными методами – для этого не хватит штатного состава МВД России, насчитывающего менее миллиона человек[2]. Вместе с тем, указанный массив данных объективно существует, его изучение необходимо.

Практикой выработаны способы обработки большого объема данных в автоматическом режиме, которые могут быть заимствованы: в 2022 г. возбуждено 183,6 млн дел об административных правонарушениях по результатам применения систем фотовидеофиксации[3]. Подобный подход позволит

---

[1] Основные результаты прокурорской деятельности за январь—декабрь 2022 года // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https:// epp.genproc.gov.ru /web/gprf/activity/statistics/office/result/&item=85327980 (дата обращения: 11.11.2023).

[2] Об установлении предельной штатной численности органов внутренних дел Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2022 г. № 878. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Правоприменительная деятельность в области безопасности дорожного движения в 2022 году : информационно-аналитический обзор / К. С. Баканов, П. В. Ляхов, М. М. Исаев [и др.]. М., 2023. С. 10.

выяснить относимость банковских сведений к латентной части экономических преступлений.

Реакции правоохранительных органов на увеличение «телефонных мошенничеств» посвятил свое выступление первый заместитель прокурора г. Санкт-Петербурга В. В. Винецкий.

Он указал, что прокурорами на основании установленных при расследовании уголовных дел фактов использования преступниками подменных телефонных номеров решается вопрос о возбуждении дела об административном правонарушении по ч. 2 ст. 13.2.1 КоАП РФ: за истекший период 2023 г. возбуждено 43 таких дела, в 2022 г. — 5 дел.

По результатам судебного рассмотрения вынесено 9 решений о привлечении операторов связи к административной ответственности в виде штрафов и предупреждений.

Обращено внимание, что операторы сотовой связи в неограниченном количестве продают компаниям-посредникам сим-карты, которые сбываются мошенникам и используются для вывода денежных средств, похищенных у потерпевших. В этой связи предложено введение законодательного регулирования продажи операторами сотовой связи сим-карт, например, обязательного лицензирования деятельности организаций, покупающих сим-карты.

Выступающим охарактеризована практика применения прокуратурой г. Санкт-Петербурга положений статьи 45 ГПК РФ — обращения в суды с исками о взыскании неосновательного обогащения с третьих лиц, принимающих на свои карты от потерпевших денежные средства и пересылающих их «по цепочке».

Подготовлено 33 иска, заочными решениями Ленинского районного суда г. Мурманска взыскано 751 тыс. руб., Ново-Савиновского районного суда г. Казани – 110 тыс. руб.

Предъявляются иски о признании недействительными договоров, заключенных потерпевшими под влиянием мошенников. Основаниями для предъявления исков стали заключения 9 судебных психолого-психиатрических экс-

пертиз по уголовным делам, которыми установлено наличие порока воли потерпевших при совершении юридически значимых действий, при этом у двоих потерпевших выявлены психические заболевания.

Руководитель отдела поиска и анализа новых киберугроз ООО «БИЗон» Г.В. Григорьев, характеризуя угрозы, связанные с утечкой конфиденциальных данных, привел сведения о росте за истекший период 2023 г. в 3 раза количество атак, связанных с утечкой информации, в результате которых скомпрометировано более 700 млн учетных записей.

По мнению указанного специалиста, сравнительно небольшой ущерб от подобного рода действий, имеющих широкое распространение, обусловлен тем, что большинство причастных лиц являются так называемыми хактивистами, которые, как правило, не ищут финансовой или иной выгоды, а их действия являются формой привлечения внимания общественности к социальным, политическим и другим вопросам с помощью кибератак.

По его оценке, поскольку подобного рода действия в первую очередь имеют цель похитить данные, обычно они не включают продвинутые тактики и техники ввиду невысокой компетенции злоумышленников, не связаны с применением вредоносного программного обеспечения и осуществляются на сетевой инфраструктуре российских провайдеров.

В выступлении заместителя прокурора Ленинградской области П.А. Данилова рассмотрены актуальные вопросы исключения факторов, способствующих совершению преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Им предложено закрепление на законодательном уровне дополнительных условий регистрации физических лиц в социальных сетях, на торговых и платежных интернет-площадках с использованием документов, удостоверяющих личность (паспорта гражданина Российской Федерации или иностранного государства, других документов) или через портал Госуслуги, что позволит идентифицировать участников онлайн-сервисов и затруднит деятельность в режиме «инкогнито».

Также предложено в ст. 137 УК РФ предусмотреть ответственность за незаконное собирание или распространение (продажу, приобретение) персональных данных лица без его согласия, а также за незаконное предоставление в преступных целях персональных данных иных лиц.

Возможные пути защиты банковского счета клиента от «телефонных мошенников» предложил технический директор ООО «Сбербанк-Телеком» Е.В. Ситников. Упомянув о распространенной практике отсева так называемых «спам-звонков» путем проверки номера звонящего абонента по различным базам данных, формирования «черных списков» номеров, контентной фильтрации, анализа истории звонков, блокировки нежелательных контактов и массового обзвона, он обратил внимание на использование самообучающихся фильтров на основе искусственного интеллекта.

К таковым относятся анализ разговора и текстов СМС-сообщений, сопоставление голоса, звонящего с базой голосов злоумышленников, «умный автоответчик», принимающий все звонки, в том числе нежелательные, расшифровывающий разговоры и направляющий абоненту их текст и аудиозапись. По результатам проведенного анализа система может транслировать абоненту неслышное для звонящего голосовое предупреждение о вероятности того, что голос последнего является синтезированным, а сам звонок – мошенническим или «спам-звонком».

Перспективной является более глубокая интеграция с банком для расширения возможностей по противодействию злоумышленникам, в частности взаимное обогащение баз данных, в том числе банковского «антифрода», позволит выявлять события, имеющие признаки противоправности (анализ геолокации, действий в момент операции, нехарактерного поведения, подлинности и репутаций интернет-сайтов).

Начальник отдела по противодействию мошенничествам Северо-Западного банка ПАО Сбербанк М.Н. Полякова остановилась на противодействии хищениям денежных средств посредством «социальной инженерии», когда определенные действия или разглашение конфиденциальной информации

осуществляются под влиянием психологического манипулирования со стороны третьих лиц.

Системой по выработанному алгоритму фиксируются нехарактерные для клиента банка операции, после чего осуществляется их блокировка, а с клиентом связываются сотрудник банка по номеру 900 для выяснения обстоятельств совершаемых действий. Вопрос о дальнейшей разблокировке операций разрешается путем приглашения клиента в офис. Соответствующее решение принимается по результатам беседы и анализа профиля финансовых связей клиента. В случае объективного подтверждения влияния третьих лиц информация передается в правоохранительные органы.

Согласно представленным данным в Санкт-Петербурге и Ленинградской области (с 31.07.2023 по 03.11.2023) и остальных субъектах Северо-Западного федерального округа (со 02.10.2023 по 03.11.2023) системой замаркировано 275 клиентов, 217 из которых обратились в структурные подразделения банка, по результатам оказались предотвращены 56 посягательств на сумму свыше 29 млн руб.

Также докладчик охарактеризовал электронное взаимодействие, в рамках которого запросы органов внутренних дел исполняются ПАО Сбербанк в течении часа. При наличии фамилии, имени, отчества, даты рождения и номера паспорта клиента возможно получить выписку по карте и по счету, сведения о дебетовых и кредитных картах лица, арендованных им сейфовых ячейках, информацию о владельце карты и счета, данные IP-адреса входа в систему, перечень СМС-сообщений от банка.

Первый заместитель руководителя СУ СК России по Ленинградской области Д.Ю. Митяев и первый заместитель начальника ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области А.А. Щепин осветили проблемы расследования преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

В частности, А.А. Щепин пояснил, что в настоящее время органы предварительного следствия могут получать информацию от ПАО Сбербанк,

АО «Альфа-Банк», ПАО «ВТБ» в электронном виде через сервисы электронного взаимодействия, которые интегрированы в информационно-аналитическую систему обеспечения деятельности МВД России.

Он привел факты, когда после оперативного получения данных о лицах, на счет которых переведены денежные средства потерпевших, следственными действиями установлено отсутствие юридических оснований для производства платежей, в связи с чем денежные средства на сумму 143 тыс. руб. и 348,9 тыс. руб. добровольно возвращены.

Начальник оперативного управления УФСИН России по г. Санкт-Петербургу и Ленинградской области А.Н. Морозов осветил организацию оперативной работы в учреждениях ФСИН России по противодействию преступлениям ИТТ. Им приведены сведения о пресечении проноса на территорию режимных учреждений сотовых телефонов и сим-карт, а также по недопущению использования указанных предметов осужденными и лицами, заключенными под стражу.

Докладчиком обращено внимание, что техническое совершенствование средств связи, уменьшение их размеров способствует возможности скрытного проноса на режимные объекты и использования на их территории. Расположение таких объектов в крупных населенных пунктах или в местностях, где активно используется сотовая связь, осложняет возможности противодействия, в том числе использование аппаратуры подавления электронных сигналов.

Как следует изо всех сделанных в рамках форума сообщений, опасность преступлений с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации осознается органами власти и банковским сообществом. Привлечение к правоохранительной деятельности сотрудников банковского сектора для обмена опытом противодействия недобросовестным практикам закрепляется в основополагающих документах[1].

[1] Об эффективности деятельности правоохранительных органов по противодействию преступным посягательствам на финансовом рынке : Постановление Координа-

Существует объективная необходимость выработки новых способов противодействия указанным преступлениям, в первую очередь на основании оперативного обмена актуальной информацией путем электронного документооборота.

Формируется система выявления признаков противоправных действий, накопления соответствующей информации и блокировки операций по хищению и выводу денежных средств.

Комплексная оценка противоправных действий с привлечением сведений банковского сообщества намечает способы преодоления латентности отдельных категорий преступлений экономической направленности.

УДК 343

Э. А. САФАРОВ

НЕЙРОСЕТЬ КАК ОРУДИЕ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ: НОВЫЕ ВЫЗОВЫ ДЛЯ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ

В современном мире использование информационных технологий в повседневной жизни общества не является чем-то экстраординарным. Сегодня любая отрасль деятельности тесно сопряжена с применением компьютеров и иных информационных систем и технологий. Отрасль высоких технологий стремительно развивается, с каждым годом актуализируясь все больше.

Тенденцией последних лет является использование искусственных интеллектуальных систем – технологии, позволяющей делегировать техническим средствам решение комплексных задач. В наши дни к применению функций искусственного интеллекта прибегают многие прогрессивные субъекты общества: как частные лица для решения обыденных задач, так и коммерческие предприятия при реализации продуктов своей деятельности. Внедрение таких технологий в процесс государственного управления находится на этапе планирования.

ционного совещания руководителей правоохранительных органов Российской Федерации от 2 февраля 2023 г. № 1 // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru (дата обращения: 29.10.2023).

Новейшей технологией в рамках искусственного интеллекта являются нейронные сети. Прежде чем дать определение нейронным сетям, следует определить трактовку более широкого термина — искусственного интеллекта.

Законодательная трактовка термина «Искусственный интеллект» в настоящий момент отсутствует. Вместе с тем, существуют официальные документы федерального уровня, которые содержат определение исследуемого термина.

Так, например, Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» в подпункте «а» пункта 5 определяет искусственный интеллект как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека».

Хотя указанный документ содержит отсылки к нейронным сетям, трактовки указанного термина в нем нет. Ввиду этого автор предлагает следующую трактовку нейронных сетей: нейронная сеть (нейросеть) — это «тип искусственного интеллекта, который имитирует мозговую деятельность человека для обработки информации и принятия решений. Это компьютерная система, состоящая из большого количества связанных элементов (нейронов), которые могут обучаться и адаптироваться к новым данным».

Нейросети способны обучаться на примерах и выявлять закономерности в больших объемах данных, что делает их полезными для анализа, прогнозирования и автоматизации в самых разных областях, включая правовую практику, где они могут анализировать процессуальные документы, прогнозировать преступную деятельность и автоматизировать рутинные задачи (например, подготовку различных запросов или ответов на них, поиск и систематизирование судебной практики по необходимым критериям).

На данный момент, к сожалению, нейросети используются не в правоохранительной деятельности, а наоборот – при совершении преступлений.

Ввиду новизны такого орудия совершения преступлений исследование темы использования технологий нейронных сетей как средства совершения преступлений является актуальным и необходимым.

Использование нейросетей при совершении преступлений открывает новые возможности для преступника. Если при уже устоявшемся на практике использовании информационных и компьютерных систем злоумышленник при помощи одного такого инструмента мог совершать ограниченный набор общественно опасных деяний, то при использовании технологий нейронных сетей ограничение такой деятельности стремится к нулю.

Это объясняется тем, что обычные информационные технологии требуют определенной настройки и направленны на выполнение конкретных задач (например, при получении неправомерного доступа к зашифрованной компьютерной информации методом автоматизированного перебора возможных комбинаций паролей доступа (Brute force) специализированная компьютерная программа нацелена на решение конкретно указанной задачи — перебора паролей). В случае с нейронными сетями, ввиду того что такие технологии способны имитировать мыслительную деятельность человека, они могут использоваться для решения неограниченного спектра задач в зависимости от запроса пользователя.

Исходя из указанной особенности технологий нейросетей необходимо признать факт того, что применение таких технологий в целом не требует специальных знаний. Например, одна из наиболее известных на момент проведения настоящего исследования технология доступная для общего пользования «ChatGPT» принимает запросы от пользователей в свободном текстовом формате.

Так, для решения задачи требуется на удобном для пользователя языке (естественном) описать ее фабулу. Несмотря на заявления разработчиками указанной технологии о том, что при функционировании и взаимодействии с пользователями «ChatGPT» руководствуется правилами недопустимости

обработки запросов, способными нанести вред человечеству[1], на момент проведения настоящего исследования существуют способы обхода данного ограничения.

Указанные способы предполагают формулировку запросов, которые, на первый взгляд, не содержат общественной опасности[2]. Такое несовершенство может быть использовано злоумышленниками для получения потенциально общественно опасной информации, которая не должна находиться в свободном доступе (например, способов компьютерного взлома или изготовления взрывчатых веществ). При этом такие общественно опасные запросы имеют бóльшую латентность ввиду того, что они задаются не в поисковую систему в виде явного текстового запроса, а в диалоговое окно программы.

Технологии нейросетей могут быть опасным инструментом автоматизации преступлений. Например, актуальное ныне телефонное мошенничество может быть усовершенствованно путем использования функционала исследуемых технологий. Ранее упомянутая особенность искусственного интеллекта имитирования когнитивных функций человека может являться мощнейшим инструментом для введения жертвы в заблуждение.

Программы, настраиваемые злоумышленниками, могут использовать аналитические функции для обработки первичных данных жертвы, после чего совершать автоматический дозвон и общение с ней посредством синтезатора речи. Ввиду быстрой обучаемости и высокой скорости анализа поступающих в естественной форме данных, нейросети могут эффективно использовать социальную инженерию, входя в доверие жертвы, и понуждать ее к совершению неблагоприятных для нее же действий.

Другим примером автоматизации совершения традиционных видов преступлений при помощи нейросети является внедрение таких технологий в сбыт наркотических средств.

---

[1] OpenAI Charter : офиц. сайт. URL: https://openai.com/charter (дата обращения: 11.11.2023).

[2] Как обмануть цензуру в ChatGPT и получить нужную информацию // iXBT.LIVE : сайт. URL: https://www.ixbt.com/live/sw/kak-obmanut-chatgpt-i-zastavit-vydat-nuzhnuyu-informaciyu.html (дата обращения: 10.11.2023).

Например, посредствам внедрения нейронных сетей в программы мессенджера «Телеграм» (боты) при помощи соответствующих программных интерфейсов (API) наркоторговцы могут автоматизировать процесс как продажи товаров, так и взаимодействия с курьерами.

Помимо описанных выше сценариев применения преступниками технологий нейронных сетей при совершении преступлений существует множество иных сфер общественных отношений, на которые возможно посягательство с использованием таких технологий.

Таковыми являются:

— Финансовый сектор и банковская деятельность. Преступники могут использовать нейросети для проведения сложных финансовых махинаций, таких как манипуляции рынком, мошенничество с кредитными картами, фишинговые атаки. Нейросети способны анализировать большие объемы данных для выявления уязвимых точек в системах безопасности банков и финансовых институтов.

— Безопасность информационных систем. Нейросети могут быть использованы для создания сложных вирусов и троянских программ, атак на киберинфраструктуру, включая правительственные системы, энергетические сети, и системы общественной безопасности. Использование искусственного интеллекта в таких атаках может повысить их эффективность и уменьшить вероятность обнаружения.

— Ритейл и электронная коммерция. Нейросети могут быть использованы для создания и распространения поддельных отзывов о товарах и услугах, манипулирования поведением потребителей и ценообразованием. Это может включать использование машинного обучения для создания фальшивых видео и аудиозаписей (технологий deepfake), что может повлиять на деловую репутацию компаний и отдельных личностей.

— Телекоммуникации и социальные сети. Преступники могут использовать нейросети для анализа больших данных (Big Data) пользователей соци-

альных сетей с целью проведения мошеннических схем, социальной инженерии. Это включает в себя создание и распространение дезинформации и контента для манипуляции.

— Здравоохранение. Нейросети могут быть использованы для нарушения работы систем здравоохранения, включая управление медицинскими данными, создание и распространение поддельных медицинских исследований или манипулирование медицинским оборудованием. Например, уязвимости в программном обеспечении кардиостимуляторов и интратекальных насосных систем могут быть использованы злоумышленниками для причинения вреда пациенту.

— Иные отрасли общественных отношений.

Использование технологий нейросетей бросает новый вызов правоохранительным органам. Такие технологии способствуют не только облегчению и совершенствованию способов совершения преступлений (как традиционных, так и специализированных в сфере компьютерных технологий), но и повышению ее латентности, осложнению квалификации и пресечения.

Возникает ряд новых правовых и правоприменительных проблем в сфере противодействия преступлениям.

Так, в настоящий момент уголовное законодательство Российской Федерации не регулирует использование искусственного интеллекта, в том числе и в качестве орудия преступлений. Право отстает от стремительного развития технологий.

Некоторые исследователи отмечают, что бурное развитие научно-технического прогресса способствовало образованию правового вакуума, причина чего – формирование новой парадигмы цифрового общества, в которую не вписывается в полной мере существующая правовая система[1].

[1] Воронин В. Н. Уголовно-правовые риски развития цифровых технологий: постановка проблемы и методы научного исследования // Вестник Университета имени О. Е. Кутафина (МГЮА). 2018. № 12. С. 73—80.

По нашему мнению, решением такой проблемы должна стать выработка стратегии не только по внедрению использования нейросетей в деятельность государства и общества, но и развитие законодательства, устанавливающего ответственность за совершение преступлений с использованием таких технологий.

Представляется целесообразным внести изменения в ст. 63 УК РФ в части признания использования в качестве орудия преступления искусственного интеллекта в целом и нейросетей в частности как отягчающего обстоятельства.

Опасность и доступность нейросетей, их многофункциональность и совершенствование способов совершения преступлений при помощи таких технологий диктует необходимость более тщательного уголовного-правового подхода к такому вопросу.

Также следует обратить внимание на проблему определения круга лиц, подлежащих уголовной ответственности за преступления, сопряженные с использованием нейросетей.

При этом некоторые авторы полагают, что к ответственности должны привлекаться не только те разработчики, которые умышленно создают вредоносный искусственный интеллект, но и те, чьи технологии допускают их использование в преступных целях ввиду допущенной при разработке «небрежности либо легкомыслия»[1].

По нашему мнению, возвращаясь к определяющей функции искусственного интеллекта – имитирования когнитивных функций человека (включая самообучение и поиск решений без заранее заданного алгоритма) необходимо констатировать, что сама сущность нейросетей заключается в самообучении и самостоятельном выведении новых алгоритмов и подходов к решению задачи.

Таким образом, основной функцией разработчиков исследуемых технологий является настройка основных принципов работы, а их дальнейшее «обучение» и работа происходит путем взаимодействия с пользователем.

[1] Антонова Е. Ю. Технологии искусственного интеллекта — субъект преступления или орудие/средство совершения преступления? // Юридический вестник Кубанского государственного университета. 2022. № 14 (1). С. 31—39.

Ввиду этого, автор настоящей работы считает, что ответственность за добросовестное использование возможностей нейросетей должна быть возложена на конечного пользователя.

Важное значение приобретает и проблема латентности преступлений, совершаемых с использованием нейросетей, проблема неиспользования нейросетей в правоохранительной деятельности, проблема классификации преступлений, совершенных при помощи нейросетей. Ввиду новизны темы использования нейронных сетей в преступных целях требуется детальное изучение указанного вопроса и разработка научных и практических подходов по противодействию таким преступлениям.

Таким образом, использование нейросетей как орудия совершения преступлений является актуальной проблемой для правоохранительной системы. В ответ на этот вызов требуется принятие комплексных мер, включающих как законодательные изменения, так и улучшение практик правоприменения, обучение квалифицированных специалистов и международное сотрудничество. Только системный подход позволит эффектно реагировать на новые угрозы и обеспечить защиту общества от использования передовых технологий в преступных целях.

УДК 343

В. Н. САФОНОВ

ПРАВОВАЯ ОЦЕНКА ХИЩЕНИЯ В МЕЛКИХ РАЗМЕРАХ ПРИ КВАЛИФИЦИРУЮЩИХ ПРИЗНАКАХ (НА ПРИМЕРЕ КРАЖИ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ)

Проблема правовой оценки мелкого хищения, когда оно совершено при квалифицирующих признаках, предусмотренных ст.ст. 158—160 УК РФ, в последнее время активно обсуждается в научных публикациях. Очевидны и противоположные подходы в судебной практике. Сложившаяся ситуация не соответствует принципам уголовного права и предполагает объединение усилий исследователей и практиков.

В законодательной плоскости проблема сводится к следующему. В соответствии с положениями ст. 7.27 КоАП РФ хищение чужого имущества, совершенное в 4-х формах: кражи, мошенничества, присвоения или растраты, когда стоимость похищенного не превышает одну тысячу рублей (ч. 1), либо превышает одну тысячу рублей, но не превышает две тысячи пятьсот рублей (ч. 2) при отсутствии квалифицирующих признаков, предусмотренных в соответствующих частях статей 158—160 УК РФ, признается мелким. Таким образом, хищение в тех же формах, когда стоимость похищенного хотя и не превышает обозначенных мелких размеров, но совершенное при квалифицирующих признаках, должно признаваться как соответствующее преступление.

Однако это, казалось бы, императивное указание закона, не столь линейно реализуется в судебной практике. В научной литературе также встречаются полярные интерпретации правовой оценки мелкого хищения при квалифицирующих признаках. «Активная фаза» дискуссии вокруг обозначенной проблемы возникла до законодательных новелл 2018 г., когда Федеральным законом от 23 апреля № 111-ФЗ статья 158 УК РФ была дополнена п. «г» ч. 3 ст. 158 УК РФ — кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Причиной оживления этой дискуссии стали выявленные и нередкие факты незаконного привлечения граждан к уголовной ответственности за мелкое хищение чужого имущества, выявленные как заметная тенденция правоприменительной практики на уровне судов субъектов Федерации при обобщении судебной практики.

Так, проведя обобщение судебной практики применения положений ч. 2 ст. 14 УК РФ, Иркутский областной суд пришел к неутешительным выводам о довольно частых незаконных привлечениях к уголовной ответственности лиц, совершивших малозначительные деяния, в том числе и при квалифицирующих признаках, указанных в нормах об имущественных преступлениях[1].

[1] Справка о результатах обобщения судебной практики применения положений части 2 статьи 14 УК РФ (малозначительность деяния) // Иркутский областной суд : офиц.

В то же время обобщил аналогичную судебную практику Ростовский областной суд и пришел к столь же неутешительному выводу[1]. В этом числе определенная доля мелких хищений была совершена и при квалифицирующих признаках. При таких обстоятельствах суды должны были обсудить вопрос о малозначительности, отмечено Ростовским областным судом.

В научной литературе мнения относительно правовой оценки мелкого хищения при квалифицирующих признаках разделились. Наиболее решительно за уголовно-правовую природу мелких хищений с квалифицирующими признаками выступает Р.Д. Шарапов[2].

К этому выводу Р.Д. Шарапов приходит, рассмотрев проблему с позиций конкуренции норм, относящихся к разным отраслям права, значимости способа в квалифицированном уголовно-правовом составе, юридической технике норм.

Позицию Р.Д. Шарапова разделяют ряд исследователей и многие правоприменители. Так, к аналогичному выводу приходит и В.Н. Винокуров[3].

И все же сложно не заметить нестабильность судебной практики и разброс мнений исследователей относительно квалификации мелкого хищения с квалифицирующими признаками[4].

Здесь чаще всего речь идет о групповом совершении кражи, о краже с проникновением в помещение или иное хранилище или о краже с проникновением в жилище. Изучение материалов судебной практики обоснованно приводит к выводу о том, что «…большинство правоприменителей… применяет положения ч. 2 ст. 14 УК РФ к квалифицированным хищениям в форме кражи,

---

сайт. URL: https:oblsud.irk.sudrf.ru/modules.php?name=docum_sud&id=431 (дата обращения: 11.10.2023).

[1] Справка о некоторых вопросах, связанных с рассмотрением судами Ростовской области уголовных дел о преступлениях небольшой и средней тяжести в I полугодии 2011 г. // Ростовский областной суд : офиц. сайт. URL: https:oblsud.ros.sudrf.ru/modules.php?name=docum_sud (дата обращения: 11.10.2023).

[2] Шарапов Р. Д. Квалификация мелкого хищения при наличии квалифицирующих признаков, предусмотренных уголовным законом // Законность. 2013. № 7(945). С. 29—35.

[3] Винокуров В. Н. Признаки и пределы малозначительности деяния в уголовном праве // Современное право. 2017. № 6. С. 64—70.

[4] Корсун Д. Ю. Малозначительное деяние с квалифицирующими признаками // Гуманитарные, социально-экономические и общественные науки. 2019. № 9. С. 131—138.

мошенничества, присвоения и растраты, ориентируясь не столько на квалифицирующие признаки, сколько на стоимость похищенного имущества»[1].

Очевидно, суды учитывают и рекомендацию Верховного Суда Российской Федерации учитывать реальную общественную опасность деяния, высказанную высшим судебным органом страны по ряду категорий уголовных дел[2].

Характерно, что после дополнения Федеральным законом от 23 апреля № 111-ФЗ ч. 3 ст. 158 УК РФ п. «г» с особо квалифицированным видом тайного хищения чужого имущества (кража с банковского счета, а равно в отношении электронных денежных средств).

Правоприменительная практика обнаруживает три разнонаправленные позиции квалификации кражи с банковского счета, а равно в отношении электронных денежных средств в мелком размере:

1) как хищение, предусмотренное п. «г» ч. 3 ст. 158 УК РФ и не рассматриваемое в качестве малозначительного деяния с учетом способа совершения деяния и «формальной» общественной опасности[3];

2) как малозначительное деяние с применением положений ч. 2 ст. 14 УК РФ[4];

3) реже — как деяние, лишенное этого квалифицирующего признака, если банковская карта использовалась не удаленно, либо без совершения действий, направленных на взлом системы безопасности доступа к банковскому счету и охраняемым данным, составляющих банковскую тайну[5].

Предпринятое исследование дает основание для следующих выводов.

---

[1] Там же.

[2] Сафонов В. Н. К вопросу о реальной общественной опасности деяния // Научная сессия ГУАП : гуманитарные науки : сборник докладов традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики, Санкт-Петербург, 14—22 апреля 2020 года. СПб., 2020. С. 223—224.

[3] Апелляционное определение Челябинского областного суда от 7 октября 2021 г. № 10-5621/2021 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 11.11.2023).

[4] Оправдательный приговор гражданину, оплатившему покупки чужой банковской картой, устоял в апелляции // Адвокатская газета : сайт. URL: https://www.advgazeta.ru/novosti/opravdatelnyy-prigovor-grazhdaninu-oplativshemu-pokupki-chuzhoy-bankovskoy-kartoy-ustoyal-v-apellyatsii (дата обращения: 11.11.2023).

[5] Определение Верховного Суда Российской Федерации по делу от 11 марта 2020 г. № 10-УДп20-1. Доступ из справ.-правовой системы «КонсультантПлюс».

1. Очевидно, что имеющаяся законодательная база в части квалификации мелкого хищения при квалифицирующих признаках, предусмотренных ст.ст. 158—160 УК РФ, сохраняет неопределенность, а сложившаяся практика носит противоречивый, разнонаправленный характер и входит в противоречие с принципами уголовного права и пониманием реальной общественной опасности деяния[1].

2. Представляется уместным дальнейшее совершенствование законодательной базы с обозначением нижнего предела размера мелкого хищения, когда такое деяние, совершенное при квалифицирующих признаках, предусмотренных ст.ст. 158—160 УК РФ, императивно признавалось бы преступлением. Полагаем, что таковым нижним размером мелкого хищения, может стать стоимость похищенного в размере более одной тысячи рублей.

УДК 343

А. Ю. СЕРДЮК

К ВОПРОСУ О СУБЪЕКТЕ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 172.2 УК РФ

Общественная опасность действий организаторов деятельности по привлечению денежных средств и (или) иного имущества не вызывает дискуссий даже при отсутствии широкой практики их привлечения к уголовной ответственности (по данным агентства правовой информации по ст. 172.2 УК РФ в 2016 году осуждено 2 лица, в 2017 году – 12, в 2018 году – 3, в 2019 году – 1, в 2020 году – 2, в 2021 году – 0, в 2022 году – 0[2]).

Такое количество выявленных правоохранительными органами преступлений, предусмотренных ст. 172.2 УК РФ, в значительной степени обусловлено сложным характером преступления, приводящему к сложностям доказывания объективной стороны, что подтвердили 55,6 % опрошенных сотрудников правоохранительных органов.

---

[1] Сафонов В. Н. Проблемы Общей части уголовного права в материалах судебной практики : учебно-методическое пособие. СПб., 2020. 68 с.

[2] Судебная статистика РФ : сайт. URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 07.11.2023).

Частично это объясняется и установлением уголовного запрета исключительно для организатора преступления и выведение из-под его действия остальных участников преступной деятельности (таких как кассиры, программисты, инженеры по программному обеспечению, консультанты, ведущие семинаров, разработчики сайтов и рекламной кампании, менеджеры по работе с клиентами, непосредственно перемещающие полученные от вкладчиков ценности охранники и водители).

Использованная законодателем конструкция ст. 172.2 УК РФ не содержит четких отсылок к субъекту данного преступления. При этом именно такое отсутствие конкретизации порождает дискуссии относительно того, кто же может быть привлечен к уголовной ответственности за организацию привлечения имущества.

Стоит отметить, что субъект преступления является обязательным элементом его состава и основанием уголовной ответственности. Общий субъект преступления – это вменяемое физическое лицо, достигшее возраста уголовной ответственности.

И если для случаев единоличной организации деятельности по привлечению имущества без использования соответствующего юридического лица вопрос о субъекте преступления не предполагает неоднозначного толкования, то в случаях создания финансовых пирамид под видом добросовестных организаций, осуществляющих инвестиционную, предпринимательскую, благотворительную или иную законную деятельность, необходим более подробный анализ.

Для ряда преступлений, к которым в первую очередь относятся преступления в сфере экономической деятельности, учеными-правоведами поднимается вопрос о возможности привлечения юридических лиц к уголовной ответственности за их совершение. Актуальным является данный вопрос и для финансовых пирамид.

В некоторых странах (Италия, Нидерланды, Франция, Бельгия, Португалия) установлена уголовная ответственность юридических лиц, Германии

и Швеции сложился смешанный институт уголовно-административной ответственности юридических лиц[1].

В Российской Федерации попытки ввода уголовной ответственности юридических лиц, предпринятые в соответствующих проектах УК РФ, не увенчались успехом[2] в связи с глобальным выходом за общую концепцию Уголовного кодекса и традиционного понимания уголовного права: противоречие таким фундаментальным принципам как личная и виновная ответственность, институтам вины и вменяемости, понятиям сущности и целей наказания, понятию преступления как действия или бездействия.

Одним из аргументов в пользу введения института уголовной ответственности юридических лиц является сложная структура управления хозяйствующими субъектами и иными организациями, в форме которых осуществляют деятельность финансовые пирамиды, приводящую нередко к невозможности однозначно установить лиц, непосредственно причастных к преступлению[3].

При этом такая конструкция может обратить в преступников акционеров, учредителей, сотрудников организаций, непосредственно не причастных к осуществлению общественно опасных деяний и принятию соответствующих решений, и одновременно освободить от персональной ответственности конкретных физических лиц, «размыв» их ответственность в акциях и дивидендах собственников[4].

Нами разделяется точка зрения, согласно которой человек является многосторонним существом, которому присущи внешняя непосредственно наблюдаемая сторона и внутренняя, характеризующая мысли и переживания определенного человека.

---

[1] Малинин В. Б., Попов В. В., Спасенников Б. А. К вопросу о субъекте преступления в уголовном праве // Пенитенциарная наука. 2009. № 7. С. 76—80.

[2] Никифоров А. С. Юридическое лицо как субъект преступления и уголовной ответственности. М., 2002. 204 с.

[3] Шишко И. В. О субъекте преступлений в сфере экономической деятельности // Вестник Нижегородского университета им. Н. И. Лобачевского. Серия: Право. 2001. № 2. С. 231—238.

[4] Малинин В. Б., Попов В. В., Спасенников Б. А. Указ. соч.

Субъективный мир человека характеризуется наличием сознания и самосознания, способностью понимать и изучать смысл своих действий, поступков, поведения, испытывать муки совести, осуществлять власть над собой, т. е. осознанностью. С другой стороны, субъективность подразумевает способность быть субъектом своей жизни, превращать жизнедеятельность в предмет постоянного преобразования, оценивать способы деятельности, контролировать ее ход и результаты. Таким образом, человек может быть субъектом преступления только как психосоциальная реальность.

Рассмотрение же юридического лица в качестве субъекта преступления является не чем иным, как разновидностью объективного вменения, игнорирующего обязанность правоприменителей определить внутреннее отношение лица к совершенному преступлению, персональный характер уголовной ответственности. Юридическое лицо не обладает субъективностью, осознанным волевым поведением, не способно осознавать свою вину, исправиться в ходе исполнения наказания, что исключает его возможность выступать субъектом преступления.

При этом учитывая бесспорную возможность привлечения юридических лиц к гражданской ответственности, в рамках ст. 172.2 УК РФ такая ответственность заслуживает отдельной разработки с целью выполнения такой задачи уголовного судопроизводства как восстановление прав потерпевших. На современном этапе механизмы возмещения вреда вкладчикам не работают либо работают на уровне несопоставимом с реальным восстановлением прав.

Полагаем, что при наличии юридического лица, должностные лица которого подозреваются в совершении преступления, предусмотренного ст. 172.2 УК РФ, должен быть предусмотрен более действенный порядок возмещения вреда за счет имущества юридического лица, до реализации процедуры банкротства, требующей значительного времени.

В случаях, когда в конкретной норме Особенной части УК РФ предусмотрен один или несколько обязательных дополнительных признаков субъекта

преступления, он становится специальным. Это могут быть как индивидуально определенные признаки лица, так и нормативные (положение в системе общественных отношений).

В данном случае стоит детально изучить вопрос о том, как признаки субъекта преступления описаны в диспозиции ст. 172.2 УК РФ в сравнении с иными статьями главы 22 УК РФ, для которой характерно прямое или косвенное указание на признаки специального субъекта. Зачастую признаки субъекта преступления необходимо выводить из описания объективной стороны, сложности и неоднозначности толкования которых обуславливают дискуссии и о признаках субъекта преступления.

Основной проблемой является то, что подавляющая часть действий, содержащих объективную сторону преступления, предусмотренного ст. 172.2 УК РФ, выполняется в процессе осуществления хозяйственной и иной законной деятельности юридических лиц, созданных для прикрытия деятельности финансовой пирамиды. Вопрос о том, кто конкретно несет ответственность за совершение преступлений в интересах таких юридических лиц остается открытым.

Согласно общей концепции гражданского права именно руководитель представляет соответствующую организацию. Такие авторы, как Б.В. Волженкин[1], А.В. Наумов[2], Т.Ю. Погосян[3], В.Е. Мельникова[4] нередко именно руководителя организации определяют единственным надлежащим субъектом соответствующих преступлений.

При этом субъектом преступлений в сфере экономической деятельности не всегда выступает руководитель или не только руководитель. Полномочия по осуществлению деяний, содержащих признаки преступлений, могут при-

---

[1] Волженкин Б. В. Экономические преступления. СПб., 1999. 312 с.

[2] Уголовное право России. Особенная часть : учебник / под ред. В. Н. Кудрявцева, А. В. Наумова. М., 1999. С. 192, 198.

[3] Уголовное право. Особенная часть : учебник для вузов / отв. ред. И. Я. Козаченко, З. А. Незнамова, Г. П. Новоселов. М., 1997. С. 291.

[4] Уголовное право России. Особенная часть : учебник / отв. ред. Б. В. Здравомыслов. М., 1996. С. 204.

надлежать заместителю руководителя, начальнику структурного подразделения, коллегиальным органам управления. Следовательно, для установления субъектов конкретного преступления необходимо четко определить круг полномочий каждого лица на основе изучения трудовых договоров, должностных инструкций, учредительных документов, нормативных актов. Стоит учитывать, что организаторы финансовых пирамид еще на этапе разработки учредительной документации могут формально исключить конкретных лиц, непосредственно причастных к преступной деятельности, из состава руководства организации при фактическом выполнении ими таких функций. Позиция о разделении сфер ответственности соответствует объективной невозможности одного лица на надлежащем уровне владеть актуальной информацией обо всех процессах, возникающих в ходе деятельности организации.

Одновременно часть исследователей рассматривают возможность привлечения за совершение отдельных преступлений в сфере экономической деятельности любых других работников юридического лица. В качестве примера Н.А. Лопашенко приводит такой состав преступления как ограничение конкуренции[1], И.В. Шишко – принуждение к совершению сделки и перемещение товаров через таможенную границу помимо таможенного контроля[2].

Отдельно стоит выделить преступления, для совершения которых необходимо выполнить от имени юридического лица юридически значимые действия. В таких случаях специальным субъектом преступления может выступать только лицо, наделенное такими полномочиями.

Применительно к ст. 172.2 УК РФ ответственности подлежат лица, которые выполнили объективную сторону – организовали деятельность по привлечению имущества в крупном размере. Закон не содержит отсылок к тому, какими дополнительными признаками специального субъекта должны обладать такие лица. На этом основании большинство ученых, среди которых В.И. Тюнин, Ю.В. Белицкий, И.Г. Сафаров сделали вывод о том, что субъект данного

[1] Лопашенко Н. А. Преступления в сфере экономической деятельности. Ростов н/Д., 1999. С. 142.

[2] Шишко И. В. Указ. соч.

преступления общий. Следуя этой логике, а также широкому пониманию понятия организация деятельности, к уголовной ответственности по ст. 172.2 УК РФ может быть привлечен широкий круг лиц: от создателей и руководителей до рядовых сотрудников.

Такое, казалось бы, не выходящее за рамки УК РФ, трактование диспозиции ст. 172.2 Уголовного кодекса Российской Федерации имеет два явных недостатка: непринятие судебно-следственной практикой и коллизия со ст. 14.62 КоАП РФ. Различия в названиях статей и описании деяния налицо. Так, КоАП РФ устанавливает ответственность за всю деятельность в сфере незаконного привлечения денежных средств и (или) иного имущества, в том числе за ее организацию и осуществление. Под уголовный запрет же подпадает только организация такой деятельности.

Включение разных действий в объективную сторону административного и уголовного запретов, безусловно, ведет и к разным субъектам, которые могут выполнять такие действия. КоАП РФ предполагает значительно более широкий круг таких потенциальных субъектов, относя к ним также и вкладчиков, привлекающих новых участников, что видно из пояснительной записки к данному законопроекту.

На этот же недостаток конструкции ст. 172.2 УК РФ обратила внимание И.Я. Яковенко, обозначив, что из-под регулирования уголовного закона выпадают лица, которые самостоятельно не выполняют объективную сторону преступления, а только содействуют, подстрекают иных лиц, подчинены вышестоящим руководителям финансовой пирамиды, поддерживают дисциплину в ней, организовывают рекламу, влияют на вкладчиков и иных сотрудников, выступая при этом значимым элементом преступной организации[1].

Необходимость такого запрета следует из того, что в отсутствие такой ответственности вышеуказанные сотрудники, получившие навыки по работе в финансовой пирамиде, после ее краха остаются безнаказанными и зачастую всем коллективом принимают участие в работе новой пирамиды.

[1] Яковенко И. А. Уголовная ответственность за организацию деятельности по привлечению денежных средств // Наука и образование сегодня. 2020. № 12 (59). С. 58—60.

Так по информации Банка России в декабре 2020 года выявлена сеть консультационных центров, представляющих собой финансовую пирамиду, организованную компанией Antares Limited, в которой работали менеджеры из финансовый пирамиды «Кэшбери», запрещенной в январе 2019 года[1].

«Кэшбери», в свою очередь, стал последователем Sky Way, вкладчики великих опционов которой в 2014-2015 потеряли 13 млрд рублей[2].

Данное противоречие может быть разрешено путем указания в диспозиции ст. 172.2 УК РФ на признаки специального субъекта. Актуальной видится формулировка, использованная законодателем в ст. 201, 285 УК РФ, — лицо, выполняющее постоянно, временно либо по специальному полномочию организационно-распорядительные или административно-хозяйственные функции.

Виновные же действия остальных сотрудников, несущие меньший вред соответствующим общественным отношениям, подпадают под действие административного запрета. В данном ракурсе видится возможным установление для них уголовной ответственности с административной преюдицией, подразумевающей привлечение к уголовной ответственности лиц, повторно совершивших правонарушение, которые ранее привлечены к административной ответственности за однократное правонарушение. Такая конструкция не является новеллой и уже использована для привлечения к уголовной ответственности за так называемые проступки – общественно вредные деяния, приобретающие общественную опасность при их многократности и на этом основании переходящие из разряда административных проступков в уголовные преступления.

При описании признаков специального субъекта преступления, предусмотренного ст. 172.2 УК РФ, нельзя исключить из перечня субъектов уголовной ответственности лиц, осуществляющих деятельность по привлечению

---

[1] Григоров Г. ЦБ выявил крупную финансовую пирамиду с выходцами из «Кэшбери» // ТАСС : сайт. URL: https://tass.ru/ekonomika/10136947 (дата обращения: 26.10.2023).

[2] Чапман А. Кешбери – привет от покойника SkyWay // Venture Business News : [информационно-аналитический портал]. URL: https://www.venture-news.ru/investicii/60083-keshberi-privet-ot-pokoynika-skyway.html (дата обращения: 04.02.2022).

имущества вкладчиков без соответствующей организации (юридического лица). Такая форма существования финансовых пирамид стала популярной с появлением у злоумышленников возможностей выполнять объективную сторону преступления без выхода в офлайн – путем создания сайтов, страниц в социальных сетях, p2p-платформ и размещения иной информации в сети «Интернет». Более того, наличие соответствующего юридического лица часто является формальным, прикрывающим деятельность по привлечению имущества, и не является обязательным.

Проведенное исследование дало возможность прийти к выводу о том, что субъект преступления, предусмотренного ст. 172.2 УК РФ, в действующем уголовном законе определен как общий, что порождает неопределенность в части возможности привлечения к уголовной ответственности сотрудников и активных вкладчиков финансовой пирамиды и коллизии с институтом соучастия в преступлении.

УДК 343

А. В. СУМАЧЕВ

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»): УГОЛОВНО-ПРАВОВЫЕ «МИНУСЫ»

Поистине безграничное использование компьютеров (компьютерной информации) в повседневной жизни, несомненно, имеет не только свои «плюсы», но и «минусы». Такие «минусы» касаются не только сферы организации деятельности или досуга детей и взрослых, но и могут иметь непосредственное отношение к преступным проявлениям.

И не случайно современный законодатель уделяет пристальное внимание конструированию уголовно-правовых норм, описывающих преступления, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

При этом использование в процессе совершения преступления информационно-телекоммуникационных сетей, в том числе сети «Интернет», может

выступать не только квалифицирующим (особо квалифицирующим) признаком состава преступления, но и одним из конструктивных признаков основного состава.

Так, при доведении до самоубийства (п. «д» ч. 2 ст. 110 УК РФ), склонении к совершению самоубийства или содействие совершению самоубийства (п. «д» ч. 3 ст. 110.1 УК РФ), организации деятельности, направленной на побуждение к совершению самоубийства (ч. 2 ст. 110.2 УК РФ), незаконном распространении информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий (ч. 3 ст. 137 УК РФ), вовлечении несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (п. «в» ч. 2 ст. 151.2 УК РФ), публичных призывах к осуществлению террористической деятельности или публичном оправдании терроризма (ч. 2 ст. 205.2 УК РФ), сбыте наркотических средств, психотропных веществ или их аналогов (п. «б» ч. 2 ст. 228.1 УК РФ), незаконным изготовлении и обороте порнографических материалов или предметов (п. «б» ч. 3 ст. 242 УК РФ), изготовлении и обороте материалов или предметов с порнографическими изображениями несовершеннолетних (п. «г» ч. 2 ст. 242.1 УК РФ), использовании несовершеннолетнего в целях изготовления порнографических материалов или предметов (п. «г» ч. 2 ст. 242.2 УК РФ), публичных призывах к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ), публичных призывах к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ч. 2 ст. 280.1 УК РФ) использование информационно-телекоммуникационных сетей (включая сеть «Интернет») выступает в качестве квалифицирующего (особо квалифицирующего) признака (обстоятельства) состава преступления.

Ко вторым случаям — когда использование информационно-телекоммуникационных сетей (включая сеть «Интернет») выступает в качестве одного из конструктивных признаков основного состава — относятся мошенничество

в сфере компьютерной информации (ст. 159.6 УК РФ), незаконные организация и проведение азартных игр (ст. 171.2 УК РФ) и манипулирование рынком (ст. 185.3 УК РФ).

Как видно, использование компьютеров (компьютерной информации) не беспредельно, а ограничено юридическими «рамками», включая уголовно-правовые пределы. Стоит также констатировать, что такие действия (использование компьютеров) порой существенно влияет на ужесточение уголовной ответственности.

Более того, иногда ужесточение наказания за совершение соответствующих видов квалифицированных (особо квалифицированных) преступлений чрезмерно и, даже, необоснованно, велико. Так, например, организация деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») (ч. 2 ст. 110.2 УК РФ), наказывается практически также как простое убийство (ч. 1 ст. 105 УК РФ) — лишением свободы на срок до пятнадцати лет.

Заметим, что даже умышленное причинение тяжкого вреда здоровью, совершенное в отношении лица или его близких в связи с осуществлением данным лицом служебной деятельности или выполнением общественного долга; в отношении малолетнего или иного лица, заведомо для виновного находящегося в беспомощном состоянии, а равно с особой жестокостью, издевательством или мучениями для потерпевшего; общеопасным способом; по найму; из хулиганских побуждений; по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы; в целях использования органов или тканей потерпевшего; с применением оружия или предметов, используемых в качестве оружия; группой лиц, группой лиц по предварительному сговору или организованной группой; в отношении двух

или более лиц более мягко наказуемо — лишение свободы на срок до двенадцати лет (ч. 2, 3 ст. 111 УК РФ).

С другой стороны, «техническая грамотность» лица, совершающего преступление посредством использования компьютеров (компьютерной информации), порой необоснованно смягчает уголовную ответственность в сравнении с «простым» мошенником. Так, максимальное наказание за «простое» мошенничество в сфере компьютерной информации составляет арест на срок до четырех месяцев (ч. 1 ст. 159.6 УК РФ), в то время как «обычное» мошенничество может быть наказуемо лишением свободы на срок до двух лет (ч. 1 ст. 159 УК РФ).

Кроме того, не вполне понятным или логически обоснованным представляется положение, определяемое в ч. 2 ст. 228.1 УК РФ. Дело в том, что в ч. 1 ст. 228.1 УК РФ речь идет о ***незаконном*** (курсив наш. — *А. С.*) производстве, сбыте или пересылке наркотических средств, психотропных веществ или их аналогов, а также ***незаконном*** (курсив наш. — *А. С.*) сбыте или пересылке растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества.

В свою очередь, в ч. 2 ст. 228.1 УК РФ термин «незаконный» не использует:

«2. Сбыт наркотических средств, психотропных веществ или их аналогов, совершенный:

а) в следственном изоляторе, исправительном учреждении, административном здании, сооружении административного назначения, образовательной организации, на объектах спорта, железнодорожного, воздушного, морского, внутреннего водного транспорта или метрополитена, в общественном транспорте либо помещениях, используемых для развлечений или досуга;

б) с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)...».

И здесь возникает вопрос: законный сбыт наркотических средств, психотропных веществ или их аналогов автоматически «превращается» в незаконный, если происходит в вышеуказанных местах либо осуществляется посредством, например, использования информационно-телекоммуникационных сетей (включая сеть «Интернет»)? Если рассуждать в таком плане, то использование «Интернета» (равно как и место сбыта наркотиков) выступает в качестве не квалифицирующего, а конструктивного признака преступления.

Если же вести речь о квалифицирующих признаках, то в ч. 2 ст. 228.1 УК РФ следует добавить слово «незаконный», как, например, это сделано применительно к ч. 4 ст. 222 УК РФ «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия, его основных частей, боеприпасов»:

«4. Незаконный сбыт гражданского огнестрельного гладкоствольного длинноствольного оружия, огнестрельного оружия ограниченного поражения, газового оружия, холодного оружия, в том числе метательного оружия...».

Здесь мы указали, так называемые, уголовно-правовые «минусы» использования информационно-телекоммуникационных сетей (включая сеть «Интернет»), связанные с установлением уголовной ответственности за определенные деяния либо ее ужесточением. Однако есть и своего рода уголовно-правовые «плюсы» в сфере использования компьютеров (компьютерной информации).

Речь идет об уголовно-правовом обеспечении такого использования — охране добросовестных пользователей посредством установления уголовной ответственности за:

— неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

— создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

— нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

УДК 343

К. И. ТИМОЩУК

ПРЕСТУПЛЕНИЯ ПРОТИВ РЕЛИГИОЗНЫХ ПРАВ ГРАЖДАН, СОВЕРШАЕМЫЕ В СЕТИ «ИНТЕРНЕТ», В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ СТРАН

Преступления против религиозных прав граждан причиняют вред конституционным правам, свободам и интересам человека и гражданина, а также законным интересам общества и государства, и поэтому представляют высокий уровень общественной опасности.

В литературе авторами поднималась тема необходимости изучения проблем повышения эффективности противодействия преступлениям, совершенным по мотивам вражды и ненависти применительно к проблемам, возникающим в связи с уголовным преследованием лиц, совершившим преступления на почве религиозной вражды и ненависти, включая совершенные с использованием сети «Интернет».

С уголовно-правовой точки зрения законодатель реализовал два подхода к установлению ответственности за совершение преступлений рассматриваемой группы. Реализуя первый из них, он включил мотив религиозной вражды и ненависти в качестве непременной составляющей диспозиций ряда статей Уголовного кодекса Российской Федерации, а реализуя второй – закрепил его в качестве квалифицирующего признака в других статья УК РФ. И особое место в этих группах преступлений занимает ст. 148 УК РФ.

При изучении проблем повышения эффективности защиты конституционного права человека и гражданина на свободу совести и вероисповедания в первую очередь представляется целесообразным обращение именно к диспозиции ст. 148 УК РФ, поскольку эта статья устанавливает ответственность за нарушение конституционного права на свободу совести и вероисповедания.

Одновременно важно учитывать, что законодатель определяет данное конституционное право как единое, рассматривая свободу совести и вероис-

поведания в едином контексте и гарантируя каждому «право исповедовать индивидуально или совместно с другими любую религию или не исповедовать никакой, свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними».

Защита возможности реализации данного конституционного права в пределах, установленных законом, может осуществляться различными средствами. Поскольку общественно опасные деяния, связанные с нарушением религиозных прав человека, являются уголовно-наказуемыми, рассмотрим особенности их защиты с использованием уголовно-правовых средств.

Так, статьей 148 УК РФ установлена уголовная ответственность за совершение таких публичных действий, которые выражают неуважение к обществу и совершены в целях оскорбления религиозных чувств верующих. В качестве квалифицирующего признака выступает совершение таких действий «в местах, специально предназначенных для проведения богослужений, других религиозных обрядов и церемоний».

Поскольку нарушение религиозных прав может заключаться не только в совершении таких действий, но в воспрепятствовании деятельности религиозных организаций, то части 3 и 4 данной статьи гласят, что уголовно-наказуемыми деяниями признается также незаконное воспрепятствование деятельности таких организаций или «проведению богослужений, других религиозных обрядов и церемоний», в том числе «совершенные... лицом с использованием своего служебного положения» или «с применением насилия или с угрозой его применения».

Однако, при этом законодатель не учитывает, что совершение указанных противоправных действий может производиться с использованием средств массовой информации или различных интернет-ресурсов, что увеличивает аудиторию, к которой могут быть обращены призывы к осуществлению противоправной деятельности, а это повышает общественную опасность преступлений рассматриваемого вида.

В результате в анализируемой статье Уголовного кодекса отсутствует такой квалифицирующий признак как «с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», хотя он присутствует в ряде других статей УК РФ, когда речь идет об ответственности за призывы к осуществлению противоправной деятельности, звучащие публично (например, в ст.ст. 280, 280.1, 280.4 и 282 УК РФ).

Результаты сравнительного исследования соответствующих положений уголовного законодательства ряда зарубежных стран позволяют сделать вывод о том, что указанный перечень вопросов не является исключительным для Российской Федерации.

Проблема носит международный характер, потому что ответственность за совершение преступлений на почве религиозной вражды и мести регламентируется уголовным законодательством большого числа государств.

В большинстве уголовных кодексов государств — участников СНГ использование сети «Интернет» упоминается в контексте установления уголовной ответственности за совершение преступлений, связанных с возбуждением вражды и ненависти (в том числе, на религиозной почве), пропагандой идей вражды и ненависти, распространением клеветы, оскорблений и т.п. Исключение составляет только УК Республики Армения.

Так, например, в Уголовном кодексе Республики Беларусь возможность совершения преступлений с использованием сети «Интернет» указана не только применительно к клевете (ст. 188 УК РБ), но и к отрицанию геноцида белорусского народа (ст. 130-2 УК РБ), а также пропаганде терроризма (ст. 289-1 УК РБ). Вместе с тем упоминание о возможности нарушения равноправия граждан (ст. 190 УК РБ) или воспрепятствование законной деятельности религиозных организаций (ст. 195 УК РБ) с использованием интернет-ресурсов законодатель упоминать не считает необходимым[1].

[1] Уголовный кодекс Республики Беларусь // Pravo.by : национальный правовой Интернет-портал Республики Беларусь : сайт. URL: https://pravo.by/document/?guid=3871&p0=hk9900275 (дата обращения: 01.11.2023).

Аналогичен подход законодателя к формулированию диспозиции статьи 143 Уголовного кодекса Туркменистана, в которой отсутствует упоминание использования сети «Интернет» для нарушения равноправия граждан, тогда как оно присутствует в иных статьях Кодекса[1]. Во многом сходным является подход, реализованный в Уголовном кодексе Республики Узбекистан и в Уголовном кодексе Республики Таджикистан[2].

Более предпочтительной представляется позиция, нашедшая отражение в Уголовном кодексе Республики Казахстан[3], в котором статья 174, установившая ответственность за разжигание, в том числе религиозной розни, оскорбление религиозных чувств граждан, а также пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, публичность указанных действий раскрывает через упоминание использования средств массовой информации или сетей телекоммуникаций. Вместе с тем, в рассматриваемой статье также отсутствует явное указание на использование информационно-телекоммуникационной сети «Интернет», в то время как в ст.ст. 105, 132, 134, 147, 272, 380 и 409 УК КР использование интернет-ресурсов прямо указано в качестве квалифицирующего признака.

Особое место в числе реализованных в уголовном законодательстве государств – участников СНГ подходов занимает позиция, нашедшая отражение в Уголовном кодексе Республика Молдова. В Общей части УК Республики Молдова раскрывается содержание ряда понятий, используемых в кодексе[4]. Однако упоминание информационно-телекоммуникационных сетей как места

---

[1] Уголовный кодекс Туркменистана // United Nations Turkmenistan : сайт. URL: https://www.untuk.org/publications/legislation/ug_kod/ (дата обращения: 15.11.2023).

[2] Уголовный кодекс Республики Узбекистан // LexUZ on-line : сайт. URL: https://lex.uz/acts/111457 (дата обращения: 15.11.2023) ; Уголовный кодекс Республики Таджикистан // Информационная Система Континент : сайт. URL: https://continent-online.com/Document/?doc_id=30397325 (дата обращения: 15.11.2023).

[3] Уголовный кодекс Республики Казахстан // Информационно-правовая система нормативных правовых актов Республики Казахстан : сайт. URL: https://adilet.zan.kz/rus/docs/K1400000226 (дата обращения: 01.11.2023).

[4] Уголовный кодекс Республики Молдова // Информационная Система Континент : сайт. URL: https://continent-online.com/Document/?doc_id=30394923 (дата обращения: 15.11.2023).

совершения преступления в статьях УК Республики Молдова присутствуют только применительно к информационным преступлениям и преступлениям в области электросвязи и также без упоминания конкретной сети – «Интернет».

Во многом небезупречны и подходы законодателей иных государств.

Так, в уголовном кодекс Федеративной Республики Германия имеются статьи, схожие с анализируемыми статьями УК РФ, а именно § 166 УК ФРГ, которая закрепляет, что «оскорбление вероисповедания, религиозных обществ и мировоззренческих объединений», которое может быть нанесено публично или посредством распространения материала, оскорбляющего суть религиозного или мировоззренческого исповедания других лиц, является уголовно-наказуемым деянием[1].

Этой же нормой установлена уголовная ответственность за публичное или путем распространения материалов (письменных материалов) оскорбление церкви, действующей на территории Германии, или другого религиозного общества или мировоззренческой организации, их организации или обычаям.

При этом системное толкование норм позволяет сделать вывод о том, что речь может идти и об ответственности за действия, связанные с теми материалами, которые распространяются с использованием различных интернет-ресурсов, поскольку § 11 УК ФРГ разъясняет нам, что под такими материалами (письменными материалами) понимаются «таковые, которые содержатся в письменных материалах, на носителях аудио- и видеозаписи, накопителях данных, в репродукциях или воплощаются иным образом, или также таковые, которые передаются независимо от их сохранения посредством информационной или коммуникационной техники», что включает в себя понятие «с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет».

[1] Головненков П. В. Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB) : научно-практический комментарий и перевод текста закона // Universität Potsdam : сайт. URL: https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cberset zung_von_Pavel_Golovnenkov.pdf (дата обращения: 01.11.2023).

Не меньший интерес для исследования при изучении указанных вопросов представляет и уголовное законодательство Швеции. Секция 8 Главы 16 Уголовного кодекса Швеции, во многом аналогичная рассмотренным выше нормам, гласит, что заявление или иное распространенное сообщение, которое выражает неуважение к группе населения, намекая, в том числе, на религиозные убеждения, поскольку оценивается, как агитация против группы населения, также является уголовно-наказуемым деянием[1].

В данном случае, когда речь идет о распространении информации, способ распространения тоже не специфицирован, законодатель принял решение ограничиться словосочетанием «в распространенном заявлении или сообщении», что включает в себя распространение через информационно-телекоммуникационные сети.

В определенной мере сходный с подходом, использованным при формулировании соответствующих положений Уголовного кодекса Швеции, и подход законодателя, в соответствии с которым в Уголовном кодексе Италии, также не выделяя в качестве самостоятельной нормы, устанавливающей уголовную ответственность за нарушение прав групп людей, объединенных одинаковым вероисповеданием, совершение преступления с использованием сети «Интернет» закреплено в качестве квалифицирующего признака только применительно к совращению несовершеннолетних (статья 609-undecies)[2].

Интересным в свете определенных событий также представляется рассмотрение формулировок, использованных законодателем в Государстве Израиль. В аналоге уголовного кодекса этой страны рассматриваемому вопросу посвящена целая глава. В данном случае, следует обратить внимание на то, что в Законе об уголовном праве Израиля не встречается слово «Интернет» и квалифицирующий признак «с использованием сети «Интернет»» или его вариации.

[1] The Swedish Criminal Code // Government Offices of Sweden : сайт. URL: https://www.government.se/4b0103/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminalcode.pdf (дата обращения: 01.11.2023).

[2] Code of Criminal Procedure // ICC Legal Tools Database : сайт. URL: https://www.legal-tools.org/doc/aee4e8/pdf/ (дата обращения: 01.11.2023).

Таким образом, результаты сравнительного анализа соответствующих статей ряда уголовных кодексов позволяют сделать несколько выводов.

Во-первых, законодательство не только Российской Федерации, но и ряда других государств справедливо рассматривает нарушение прав групп людей, объединенных одинаковым вероисповеданием, как серьезное преступление, за которое установлена уголовная ответственность и должно быть назначено наказание, в том числе, связанное с лишением свободы.

Во-вторых, отсутствие в качестве признака или квалифицирующего признака нарушения конституционного права на свободу совести и вероисповедания указания на возможность его совершения с использованием сети «Интернет» или аналогичного наблюдается в уголовном законодательстве не только Российской Федерации, но и ряда других стран. Вместе с тем, уровень развития информационных технологий на современном этапе таков, что интернет-пространство используется в целях обеспечения достижения преступных целей, поскольку позволяет вовлекать в преступную деятельность все большее количество людей, а применительно к рассматриваемым вопросам — существенно увеличивать количество лиц, чьи религиозные права и чувства могут быть нарушены, подвергнуты оскорблениям и т. п.

Определяя религиозные чувства, как объект, требующий повышенной защиты, законодатель должен принять все меры для того, чтобы обеспечить необходимый уровень эффективности такой защиты. Представляется, что это возможно только в случае обеспечения логичности и единства подходов при формулировании диспозиций статей, объединенных тем или иным признаком.

Следует обеспечить единство подходов к определению мотива религиозной вражды или ненависти в качестве обстоятельства, отягчающего не только наказание, но и ответственность. И реализуя единство подходов, в диспозиции статей, устанавливающих уголовную ответственность за нарушение религиозных прав граждан, совершаемых путем выполнения действий пропагандистского характера или связанных с распространением идей ненавистнического характера, включить признак совершения этих действий с использованием

средств массовой информации и информационно-телекоммуникационных сетей, включая сеть «Интернет», в качестве квалифицирующего.

Применительно к рассмотренным в статье вопросам видится необходимым внести дополнения, в том числе, в статью 148 УК РФ и аналогичные статьи уголовных кодексов иных государств, указав, что использование средств массовой информации и информационно-телекоммуникационных сетей, в том числе сети «Интернет», при совершении преступлений следует рассматривать как квалифицирующий признак.

УДК 343.34

С. Н. ТИТОВ

ПРИЗНАК ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОСТАВАХ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

По данным МВД России, в 2022 году с использованием кибертехнологий совершалось каждое четвертое преступление в стране[1].

На момент вступления в силу Уголовного кодекса Российской Федерации в нем не содержалось упоминания об информационных технологиях. По истечении 25 лет они только в качестве квалифицирующего признака указаны в 27 составах преступлений.

При этом в российской науке и документах стратегического государственного планирования отсутствует ясное концептуальное понимание того, насколько сильно и в каких направлениях должно измениться уголовное право под влиянием «виртуализации» жизнедеятельности, развития систем обработки и передачи информации и развития систем искусственного интеллекта[2].

Все это говорит не просто об актуальности, а о злободневности исследования вопросов уголовно-правового противодействия киберпреступле-

[1] Краткая характеристика состояния преступности в Российской Федерации за январь—декабрь 2022 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 29.04.2023).

[2] Бабаев М. М., Пудовочкин Ю. Е. Проблемы российской уголовной политики. М., 2014. С. 93.

ниям. Чрезвычайно важными эти вопросы являются применительно к преступлениям против интеллектуальной собственности, поскольку последняя приставляет собой информацию, а значит крайне подвержена незаконному использованию, изменению и передаче с помощью информационных технологий.

Очертим круг преступлений, относимых к преступлениям против интеллектуальной собственности. Это составы незаконного использования объектов авторского права (ст. 146 УК РФ) и патентных прав (ст. 147 УК РФ). К этой же категории преступлений относятся незаконные действия в отношении товарного знака (ст. 180 УК РФ).

Сложнее обстоит дело с незаконными действиями в отношении сведений, составляющих ту или иную тайну (ст. 183 УК РФ). Системный анализ ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и ст. 1465 ГК РФ позволяет заключить, секрет производства (ноу-хау) и сведения, составляющие коммерческую тайну, суть одно и то же. В связи с этим к преступлениям против интеллектуальной собственности следует относить преступления, предусмотренные ст. 183 УК РФ, в части незаконных действий в отношении сведений, составляющих коммерческую тайну.

Следует конкретизировать, в каких аспектах следует исследовать вопросы, связанные с использованием таких технологий при совершении преступлений против интеллектуальной собственности. Представляется, что таких аспектов три, – использование при совершении преступлений компьютерной информации, информационно-телекоммуникационных сетей, включая сеть «Интернет», и использование при совершении преступлений технологий искусственного интеллекта.

Исходя из п. 1 примечаний к ст. 272 УК РФ под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов.

Поскольку интеллектуальная собственность зачастую представлена в виде компьютерной информации, неправомерные манипуляции с послед-

ней ставят вопрос о квалификации соответствующих деяний. Ответственность за неправомерные действия с компьютерной информацией предусмотрены нормами главы 28 УК РФ.

Из содержащихся в ней составов наиболее вероятными деяниями, сопряженными с преступлениями против интеллектуальной собственности, являются неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Вопрос о квалификации незаконных действий в отношении интеллектуальной собственности, сопряженных с преступлениями в сфере компьютерной информации, решен Пленумом Верховного Суда Российской Федерации следующим образом.

Если действия, оцениваемые как преступления в сфере компьютерной информации, были способом совершения преступления против интеллектуальной собственности, квалификация осуществляется по совокупности преступлений[1]. Аналогичный подход должен, очевидно, применяться и в отношении прав на средства индивидуализации и секреты производства.

Иначе обстоит дело с использованием информационных систем. В настоящее время использование сетей никак не учитывается в составах преступлений против интеллектуальной собственности. Между тем, повышенная общественная опасность совершения преступления таким способом не вызывает сомнений.

В УК РФ квалифицирующий признак преступления, связанный с использованием информационных технологий, встречается в нескольких формулировках: «то же деяние, совершенное в… информационно-телекоммуникаци-

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

онных сетях» (ч. 2 ст. 110 УК РФ), «… с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» (ч. 2 ст. 128[1] УК РФ), «… с использованием… информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ч. 3 ст. 133 УК РФ), «… с использованием… электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ч. 2 ст. 205[2] УК РФ) и др. В целом все формулировки близки по значению. Они встречаются в составах преступлений, которые предполагают какую-либо коммуникацию.

Согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Использование сетей повышает степень общественной опасности деяния за счет упрощения совершения деяния, анонимности преступников, а также массовости, быстроты и глубины проникновения негативного информационного воздействия на общество[1].

Использование информационных технологий приводит к высокой латентности преступлений. По некоторым данным она доходит в этом случае до 90 %[2]. Это является еще одним поводом для усиления ответственности за такие преступления.

В законотворческой практике последних лет имеются удачные примеры на этот счет. Например, ст. 228.1 УК РФ содержит квалифицированный состав – совершение этого деяния с использованием сети «Интернет».

В подобных преступлениях использование сети облегчает передачу информации, расширяет аудиторию преступника, повышает его анонимность, делает неважной место его нахождения, упрощает обмен денежными средствами.

---

[1] Косарев М. Н. Информационно-телекоммуникационные сети как признак преступления // Вестник Уральского юридического института МВД России. Екатеринбург, 2014. № 2. С. 56.

[2] Рассолов И. М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 45.

Согласимся здесь с Е.А. Русскевичем в том, что квалифицирующий признак должен вводиться в тех случаях, когда использование информационных технологий способно привести к повышению общественно опасных последствий[1].

Таким образом, использование информационных технологий должно признаваться квалифицирующим признаком преступления тогда, когда оно существенно облегчает его совершение, ведет к расширению числа получателей деструктивной информации или незаконных товаров и веществ и в перспективе способно увеличить число совершаемых преступлений.

Квалифицирующий признак использования сетей применим не ко всем составам преступлений против интеллектуальной собственности. Представляется, что составы плагиата и разложения сущности объектов промышленной собственности, во всяком случае в настоящее время, не соответствуют описанным выше критериям введения квалифицированного состава, связанного с использованием информационных технологий. Еще одним аргументом здесь может быть нулевая статистика преступности по этим статьям[2].

Зато этим критериям вполне соответствуют незаконное использование объекта интеллектуальной собственности и приобретение, хранение, перевозка контрафактных экземпляров объектов интеллектуальной собственности. Типичными для данной категории дел являются следующие обстоятельства.

Имея умысел на незаконное использование объектов авторского права в целях сбыта, М. в период с октября 2016 года по 7 ноября 2016 года в сети «Интернет» приобрел программное обеспечение корпорации <...> и <...>, после чего М. указанное программное обеспечение с признаками контрафактности хранил на электронных носителях информации до 7 ноября 2016 года[3].

---

[1] Русскевич Е. А. Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 78.

[2] Сводные статистические сведения о состоянии судимости в России за 2022 год // Судебный департамент при Верховном Суда Российской Федерации : сайт. URL: https://www.cdep.ru/index.php?id=79&item=7649 (дата обращения: 30.04.2023).

[3] Приговор Октябрьского районного суда г. Ростова-на-Дону от 20 февраля 2017 г. по делу № 1-160/2017 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 12.11.2023).

В данном примере сеть «Интернет» явилась источником получения виновным контрафактной продукции и способом связи с клиентом. Это в точности соответствует критерию облегчения совершения преступления, описанному нами выше.

Предлагается включить использование сети «Интернет» в качестве квалифицирующего признака незаконного использования объектов интеллектуальной собственности, приобретения, хранения, перевозки контрафактных экземпляров объектов интеллектуальной собственности, незаконного собирания и разглашения сведений, составляющих коммерческую тайну.

В отношении этих же составов стоит рассмотреть вопрос об усилении ответственности при использовании систем искусственного интеллекта.

Технологии искусственного интеллекта в настоящее время получают взрывное развитие. В нашей стране это связано и с экономическими, и с техническими причинами, и с позицией руководства страны, оказывающего всемерную поддержку этим процессам. На конференции по искусственному интеллекту 24 ноября 2022 г. Президент России В.В. Путин заявил: «Задача нового этапа в горизонте текущего десятилетия – обеспечить именно массовое внедрение искусственного интеллекта. Оно должно охватить все отрасли экономики, социальной сферы и систему госуправления»[1].

Несомненными являются достижения в этой области. В то же время технологии искусственного интеллекта, имеющие неоспоримое значение для социальной сферы и экономики, являются эффективным вредоносным орудием в руках преступников.

И.Р. Бегишев, З.И. Хисамова выделяют два вида криминологических рисков применения искусственного интеллекта – прямой и косвенный. Прямой риск связан с непосредственным действием на человека и гражда-

[1] URL: https://kremlin.ru/events/president/news/69927 (дата обращения: 10.02.2023).

нина той или иной опасности, вызванной применением искусственного интеллекта. Косвенный связан с непреднамеренными опасностями в контексте применения таких систем[1].

Представляется, что в случае с интеллектуальной собственностью применение технологий искусственного интеллекта должно быть учтено как квалифицирующий признак преступления, поскольку способно многократно увеличить общественную опасность деяния, будучи потенциально совершенно не ограничено в масштабах получения, обработки и распространения информации.

Таким образом, использование информационных технологий должно влечь более строгую ответственность в тех случаях, когда оно существенно облегчает совершение преступления, ведет к расширению числа получателей деструктивной информации или незаконных товаров и веществ и в перспективе способно увеличить число совершаемых преступлений.

Квалифицирующий признак преступлений против интеллектуальной собственности, связанный с использованием информационных технологий, может быть сформулирован следующим образом: «деяние, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», либо с использованием систем искусственного интеллекта».

УДК 343

Н. В. ТЫДЫКОВА

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПОЛОВЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ДИСТАНЦИОННЫМ СПОСОБОМ

Пункт «б» ч. 3 ст. 133 УК РФ предусматривает такое квалифицирующее обстоятельство, как использование средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет».

[1] Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 775.

Другие составы половых преступлений не содержат такого же квалифицирующего признака. Но среди всех преступлений, ответственность за которые предусмотрена главой 18 УК РФ, чаще всего таким способом совершаются развратные действия и насильственные действия сексуального характера в отношении лиц, не достигших двенадцати лет.

Однако не усматривается оснований, с которыми можно было бы связать существенное повышение уровня общественной опасности понуждения к действиям сексуального характера, учитывая персонифицированный характер такого воздействия.

Вряд ли более общественно опасными становятся и развратные действия или насильственные действия сексуального характера, совершаемые таким способом. Очевидно, что более опасны они именно при контактном совершении.

Поэтому применительно к группе половых преступлений их совершение с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», интересен не в связи с необходимостью выделения соответствующего квалифицирующего обстоятельства и даже не в связи с необходимостью конструирования отдельного состава, в чем также не видится необходимости, а в связи с тем, что такой способ их совершения требует решения ряда квалификационных вопросов.

Так как развратные действия и насильственные действия сексуального характера с использованием сети «Интернет» совершаются в отношении определенной возрастной категории несовершеннолетних потерпевших, то одним из вопросов квалификации является вопрос об установлении виновным знания об их возрасте.

Правила установления осознания виновным возраста потерпевшего, сложившиеся в правоприменительной практике применительно ко всем случаям, требуют уточнения с учетом специфики дистанционного способа совершения деяния.

Не вызывают серьезных проблем ситуации, когда виновный вступает в общение с ранее знакомым потерпевшим в социальных сетях или мессенджерах, или потерпевшие в переписке или среди анкетных данных сообщают свой возраст.

Квалификация усложняется, если потерпевшее лицо в анкетных данных указывает возраст старше, чем им или ей фактически достигнут, а в переписке – реальный или возраст не указывается, а вопрос о нем не становится предметом беседы виновного и потерпевшей, а также когда потерпевшие размещают на своей странице в социальной сети фотографию с изображением взрослого человека или свою, но с ярким макияжем и во взрослой одежде.

Однако говорить о невозможности установления осознания виновным реального возраста потерпевшего в таких случаях нельзя. Знание виновного о недостижении потерпевшим определенного возраста, в частности, может быть основано на следующих обстоятельствах: оценка виновным возраста по внешним признакам изображения потерпевшего на фото или видео, по голосовым признакам возраста, иной информации, размещенной на странице потерпевшего в социальной сети, исходя из контекста получаемых от потерпевшего сообщений.

Деяние не может квалифицироваться как совершенное в отношении потерпевшего, не достигшего определенного возраста, если виновный заблуждался относительно возраста потерпевшего в силу введения его в заблуждение самим потерпевшим путем сообщения недостоверной информации о своем возрасте, размещении фотографий, на которых он выглядит старше своего возраста, при использовании технических средств коррекции внешности в ходе общения с использованием видеосервисов или иными способами.

Если лицо полагает, что совершает половое преступление в отношении лица, не достигшего определенного возраста, а на самом деле лицо такого возраста достигло, то квалифицировать содеянное необходимо по направленности умысла, т. е. как покушение на соответствующее преступление.

Аналогичным образом необходимо квалифицировать и отправление сообщений соответствующего содержания лицу, не достигшему определенного возраста, если оно не ознакомилось с ними.

Анализ правоприменительной практики показал, что существенная часть таких действий имеет «гибридный» характер, когда часть действий виновные совершают дистанционно, например, в ходе переписки, пересылки фото и видео, а часть — контактно при личной встрече.

Квалификация таких случаев будет зависеть от того в какой момент времени виновный узнал о возрасте потерпевшего.

Если в момент первых действий, совершаемых дистанционно, виновный заблуждался относительно возраста потерпевшего лица, полагая, например, что ведет переписку со взрослым лицом, то его действия как развратные или насильственные сексуального характера могут быть квалифицированы только те, которые были совершены, когда возраст потерпевшего лица ему стал известен (например, визуально при встрече).

Анализ практики показывает, что таких случаев немного, так как виновные, как правило, осуществляют в социальных сетях поиск потерпевших определенной возрастной категории, совершают первые эпизоды таких преступлений для того, чтобы другие совершить контактным способом.

Либо, наоборот, первые эпизоды совершаются контактно, а другие, так как социальные сети, мессенджеры и другие средства дистанционного общения стали обычной частью жизни, — дистанционно. Практика знает случаи, когда действия подобного рода совершались длительный период времени в «гибридном» формате, однако не выработала подхода к их оценке как единого преступления или необходимости квалификации по совокупности преступлений.

Совершение половых преступлений с использованием информационно-телекоммуникационных сетей также предполагает некоторые особенности установления других признаков. Например, особенных подходов требует институт соучастия, вопросы которого всегда разрабатывались в приложении к контактно совершаемым действиям.

Приватность действий, совершаемых с использованием информационно-телекоммуникационных сетей, обуславливает то, что, чаще всего половые преступления совершаются именно одним лицом, однако встречаются в практике последних лет и совершаемые в составе группы лиц.

Так, например, Ф. договорилась с С. за материальное вознаграждение совершить насильственные действия сексуального характера в отношении своих малолетних детей, а также воспитанников детского сада, в котором работала, и продемонстрировать эти действия посредством голосовой и видеосвязи.

Обоснованием того, что подобные действия образуют соисполнительство, стало описание этих действий как двухстороннего процесса: Ф. совершает физические действий сексуального характера в отношении малолетних, а С. наблюдает за этим, что известно и потерпевшим, которые воспринимают происходящие действия как совершаемые в отношении них двумя лицами, одно из которых действует дистанционно.

При этом, Ф. и С. действуют согласованно, поддерживая связь в процессе выполнения описанного преступления. С учетом того, что подобные случаи, к сожалению, не являются редкостью в правоприменительной практике, целесообразно в соответствующем Постановлении Пленума Верховного Суда Российской Федерации закрепить разъяснение относительно того, что действия лиц могут быть квалифицированы по признаку их совершения группой лиц или группой лиц по предварительному сговору, в том числе, и тогда, когда виновные, действуя согласованно, выполняют объективную сторону соответствующего преступления с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Однако такие случаи необходимо отличать от совершаемых также в соучастии, но с распределением ролей, когда, одно из двух лиц выполняет действия, свойственные для пособника или подстрекателя. Например, только обеспечивает техническую связь или только порождает у другого лица совершить подобное преступление. Аналогичные вопросы требуют разрешения и при совершении действий сексуального характера в отношении несовершен-

нолетних соответствующих возрастных категорий при их трансляции для зрителей. В ряде случаев и для зрителей не исключена квалификация действий как соответствующего полового преступления, совершенного в соучастии.

Совершение половых преступлений с использованием информационно-телекоммуникационных сетей ставит и проблему их квалификации по совокупности с другими преступлениями.

Например, предусмотренных ст.ст. 137, 242, 242.1, 242.2 УК РФ. В правоприменительной практике, чаще всего, квалификация в необходимых случаях осуществляется по совокупности ст.ст. 135 или 132 УК РФ и соответствующим из указанных составов преступлений. Однако можно встретить и случаи, когда они не вменяются дополнительно.

Эта проблема является частью более общего вопроса о дополнительной квалификации действий, которые, образуя самостоятельный состав преступления, могут быть способом выполнения объективной стороны другого преступления.

В качестве универсального правила видится такое: если способ, который сам по себе образует состав самостоятельного преступления, специально не указан в норме об ответственности за другое преступление, то требуется дополнительная квалификация по статье об ответственности за деяние, ставшее таким способом.

Например, если виновный совершает в отношении потерпевшего, не достигшего двенадцати лет, действия сексуального характера и осуществляет видеозапись, то при установлении соответствия такой записи предмету рассматриваемого преступления и соответствующей цели (например, последующего распространения), дополнительно должен вменяться состав преступления, предусмотренный п. «а», «г» ч. 2 ст. 242.1 УК РФ.

С учетом положений примечания 1 к ст. 242.1 УК РФ под порнографическими материалами необходимо понимать не только изображения, но и соответствующие описания половых органов или действий сексуального характера. Поэтому совокупность с соответствующим пунктом части ст. 242.1

УК РФ возможна и в случае аудиозаписи разговоров соответствующего содержания.

В тех случаях, когда текст переписки подпадает под признаки порнографических описаний и установлена одна из целей, указанных в ч. 1 ст. 242.1 УК РФ, то такая совокупность также может иметь место. Также видится правильным в случае фактического распространения видеоматериала, фото, аудиозаписи или текстовых сообщений, содержанием которых является еще и личная или семейная тайна, квалифицировать содеянное по совокупности со ст. 137 УК РФ.

Статья 242.2 УК РФ предусматривает ответственность за фото-, кино- или видеосъемку несовершеннолетнего в целях изготовления и (или) распространения порнографических материалов или предметов, совершенные лицом, достигшим восемнадцатилетнего возраста. Не исключена уголовная ответственность по совокупности преступлений, предусмотренных статьями 132 или 135, 242, 242.1 и 242.2 УК РФ.

Если насильственные действия сексуального характера совершаются путем отправки малолетним, не достигшим двенадцатилетнего возраста, фото- и видеоизображений порнографического характера, требуется дополнительная квалификация по ст. 242 УК РФ.

Такая позиция сегодня является доминирующей в литературе[1], хотя отдельные авторы и отмечают, что в правоприменительной практике можно встретить отдельные случаи, когда этот состав не вменяется в совокупность[2].

Однако с учетом того, что ст. 242 УК РФ устанавливает ответственность за распространение, которое предполагает передачу соответствующего предмета группе лиц или неограниченному кругу лиц[3], то пересылка фото, видео

---

[1] Коняхин В. Развратные действия // Законность. 2008. № 12. С. 16—17 ; Миллерова Е. А. О некоторых проблемах квалификации развратных действий, сопряженных с изготовлением и распространением порнографических материалов // Уголовное право. 2015. № 2. С. 36—39.

[2] Скворцова О. В., Макаренко Д. Д. Развратные действия с использованием сети «Интернет» // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2021. Т. 7 (73), № 1. С. 150—151.

[3] Шарапов Р. Д. Преступления против общественной нравственности : учебное пособие. СПб., 2022. С. 49.

или текстового сообщения одному лицу, не достигшему определенного возраста, не образует состава рассматриваемого преступления и, соответственно, не требует дополнительной квалификации. Вероятно, этим и объясняется разность подходов правоприменителей.

Также для решения вопроса о совокупности рассматриваемых преступлений необходимо анализировать субъективную сторону деяний. Так, П. на своей странице в социальной сети «ВКонтакте» разместил 2 видеозаписи порнографического характера, которые были доступны для просмотра всем пользователям социальной сети, в том числе и не достигшим шестнадцати лет, так как какие-либо ограничения для просмотра отсутствовали. Его действия были квалифицированы только по п. «б» ч. 3 ст. 242 УК РФ[1].

В таких случаях необходимо анализировать все обстоятельства содеянного для правильного установления субъективной стороны. Если виновный не предвидел возможности причинения вреда половой неприкосновенности и нормальному нравственному и половому развитию несовершеннолетних, например, указав в сопроводительной информации, что видео предназначено только для просмотра лицами, достигшими 18 лет, или не указал, но ввиду того, что его друзьями (подписчиками) являются только взрослые лица, он полагал, что только они будут знакомиться с предлагаемым контентом.

В таком случае при необходимой внимательности и предусмотрительности он мог и должен был предвидеть, что, так как пользователями указанной сети являются, в том числе и малолетние, то нельзя исключать и просмотр материала такими лицами.

Очевидно, что «средний пользователь» социальных сетей такое развитие событий бы прогнозировал и допускал. Все это говорит о неосторожной форме вины относительно демонстрации видео порнографического содержания лицам, не достигшим определенного возраста, что, конечно же,

[1] Приговор Усть-Куломского районного суда Республики Коми по делу № 1-72/2022. // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 14.11.2023).

не предполагает квалификации преступления, предусмотренного п. «б» ч. 3 ст. 242 УК РФ, по совокупности с развратными действиями или насильственными действиями сексуального характера.

Однако ситуация может быть иной, если, например, среди друзей и подписчиков виновного имеются в том числе (или только) лица, не достигшие шестнадцати лет или не достигшие двенадцати лет. Публикуя соответствующие материалы, такое лицо могло либо желать, чтобы они ознакомились с ними или сознательно допускать, соответственно либо желать нарушения их половой неприкосновенности и (или) нормального нравственного и полового развития, либо безразлично к этому относиться.

В этом случае требовалась бы квалификация по совокупности с соответствующим половым преступлением. Удачным видится критерий индивидуальной определенности, предлагаемый А.А. Энгельгардтом. Идея заключается в том, что если адресат информационного воздействия представлен индивидуально-неопределенным для виновного кругом лиц, то уместно говорить о преступлении, предусмотренном ст. 242 УК РФ[1].

Однако необходимо уточнить, что этот критерий в каждом конкретном случае также должен устанавливаться индивидуально. Так, если соответствующая информация размещена на странице пользователя, но доступна только для одного пользователя (или нескольких) или одному или нескольким пользователям направляется сообщение с предложением ознакомиться с такой информацией, то можно ставить вопрос о том, что такое информационное воздействие носит индивидуально-определенный характер.

В связи с тем, что дистанционно совершаемые развратные действия и насильственные действия сексуального характера в правоприменительной практике стали занимать существенную долю, в научной литературе можно встретить предложения о закреплении в тексте уголовного закона специального состава преступления. Но, думается, что вопросы криминализации и дифференциации уголовной ответственности не должны решаться в приложении

[1] Энгельгардт А. А. Система половых преступлений (в контексте примечания к статье 131 УК РФ) // Lex Russica. 2017. № 12. С 90.

к таким локальным вопросам, а требуют системного подхода и решений, обеспечивающих интересы всей системы норм об ответственности за посягательства на половую свободу и половую неприкосновенность.

Таким образом, в настоящее время правоприменительная практика имеет потребность в решении ряда вопросов квалификации, связанных с толкованием признаков половых преступлений, совершенных с использованием информационно-телекоммуникационных сетей.

УДК 343

К. А. ФЕДОТОВА

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ДЛЯ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

С помощью сети «Интернет» можно находить, передавать, обрабатывать и хранить информацию. Сеть «Интернет» позволяет нам выстраивать коммуникацию с человеком из любой точки земного шара, но кроме того, с помощью информации можно совершать преступления. При этом в сети «Интернет», есть социальные сети и мессенджеры.

Социальные сети выступают сейчас не только, как площадки для общения, но и как платформы, для рекламы товаров, услуг, обсуждения новостей, развития личного бренда.

При этом у преступников постоянно увеличивается возможность для совершения преступлений против собственности (ст. 158, ст. 159, ст.ст. 159.1-159.6 УК РФ). Но предметом преступлений, являются не только, имущество, но и сама информация (ст. 137, ст. 242 УК РФ).

Согласно статистике совершения преступлений, с 2020 года около 70 процентов всех хищений, совершенных с помощью обмана или злоупотребления доверием, именно с помощью информационно- телекоммуникационных сетей, а в частности с помощью сети «Интернет». Рост преступлений пришелся на 2020 год, т. к. в данный момент в России началась пандемия COVID-19. Люди перестали выходить из дома и начали 99 процентов времени проводить за компьютером или ноутбуком, соответственно стали заказывать товары, услуги, покупать курсы, общаться в сети «Интернет».

В сети «Интернет» есть области, в которых можно хранить и открывать любую информацию, не оставляя следов, она получила название теневая сторона сети «Интернет» или «DarkNet».

Для начала стоит сказать, что у сети «Интернет», как у информационно-телекоммуникационной сети, есть несколько уровней. Первый уровень — общедоступный, мы попадаем в него через поисковые системы, т. е. для того, чтобы поучать информацию на этом уровне, не нужно использовать специальные программы или специальный язык.

Для доступа ко второму уровню необходимо использовать специальные программы по типу «Tor». Данный уровень включает в себя защищенные ресурсы. Данный уровень подразумевает, что пользователи должны аутентификацию (необходимо подтвердить данные учетной записи или данные о личности), как правило такую систему используют скрытые сайты, криптовалюты биржи, финансовые сервисы, торговые площадки.

Третий уровень является самым глубоким уровнем сети «Интернет». Он как правило используется для скрытой коммуникации и обмена информацией между организациями и группами. Попасть в глубокие слои «DarkNet» можно только через программы «Freenet» и «I2P».

Теневая сторона интернета не безопасна, т.к. киберпротоколы, которые используются для передачи и обработки данных не обеспечивают защиту, соответственно мы получаем уровни на котором данные в полной мере не защищенный, могут переходить из одних рук в другие.

В июле 2023 года группа хакеров, которые имеют себя «BlackCat» вскрыли базы данных медицинских учреждений Великобритании, так объектами атаки стали больницы Barts Health — столичного треста NHS, объединяющего шесть больниц и 10 медицинских центров в лондонском Сити и Ист-Энде.

В руки группировки попали данные, включая конфиденциальную информацию о двух с половиной миллионов человек, банковские реквизиты, личные данные, диагнозы и многое другое.

Таким образом, информационно-телекоммуникационные технологии облегчают нам жизнь, делая ее проще и мобильнее, но при этом все наши данный открытый и доступны для всех.

Информация связана с личностью, отсюда вытекает, что с помощью информационно-телекоммуникационной сети и средств массовой информации можно совершить преступления против личности.

В 2016 году журналистка Галина Мурсалиева подготовила материал для «Новой Газеты». В рамках, проведенного журналистского расследования раскрывалась тема «групп смерти», журналистка, говорила, что в период с ноября 2015 по апрель 2016 года зафиксировано 130 случаев самоубийства несовершеннолетних.

Как утверждает автор, все подростки состояли в одних и тех же интернет-группах, а семьи их были благополучными. В материале приведены две истории о реальных самоубийствах двух девочек-подростков, автор статьи указала, что подлинные имена героев изменены, но они есть в редакции, а далее идет рассказ о том, как проходило расследование.

Также в своей работе Галина Мурсалиева, говорила о том, что известно следствию, какие показания дали родители погибших детей и их ближайшее окружение. Материал произвел огромный общественный резонанс, что привело к тревожности и паники в обществе, но потенциальный преступник или преступники, могли выяснить подлинные имена свидетелей и их контактную информацию, начать угрожать в социальных сетях и заставить изменить показания.

Таким образом, данный материал должен был привлечь внимание общественных организаций, родителей, правоохранительных органов, но вместо этого привел к развитию паники, а вместе с тем указал преступникам на то, что известно следствию.

В настоящее время широкое распространение получили стриминговые площадки, которые позволяют размещать видео-контент, а также вести трансляции в режиме реального времени. Самыми распространенными стриминговыми платформами, являются: YouTube, Twitch, FacebookLive (запрещен на территории Российской Федерации), Viemo и т. д.

Стриминговые площадки начали появляться в 2010 году и к 2023 году начали вытеснять средства массовой информации, а также социальные сети.

Феномен стриминговых платформ, аналогичен феномену реалити шоу. Пользователи снимают юмористические ролики, играют в игры в онлайн формате, но когда стриминговые площадки начали авторам контента приносить донаты (или деньги), то погони за лайками и просмотрами стали переходить все законные границы.

Авторы контента смотрели, как далеко они могут зайти и сколько могут заработать на «хайпе».

В октябре 2020 года популярный стример «Mellstory» (Андрей Бурмин) во время своего стрима на аудиторию в 100 000 тысяч человек избивал и унижал модель Аллу Ефремову. Он ударил несколько раз девушку лицом об стол, в результате чего у нее были разбиты губы, пострадали зубы и были многочисленные кровоподтеки на лице.

Таким образом, хотелось бы отметить, что средства массовой информации и информационно-телекоммуникационная сеть «Интернет» способны управлять психоэмоциональным фоном людей.

В сети «Интернет» можно анонимно выплескивать свою агрессию и получать доход, с помощью криптографических ключей получать данные о пользователях и продавать крупным корпорациям или иным заинтересованным структурам, а можно причинять вред людям, при этом физический с ними не контактируя.

Получать признание от общества, в виде лайков и комментариев, но при этом лишать жизни людей.

Отсутствие детального законодательного регулирования, а также полная анонимность в информационно-телекоммуникационных сетях позволяет людям выражать свою агрессию, которая доходит до крайних форм, а именно убийств, за которое не всегда преступники получают заслуженное наказание.

Средства массовой информации, также, как и сеть «Интернет», позволяют получать преступникам информацию, следить за ходом расследования и заметать следы.

СМИ не проверяют материал, а пытаются гиперболизировать новости, чтобы прилечь внимание правоохранительных органов, но на самом деле до окончания следствия дают возможность преступникам замести следы.

Без четкого механизма правового регулирования средств массовой информации и информационно-телекоммуникационной сети «Интернет», а также открытости всех пользователей, мы будем получать площадки на которых будут формироваться идеологии и новые правила игры, где ключевым будет информация и отсутствие ответственности за ее ложное распространение.

УДК 343

В. В. ФИРСОВ

УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА КОНСТИТУЦИОННЫХ ПРАВ ГРАЖДАН В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Право на уголовно-правовую защиту и справедливое судебное разбирательство в сфере высоких технологий является одним из важнейших конституционных прав граждан. Участие государственных органов в создании условий для беспрепятственной реализации данного права заключается в обеспечении деятельности органов правосудия и исполнении судебных решений в принудительном порядке.

Гарантия реализации права на судебную защиту и справедливое судебное разбирательство в сфере высоких технологий предусматривает обеспечение

реального доступа граждан к правосудию, неукоснительное соблюдение процедуры судебного разбирательства, обеспечение предусмотренных прав и гарантий участников судебного процесса, а также возможности обжалования судебных решений. При этом справедливость понимается как обеспечение гарантий равенства граждан перед законом и судом, независимость, честность и беспристрастность судей при осуществлении правосудия.

Анализ поступивших жалоб в правоохранительные органы свидетельствует о наличии ряда проблем, возникающих при реализации гражданами вышеуказанных прав.

Чаще всего граждане жалуются на необоснованное затягивание сроков рассмотрения гражданских дел в суде. Судебные процессы, длящиеся порой годами, подрывают доверие к судебной власти.

Среди обращений, поступивших в правоохранительные органы, значительную часть составляют жалобы от граждан (в т. ч. осужденных) о несогласии с судебными постановлениями по уголовным делам и нарушении норм уголовно-процессуального законодательства в ходе предварительного следствия и суда. Большинство из вышеуказанных обращений содержали просьбу дать оценку вынесенным судебным постановлениями и оказать содействие в их отмене.

В подобных случаях изучались представленные материалы и заявителям разъяснялось, что в соответствии с конституционным принципом разделения властей, суды осуществляют судебную власть самостоятельно, независимо от чьей бы то ни было воли, подчиняясь только Конституции Российской Федерации и закону, что исключает вмешательство государственных органов (должностных лиц), в судопроизводство, а также разъяснялся порядок обжалования судебного решения.

Вместе с тем, в целях содействия восстановлению нарушенных прав и свобод человека и гражданина, при наличии оснований, Правоохранительные органы должны реализовывать предусмотренное законом право обращаться к должностному лицу, наделенному правом приносить кассационные

или надзорные представления на незаконные судебные постановления, и это дает свои положительные результаты, основываясь на нормах УК РФ.

В целях более эффективной защиты прав граждан в области уголовного судопроизводства, оказания содействия в проверке законности судебных решений и деятельности сотрудников правоохранительных органов, должно осуществляться взаимодействие с прокуратурой субъектов, Следственным комитетом, военной прокуратурой, транспортной прокуратурой, ГУВД по субъектам.

Такое взаимодействие позволяет не только оперативно восстанавливать нарушенные права и справедливость, но и преодолевать формальный и бездушный подход некоторых лиц правоохранительных органов, принимающих решения, нарушающие закон и права граждан.

Так, например, в правоохранительные органы обратился гражданин Т. с жалобой на постановление мирового судьи, оставленное без изменения апелляционной инстанцией, о признании его виновным в совершении административного правонарушения и лишении права управления транспортным средством на срок четыре месяца. Т. указал, что судебное решение принято с нарушением норм материального и процессуального права, в результате чего он лишен источника средств к существованию. Его самостоятельные обращения в различные государственные инстанции с целью восстановления нарушенных прав остались безрезультатными.

Изучив представленные материалы и посчитав доводы Т. обоснованными направил обращение прокурору субъекта с просьбой поручить проверить законность и обоснованность принятого решения. В результате проведенной проверки прокуратурой субъекта принесен протест на судебные постановления мирового судьи и апелляционной инстанции.

Анализ обращений показывает, что в последнее время уровень правового образования населения значительно вырос, также появилась явная заинтересованность граждан в отстаивании своих прав именно в рамках правового поля, в первую очередь с использованием административных и судебных процедур.

Деятельность судебных органов в социальном государстве является индикатором, объективно показывающим уровень гарантированности судебной защиты для каждого человека.

Проводимая судебная реформа в целом способствовала решению фундаментальных проблем в этой сфере, но одновременно выявила вопросы, требующие принятия безотлагательных мер.

Динамика, тенденции и актуальные проблемы судебной системы, характерные как для РФ в целом, так и для субъектов РФ, в том числе и для Санкт-Петербурга, наглядно отражаются в обзоре деятельности судов Российской Федерации за прошедший календарный год.

Так, данный обзор показывает, что в суды поступило более 1 млн уголовных дел, по которым в 80 % случаев вынесены обвинительные приговоры. Аналогичный порядок цифр имел место и в предыдущие годы. Таким образом, практически каждый год в России число граждан, осужденных за уголовно-наказуемые деяния, увеличивается на 1 млн чел.

Из года в год в суды направляется примерно одинаковое количество уголовных дел. При этом согласно судебной статистике, уменьшается, хотя и незначительно, количество дел по тяжким и особо тяжким преступлениям и, соответственно, увеличивается количество дел о совершении преступлений небольшой и средней тяжести.

Несмотря на меняющуюся структуру совершенных преступлений, статистика назначаемых видов уголовных наказаний показывает, что судебная практика принципиально не меняется. Самым распространенным видом уголовного наказания остается лишение свободы. Так, ежегодно к реальному лишению свободы осуждаются более 300 тыс. граждан, что составляет около 1/3 от общего числа осужденных[1].

[1] Минюст: число осужденных в колониях за 10 лет сократилось более чем в два раза // Ведомости : газета. 2023. 5 окт. URL: https://www.vedomosti.ru/society/news/2023/10/05/999038-chislo-osuzhdennih-v-koloniyah (дата обращения: 09.11.2023).

Вместе с тем виды наказания, не связанные с лишением свободы, следует шире применять при назначении наказаний лицам, совершившим преступления небольшой и средней тяжести, а также в сфере экономики. Назначение альтернативных лишению свободы видов наказания во многих случаях будет отвечать принципу соразмерности уголовного наказания за совершенное деяние, что в свою очередь повысит уровень доверия граждан к суду. И одновременно это будет целесообразно с экономической точки зрения для самого государства, учитывая, что расходы бюджета на содержание одного осужденного в большинстве случаев значительно превышают ущерб, причиненный им государству либо потерпевшему.

Вызывают озабоченность также показатели судебной статистики, характеризующие деятельность судов при рассмотрении ходатайств об избрании и продлении мер пресечения в виде заключения под стражу.

Законодатель определил, что данная мера пресечения должна применяться в исключительных случаях. Однако, как показывает судебная статистика, судами удовлетворяются 9 из 10 ходатайств органов предварительного следствия об избрании меры пресечения в виде заключения под стражу. Таким образом, складывается впечатление, что судьи идут на поводу у органов предварительного следствия и только в редких случаях отказывают в удовлетворении указанных ходатайств.

Анализ статистических показателей, характеризующих позицию судов при продлении сроков содержания под стражей, свидетельствует, что суды удовлетворяют данные ходатайства в 98,5 % случаев от общего числа поступающих ходатайств. При этом постановления судей фактически повторяют постановления об избрании меры пресечения, т.е. выносятся по тем же основаниям, изложенным в ходатайствах органов предварительного следствия. Однако данные основания не всегда являются бесспорными[1].

[1] Верховный Суд Российской Федерации : офиц. сайт. URL: https://www.vsrf.ru/about/info/systems/oficial_sait/ (дата обращения: 09.11.2023).

Необоснованные аресты в качестве меры пресечения приводят к тому, что значительное количество людей содержится под стражей не всегда законно. Как показывает статистика наказаний и данных об освобождении из мест изоляции от общества, нередко вина данных лиц в совершении инкриминируемых им уголовно-наказуемых деяний в установленном порядке не подтверждается.

Согласно анализу, проведенному Главным Управлением Федеральной службы исполнения наказаний, за 12 месяцев предшествующего календарного года из следственных изоляторов из-под стражи было освобождено незначительное количество человек.

Указанные лица обрели свободу в связи с изменением меры пресечения на иную, не связанную содержанием под стражей, прекращением дел органами следствия и судами, и по судебным приговорам – оправдательным либо обвинительным, когда в отношении осужденных назначаются наказания, не связанные с лишением свободы.

Кроме того, по данным статистики, в ходе судебного рассмотрения оправдано менее 0,5 % подсудимых, что также свидетельствует об обвинительном уклоне правосудия в целом, несмотря на процессуальные и материальные гарантии независимости суда.

Вышеуказанные проблемы в деятельности судебных органов являются актуальными и на государственном уровне. Министр юстиции Российской Федерации на международном юридическом форуме в мае 2022 г. обратил внимание на необходимость внесения изменений в систему правосудия, в целях повышения эффективности судебной власти для общества, государства и каждой личности.

Первостепенными задачами в рассматриваемой нами сфере являются внесение изменений в законодательство в части декриминализации деяний, не имеющих высокой степени общественной опасности, пересмотр принци-

пиальных подходов при применении наказаний, а именно - широкое использование альтернативных видов наказания, не связанных с лишением свободы, и изменение судебной практики.

Все это будет способствовать укреплению доверия граждан к судебной власти, веры в независимость судей и справедливость судебных решений. Деятельность органов правосудия, вызывающая уважение граждан, является таким же важным показателем благополучия человека, как политическая и экономическая стабильность.

УДК 343

П. В. ЦВЕТКОВ,
И. Д. ДРУК

КИБЕРПРЕСТУПЛЕНИЯ: ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ И КВАЛИФИКАЦИИ

В настоящее время все большую популярность набирает компьютерная преступность, что ставит под угрозу безопасность каждого человека, поскольку нарушаются его основные права, закрепленные в главе 2 Конституции Российской Федерации.

В зависимости от различных жизненных обстоятельств, большинство людей стали активными пользователями компьютеров, в том числе интернета, независимо от того, хотели они этого или нет. Например, многие работники вынуждены были выполнять свои трудовые функции дистанционно в связи со сложившейся эпидемиологической обстановкой, вызванной COVID-19; образовательные учреждения, школы и институты в поисках возможности продолжать обучение в условиях пандемии, осваивали новые для себя интернет-платформы[1].

[1] Рахманова Е. Н., Пономарева Е. В. Киберпреступность, цифровая преступность и безопасность: проблемы определения взаимосвязи // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 203.

Более того, в современном мире, подавляющее большинство жителей нашей планеты, в том числе и граждане нашей страны, используют компьютеры и иные средства телекоммуникационной связи для общения или развлечений.

Весь процесс компьютеризации, обеспечивающий автоматизацию информационных процессов и технологий в различных сферах человеческой деятельности, преследовал цель улучшения качества жизни людей за счет увеличения производительности и облегчения условий их труда, но несмотря на эти преимущества, одновременно с ними, появилась опасность в виде компьютерных преступлений или преступлений, совершаемых с использованием современных информационных технологий.

Российская Федерация не является исключением. Преступления, которые совершаются в компьютерной сфере не только актуальны, но некоторые из них, вызывают общественный резонанс. Так, в последние годы широкое распространение получили так называемые треш-стримы, которые представляют собой прямые трансляции в интернете, в ходе которых участники за вознаграждение выполняют различные задания, сознательно нарушая границы дозволенного и приемлемого в обществе поведения[1]. Причем задания могут заключаться в причинении физических страданий либо в выполнении действий, унижающих честь и достоинство как самого ведущего стрима, так и третьих лиц.

Так, например, двое подростков в Ленинградской области убили молотком 13-летнюю девочку, а расправу над ней транслировали в соцсети. Никакой личной неприязни у подозреваемого и его сообщницы к потерпевшей не было, процесс был заранее ими спланирован[2].

[1] Рахманова Е. Н., Берестовой А. Н., Цветков П. В. Треш-стрим — форма сетевой агрессии: уголовно-правовой анализ // Вестник Санкт-Петербургского университета МВД России. 2023. № 1 (97). С. 137—143.

[2] В Петербурге расследуют резонансное дело подростков, убивших 13-летнюю девочку на стриме // RGRU. Новости : сайт. URL: https://rg.ru/2023/05/04/ubijstvennyj-strim.html (дата обращения: 17.10.2023).

Неслучайно судья Верховного Суда Российской Федерации Геннадий Иванов в своем выступлении на заседании Клуба имени Замятина отметил, что киберпреступность стала одним из вызовов современности, а количество киберпреступлений неуклонно растет[1].

Его слова подтверждает А. Некрасов, начальник Главного организационного-аналитического управления Генеральной прокуратуры Российской Федерации. В своем интервью он обратил внимание на то, что в среднем раскрываемость таких преступлений не достигает и 25 % от всех совершенных преступлений, при этом правоприменителями отмечается их постоянный рост. Причем, наибольший рост зафиксирован в Санкт-Петербурге и Ленинградской области[2].

Опасность киберпреступлений обусловлена методами их совершения. Г.М. Рамон пишет в этой связи, что «киберпространство не имеет территориальных границ, но стандарты или технические, регулирующие системы не принадлежат к юридическому миру»[3].

Таким образом, лицо, совершающее преступление может находиться за тысячи километров от предполагаемой жертвы его деяния и с легкостью получает доступ к личным данным (что нарушает п. 1 ст. 23 Конституции Российской Федерации «каждый имеет право на неприкосновенность частной жизни»), финансовым ресурсам (п. 2 ст. 35 Конституции Российской Федерации «каждый вправе иметь имущество в собственности, владеть, пользовать и распоряжаться им») и конфиденциальной информации (п. 2 ст. 23 Конституции Российской Федерации «каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»).

---

[1] Эксперты обсудили актуальные проблемы киберпреступности // Адвокатская газета. 2023. 8 июня. URL: https://www.advgazeta.ru/novosti/eksperty-obsudili-aktualnye-problemy-kiberprestupnosti/ (дата обращения: 17.10.2023).

[2] Киберпреступность представляет угрозу нацбезопасности, заявили в Генпрокуратуре // Парламентская газета. 2021. 24 мая. URL: https://www.pnp.ru/social/kiberprestupnost-predstavlyaet-ugrozu-nacbezopasnosti-zayavili-v-geprokurature.html (дата обращения: 17.10.2023).

[3] Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 79.

Среди всех киберпреступлений особой популярностью пользуется фишинг. Резкий рост фишинговых атак затрагивает как частных лиц, так и организации, государственные учреждения и крупные предприятия. По данным Лаборатории Касперского, «каждый восьмой россиянин (12 %) подвергся компьютерным атакам в 2023 году. Каждый пятый (21 %) пожаловался на локальные угрозы, а почти каждый третий (29 %) — на звонки с подозрением на мошенничество. Всего за полгода в России было зафиксировано 6,2 млн атак на смартфоны и 23,6 млн попыток переходов на фишинговые сайты. При этом в половине случаев мошенники отправляли жертвам спам на электронную почту»[1].

Под фишингом, по нашему мнению, понимается совокупность действий, которые совершаются обманным путем, воздействуя на пользователей интернет-сетей с целью завладения их конфиденциальными данными, содержащими информацию о логинах, паролях и других данных, необходимых к доступу, например, к имуществу или правам на имущество граждан, организаций и т. д.

Фишинг реализуется путем массовых интернет-рассылок, причем источник может быть различен. В содержание писем входит информация, направленная на возбуждение у читателей желания действовать в соответствии с указаниями к данному сообщению. Следовательно, можно прийти к выводу, что мошенники, использующие фишинг – тонкие психологи, которые точно знают, на чем «сыграть», чтобы даже у взрослого человека случилось «помутнение рассудка», и он добровольно поддался на провокацию.

Также мошенники действуют исходя из анализа аудитории, находя доверчивых людей или тех, кто мало разбирается или является нечастым пользователем данной сферы и своими указаниями побуждают потерпевшего совершить все необходимые для киберпреступника действия.

[1] На старые траблы: какие схемы обмана использовали мошенники в 2023 году // Известия. 2023. 11 июня. URL: https://iz.ru/1525423/mariia-frolova/na-starye-trably-kakie-skhemy-obmana-ispolzovali-moshenniki-v-2023-godu (дата обращения: 17.10.2023).

Если мошенники преследуют цель завладения логином, паролем потерпевшего, то и активные действия, на которые выводят потерпевших преступники, подразумеваются с их использованием. В большинстве случаев ввод логина или пароля происходит на поддельном сайте, который на первый взгляд не отличить от оригинального. Также воздействие на потерпевшего возможно от имени лже-третьих лиц, которые заведомо для преступника являются близкими или знакомыми потерпевшего, либо же через имитацию/взлом аккаунта публичной личности, которой верит и доверяет потерпевший.

Помимо того, что киберпреступления представляют опасность для неопределенного количества людей, равным образом под угрозу ставится и безопасность государства.

Согласно Закону Российской Федерации от 21.07.1993 № 5485-1 (в ред. от 04.08.2023) «О государственной тайне» к государственной тайне относятся защищаемые государством сведения в областях военной, внешнеполитической, экономической, разведывательной, оперативно-розыскной и контрразведывательной деятельности, распространение которых может нанести ущерб безопасности России[1]. Очевидно, что использование Интернета и информационных процессов и технологий во многом облегчает возможность неправомерного завладения информацией и ее распространение.

В связи со специальной военной операцией участились случаи выдачи иностранному государству сведений, составляющих государственную тайну, которая в дальнейшем может быть использована против безопасности Российской Федерации. К числу таких случаев относятся действия жителя Самарской области, который инициировал переписку в интернет-мессенджере с представителем спецслужбы Украины, по заданию которого осуществлял фотофиксацию российской военной техники[2].

---

[1] О государственной тайне : Закон Российской Федерации от 21 июля 1993 г. № 5485-1 : текст с изм. и доп. на 4 авг. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс.

[2] ФСБ возбудила дело о госизмене за передачу Украине снимков военных эшелонов // Интерфакс : сетевое издание. URL: https://www.interfax.ru/russia/915583 (дата обращения: 17.10.2023).

Под «киберпреступлениями» обычно понимается девиантное поведение, осуществляемое в виртуальном пространстве с помощью компьютерных устройств.

В российском уголовном законодательстве в главе 28 УК РФ установлена ответственность за преступления в сфере компьютерной информации. Кроме того, ряд статей дополнены самостоятельным признаком — совершение преступления «в информационно-телекоммуникационных сетях (включая сеть «Интернет»)» или с их использованием.

В этой связи В.А. Номоконов и Т.Л. Тропина справедливо указывают, что «киберпреступление» понимается шире, чем компьютерная преступность, но полностью содержит в себе то, что определяется под преступлениями в информационном пространстве»[1]. Что же касается «телекоммуникационных сетей (включая сеть «Интернет»)», то в настоящее время специальные нормативные акты, регулирующие общественные отношения, возникающие в связи с совершением в них преступлений, пока отсутствуют[2].

В настоящее время делаются серьезные шаги по устранению данного противоречия. В 2019 году под эгидой ООН и по инициативе России был создан специальный комитет для разработки конвенции по борьбе с использованием информационно-коммуникационных технологий (ИКТ) в преступных целях. В 2021 году данный проект, подготовленный российской делегацией, был внесен на рассмотрение в ООН и в ближайшее время ожидается его принятие[3]. Особый интерес представляет расширение круга составов преступлений по

[1] Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2012. №1 (24). С. 47.

[2] Каримов А. М. Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. 2023. Т. 14, № 1 (51). С. 78.

[3] Россия внесла в специальный комитет ООН проект конвенции о борьбе с киберпреступностью // Парламентская газета. 2021. 27 июля. URL: https://www.pnp.ru/in-world/rossiya-vnesla-v-specialnyy-komitet-oon-proekt-konvencii-o-borbe-s-kiberprestupnostyu.html (дата обращения: 17.10.2023).

сравнению с теми, что указаны в Будапештской конвенции (Конвенция о компьютерных преступлениях принята в г. Будапеште 23.11.2001[1]. Россия не является участником Конвенции), с десяти до двадцати трех. В их число вошли несанкционированный доступ к личным данным, вовлечение детей в противоправную деятельность, терроризм и экстремизм и др.

Таким образом, международное сообщество признало необходимость расширения понятия «киберпреступления», что позволит, по нашему мнению, правильно квалифицировать такие деяния, поскольку следует признать, что преступления «в сфере компьютерной информации» (глава 28 УК РФ) и преступления, совершенные при помощи «телекоммуникационных сетей (включая сеть “Интернет”)» являются различными, следовательно, представляется невозможным отнесение последних к главе 28 УК РФ.

Подводя итоги, мы приходим к выводу, что совершаемые в виртуальной сети или с помощью телекоммуникационных средств преступления, не охваченные главой 28 УК РФ, например, ст. 136,137, 275, 276 УК РФ, и посягающие на интересы граждан, предприятий, организаций и государства, должны быть дополнены квалифицирующим признаком «с использованием информационно-телекоммуникационных сетей, включая сеть “Интернет”».

УДК 343

А. М. ЧИХРАДЗЕ

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК СРЕДСТВА СОВЕРШЕНИЯ ПРОВОКАЦИОННЫХ ДЕЙСТВИЙ ПОТЕРПЕВШИМ В КОНТЕКСТЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА УБИЙСТВО, СОВЕРШЕННОЕ В СОСТОЯНИИ АФФЕКТА

Электронные и информационно-телекоммуникационные сети как средства передачи информации и данных сегодня являются неотъемлемым элементом, способствующим процессам интенсивной цифровизации современного общества. Они уже давно проникли практически во все сферы общественной

[1] URL: https://rm.coe.int/1680081580 (дата обращения: 17.10.2023).

жизни – от образования и медицины до предоставления государственных и муниципальных услуг. Активно поощряется и стимулируется указанный процесс со стороны государства.

Так, например, Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов[1].

Однако подобный процесс интенсивной и повсеместной цифровизации общества, активного пользования информационными и электронно-телекоммуникационными сетями характеризуется не только положительными факторами, такими как доступ к большому объему информации, возможность для образования, коммерции и социализации на новом уровне, но и рядом негативных, в частности появление новых угроз безопасности, ростом преступности, появлению новых преступлений, модификация способов совершения тех, которые уже предусмотрены УК РФ. На это обращают внимание и в российской уголовно-правовой науке.

Как отмечает А.Н. Попов, преступления в сфере использования электронных и информационно-телекоммуникационных сетей включают в себя преступления, предусмотренные главой 28 УК РФ и другие преступления, которые связаны с использованием компьютеров и подобного рода технологий[2].

Ю.В. Гаврилин, анализируя статистические данные о совершаемых в России киберпреступлениях, обращает внимание на то, что в них не отображаются данные о преступлениях, которые содержатся в иных разделах и главах,

[1] О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы : Указ Президента Российской Федерации от 9 мая 2017 г. № 203. Доступ через информ.-правовой портал «Гарант».

[2] Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб., 2018. С. 8.

нежели глава 28 УК РФ, хотя они совершаются дистанционно, с использованием сети «Интернет», социальных сетей, мессенджеров и иных подобных сервисов[1].

Следует выделить целый ряд составов преступлений, которые сегодня возможно совершить посредством использования электронных и информационно-коммуникационных сетей. Необходимо отметить, что указанные составы находятся в различных главах УК РФ, при этом, как правило, признак использования соответствующего рода сетей указан как обстоятельство, которое отягчает меру уголовной ответственности, реже – в законодательной конструкции основного состава. В иных случаях он не указан как обязательный признак, описанный в диспозиции. Тем не менее, уголовно-правовой анализ элементов этих составов преступлений позволяет прийти к выводу о том, что их совершение возможно с помощью электронных и информационно-телекоммуникационных сетей. Приведем некоторые примеры.

К первой группе можно отнести: ст. 110 УК РФ «Доведение до самоубийства», ст. 110.1 УК РФ «Склонение к совершению самоубийства или содействие совершению самоубийства», ст. 110.2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства», ст. 128.1 УК РФ «Клевета», ст. 133 УК РФ «Понуждение к действиям сексуального характера», ст. 137 УК РФ «Нарушение неприкосновенности частной жизни» и др.

Ко второй группе: ст. 119 УК РФ «Угроза убийством или причинением тяжкого вреда здоровью», ст. 120 УК РФ «Принуждение к изъятию органов и тканей человека для трансплантации», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 147 УК РФ «Нарушение изобретательских и патентных прав», ст. 155 УК РФ «Разглашение тайны усыновления (удочерения)», различные виды мошенничества и др.

[1] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий. Учебное пособие. В 2 ч. Т. 1 / [Ю. В. Гаврилин, А. В. Аносов, В. В. Баранов и др.]. М., 2019. С. 6.

При подобном векторе развития отечественного уголовного законодательства, поддерживая мнение Ю.В. Гаврилина о необходимости квалифицировать деяния субъектов, которые при совершении преступлений используют компьютерные технологии, в соответствии с теми нормами уголовного права, ответственность за которые уже закреплена в «некомпьютерных» статьях УК РФ[1] представляется актуальным обратить внимание на положения ст. 107 УК РФ «Убийство, совершенное в состоянии аффекта» и ее практическое использование.

Исследование научных источников позволяет утверждать, что, хотя авторы в своих научных работах указывают на различные преступления, которые сегодня могут быть совершены с помощью электронных и информационно-коммуникационных сетей, указанный состав преступления в них не упоминался.

Можно предположить, что это связано с тем фактором, что в случае ст. 107 УК РФ субъект никак не может совершить уголовно-наказуемые действия с помощью электронных и информационно-телекоммуникационных сетей. В контексте взаимосвязи данного состава и компьютерных технологий необходимо рассматривать провоцирующие действия потерпевшего, а также способы и средства их совершения.

Такая целесообразность актуальна еще и в связи с тем фактом, что в науке уголовного права активно исследуется и обращается внимание в основном на противоправное поведение субъекта преступления, а также способы совершения им уголовно-наказуемых деяний с помощью компьютерных технологий, в то время как действия потерпевшего в указанном направлении остаются, как правило, за рамками научных исследований, хотя в ряде случаев именно они занимают в механизме совершения преступления не последнее место.

Значительную часть объективной стороны этого состава преступления составляют такие действия потерпевшего, которые находятся в причинно-

[1] Там же. С. 10.

следственной связи с возникновением состояния аффекта или сильного душевного волнения у субъекта совершения преступления — это совершенные в отношении субъекта: насилие, издевательство, тяжкое оскорбление, иные противоправные или аморальные действия, а также длительная психотравмирующая ситуация, возникшая в связи с систематическим противоправным или аморальным поведением потерпевшего.

Следует отметить, что точное определение этих терминов сегодня не содержит ни уголовное законодательство, ни правоприменительная практика, хотя в уголовно-правовой науке неоднократно обращалось внимание на целесообразность их правовой регламентации. Следовательно, актуальным и необходимым является современное теоретико-практическое исследование содержания указанных в диспозиции признаков объективной стороны ст. 107 УК РФ с позиции перехода от оценочных категорий к закреплению в нормах уголовного права.

Большой юридический словарь достаточно широко толкует значение термина «насилие», понимая под ним как физическое, так и психическое воздействие одного человека на другого, посягающее на право граждан на личную неприкосновенность, которое гарантирует Конституция Российской Федерации[1].

Ученые также поддерживают такое толкование насилия в смысле ст. 107 УК РФ, поскольку законодатель непосредственно в диспозиции уголовно-правовой нормы не указал его вид, степень тяжести либо границы совершения[2].

Главное условие, предъявляемое к правовой оценке насилия — оно должно стать причиной-катализатором, которая способствует возникновению состояния аффекта (сильного душевного волнения) у виновного лица.

---

[1] Большой юридический словарь / М. Я. Сухарев, В.Е. Крутских, А.Я. Сухарева // Академик : сайт. URL: https://dic.academic.ru/dic.nsf/lower/16353 (дата обращения: 01.11.2023).

[2] Чугунов А. А. Ответственность за убийство, совершенное в состоянии аффекта : автореф. дис. … канд. юрид. наук. М., 2008. С. 16.

Издевательство как альтернативное действие, вызывающее особое эмоциональное состояние субъекта совершения преступления, предусмотренного ст. 107 УК РФ, также характеризуется большой вариативностью своего проявления, что отражает и его определение, данное в словаре С.И. Ожегова: «…под издевательством следует понимать особо циничное глумление, длительные насмешки над личностью, оскорбление действием или словом»[1].

Оскорбление, согласно толковому словарю С.И. Ожегова, — умышленное грубое унижение чести и достоинства[2]. Подобная формулировка также позволяет утверждать о множественности форм объективной реализации тяжкого оскорбления по ст. 107 УК РФ. Как справедливо отмечает Т.В. Сысоева, при оценке тяжести оскорбления необходимо руководствоваться не только общепринятыми нормами морали, но и индивидуальными особенностями личности виновного (болезнь, увечье, физические недостатки, беременность, психологические травмы, расстройства психики и т. п.)[3].

Необходимо отметить, что ряд вышеуказанных действий со стороны потерпевшего содержательно корреспондирует с таким современным интернет-явлением как кибербуллинг. Установление соответствующих связей этого негативного социального явления с вышеперечисленными объективными и субъективными признаками состава преступления, предусмотренного ст. 107 УК РФ, по нашему мнению, позволит уже сейчас квалифицировать использование электронных и информационно-телекоммуникационных сетей в механизме совершения убийств в состоянии аффекта. Уголовно-правовая характеристика указанных действий, которые в таком ракурсе необходимо исследовать с позиции уголовного права и определить степень их со-

[1] Ожегов С. И. Толковый словарь русского языка : Около 100 000 слов, терминов и фразеологических выражений / под ред. проф. Л. И. Скворцова. 27-е изд., испр. М., 2018. С. 857.

[2] Там же. С. 1007.

[3] Сысоева Т. В. Убийство, совершенное в состоянии аффекта: уголовно-правовые и виктимологические аспекты : дис. … канд. юрид. наук. Екатеринбург, 2000. С. 83.

отношения с провоцирующими действиями потерпевшего лица, составляющие неотъемлемое условие механизма возникновения и реализации объективной стороны преступления, предусмотренного ст. 107 УК РФ.

Термин «кибербуллинг» образован из двух составляющих: «кибер-» и «буллинг». Рассмотрим этимологию каждой из этих частей:

1. Кибер-: Происходит от древнегреческого слова «κυβερνάω» (kybernao), что означает «управлять» или «руководить». Этот корень стал популярным в контексте технологий и информатики, прежде всего, благодаря термину «кибернетика» — науке о процессах управления и передачи информации в машинах и живых организмах. С течением времени приставка «кибер-» стала использоваться для обозначения всего, что связано с компьютерами, интернетом и виртуальной реальностью, в том числе и в контексте уголовной ответственности.

2. Буллинг: Это англицизм, происходящий от английского слова «bullying», что означает «травля» или «издевательство». Таким образом, «кибербулинг» можно перевести как «электронное» или «виртуальное» издевательство и травля. Этот термин используется для описания аморального, вызывающего поведения или травли в интернете либо в электронных средствах общения.

В зарубежных странах государственная реакция на «кибербуллинг» не носит единообразного характера, хотя его общественная опасность давно признана рядом государств, в которых всеобщая цифровизация сформировалась в 60—80-х годах прошлого столетия. В США, например, на уровне штатов «кибербуллинг» подлежит уголовному преследованию как форма угрозы, травли, издевательства. В Великобритании существует ряд законодательных актов, которые применимы к «кибербуллингу», такие как «Закон о защите от преследования» (1997 г.), «Закон о наказании и предупреждении преступлений» (2006 г.). Указанные нормативные акты предусматривают наказание за угрозы, оскорбления и иное агрессивное поведение интернет-пользователей. Австралийский закон «О безопасности в интернете» (2021 г.)

предоставляет возможность дать юридическую оценку случаям «кибербуллинга» в отношении детей. В 2015 году Новая Зеландия приняла закон «О вреде в цифровом общении», который направлен на предотвращение вреда, причиняемого в процессе цифрового общения, а также предусматривающий ряд средств его возмещения. Филлипинский закон «О предотвращении и борьбе с киберпреступностью» (2012 г.) включает в себя статьи, предусматривающие пределы ответственности за «кибербуллинг».

На сегодняшний день отечественное законодательство не определяет содержание термина «кибербуллинг», а Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации» регулирует отношения, которые возникают непосредственно в условиях пользования Интернетом в целом[1].

В свою очередь анализ научных источников по психологии, социологии, педагогике позволяет сформулировать определение термина «кибербуллинг» и выявить его существенные признаки, имеющие существенное значение для понимания его природы, а также возможности дать юридическую оценку этого явления с позиции уголовного права.

«Кибербуллинг» — это умышленные, систематические, оскорбляющие, унижающие честь и достоинство личности действия, осуществляемые другим лицом с помощью электронных и информационно-телекоммуникационных сетей. Формами объективного проявления «кибербуллинга» является широкий спектр альтернативных действий. Например: прямое оскорбление, отправка угроз, публикация компрометирующей или уничижительной информации, а также другие действия, направленные на реализацию психологического насилия над лицом.

Базовыми признаками «кибербуллинга» как уголовно-правового явления современного типа, по нашему мнению, следует выделить из указанного выше перечня:

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ : текст с изм. и доп. на 2 нояб. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

1. Активность действий – формы реализации «кибербуллинга» предполагают активное, вызывающее аморальное либо противозаконное поведение лица;

2. Умышленность, то есть лицо осознает аморальность характера своих действий. Уголовно-правовая оценка осознания противозаконности действий, которые составляют «кибербуллинг» необходима при квалификации в каждом конкретном случае;

3. Систематичность – повторяющиеся или носящие регулярный характер аморальные либо противоправные действия в цифровой среде, в отношении одного лица или группы лиц (систематические оскорбления в социальных сетях, угрозы через мессенджеры или электронную почту). Один из основных факторов, отличающих «кибербуллинг» от единичных случаев цифровой агрессии, — это его систематичный характер, который и способствует формированию и последующему существованию психотравмирующей ситуации.

4. Виртуальная дистанционность – аморальные либо противоправные деяния совершаются в цифровом пространстве электронных или информационно-телекоммуникационных сетей, а не в физическом мире (через социальные сети, мессенджеры, электронную почту, игровые платформы и другие онлайн-сервисы). Виртуальная дистанционность как признак «кибербуллинга» создает уникальные для него условия: постоянство, поскольку цифровая информация может сохраняться и распространяться неограниченное время, причиняя ущерб психике другого лица; доступность результатов «кибербуллинга» для ознакомления и использования в дальнейшем неограниченным кругом лиц. В контексте уголовно-правовой характеристики виртуальной дистанционности следует исключать такую форму проявления «кибербуллинга» как анонимность, поскольку она носит альтернативный характер, а при квалификации преступления, предусмотренного ст. 107 УК РФ, анонимность «кибербуллинга» должна быть и вовсе исключена.

Практически все вышеуказанные признаки (активность действий, их умышленность, систематичность), присущие «кибербуллингу» и имеющие, по нашему мнению, первоочередное значение для квалификации, полностью охватываются теми провоцирующими действиями потерпевшего, которые описаны в диспозиции ст. 107 УК РФ с тем условием, что возможно причинение именно психологического насилия в отношении субъекта преступления, который объясним таким признаком, как «виртуальная дистанционность». Таким образом, с содержательной стороны «кибербуллинг» в полной мере соотносится с объективной характеристикой противоправных либо аморальных действий, вызывающих создание психотравмирующей ситуации, описанных в диспозиции ст. 107 УК РФ «Убийство, совершенное в состоянии аффекта».

С учетом вышеизложенного можно констатировать тот факт, что сегодня, на современном этапе цифровизации общества, уже существует новая форма реализации аморального либо противоправного поведения потерпевшего от преступления, предусмотренного ст. 107 УК РФ «Убийство, совершенное в состоянии аффекта»: он может совершать провоцирующие действия не только при личном взаимодействии с субъектом преступления, но и посредством использования электронных либо информационно-телекоммуникационных сетей, а также в комбинированной форме — когда от аморального или противоправного поведения в виртуальном дистанционном формате возможен переход к прямому личному контакту.

В контексте взаимосвязи данного состава и компьютерных технологий необходимо рассматривать провоцирующие действия потерпевшего, а также способы и средства их совершения. Уголовно-правовая характеристика «кибербуллинга» как обязательная составляющая поведения потерпевшего, а также особенности механизма совершения преступления, предусмотренного ст. 107 УК РФ, о которых говорилось выше, определяют актуальность исследования аморального или противоправного поведения потерпевшего как существенного фактора в механизме совершения преступления субъектом.

УДК 343

Ю. А. ШУТОВА

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА УГРОЗУ УБИЙСТВОМ ИЛИ ПРИЧИНЕНИЕМ ТЯЖКОГО ВРЕДА ЗДОРОВЬЮ, СОВЕРШЕННУЮ В СЕТИ «ИНТЕРНЕТ»

Уголовно-правовые нормы охраняют права и свободы личности. Отношение к человеку, его базовым ценностям определяет гуманность Уголовного закона. В главе 16 УК РФ содержится норма, выполняющая функцию двойной превенции — ст. 119 УК РФ (угроза убийством или причинением тяжкого вреда здоровью).

Во-первых, указанная норма защищает личность от психического насилия, а во-вторых — предупреждает совершение тяжких и особо тяжких насильственных преступлений против личности. От оценки эффективности функционирования уголовно-правовой нормы зависит степень защищенности прав личности. В контексте данной статьи будет рассмотрена результативность применения ст. 119 УК РФ для защиты личности от психического насилия, совершенной с использованием средств массовой информации, информационно-телекоммуникационных сетей, в том числе сети «Интернет»

Проблемы эффективности применения уголовного права давно уже занимают представителей юридической науки[1]. Этот интерес был вызван изменениями в структуре и динамике преступности в сторону неуклонного роста. А.М. Яковлев писал: «Для социологии права важна прежде всего «реальность» права, т. е. интересна не столько норма «в законе», сколько ее реальное бытие в жизни»[2].

Важным этапом в развитии учения об эффективности правоприменительной деятельности в области уголовного права и процесса стал выход

[1] Карпец И. И. Наказание. Социальные, правовые и криминологические проблемы. М., 1973. 287 с. ; Стручков Н. А. Уголовная ответственность и ее реализация в борьбе с преступностью. Саратов, 1978. 288 с. ; Шаргородский М. Д. Наказание, его цели и эффективность. Л., 1973. 160 с.

[2] Яковлев А. М. Преступность и социальная психология. Юридическая литература. М., 1971. С. 214—234.

сборника научных статей под руководством Н.Ф. Кузнецовой и И.Б. Михайловской[1].

Среди современных ученых проблему социально-криминологической обусловленности уголовно-правового запрета рассматривает Ю.Е. Пудовочкин[2]. Н.А. Лопашенко полагает, что «для оценки эффективности уголовного закона следует использовать ряд критериев, в числу которых относятся: криминологическая обусловленность, качественная сформулированность нормы, способность применения нормы»[3].

Из представленных положений уясняется мысль о том, что изучение механизма социального действия уголовно-правовой нормы помогает найти ответ два ключевых вопроса: «Нужна ли обществу норма, охраняющая определенную сферу общественных отношений?»; «Если такая норма нужна, то в каком виде она должна быть представлена в Уголовном Законе?».

При анализе эффективности уголовно-правовой нормы, В.М. Коган одним из уровней предлагает выделять реализацию уголовно-правовой нормы[4]. Соглашаясь с позицией автора, представляется целесообразным рассмотреть данный уровень применительно к норме, предусматривающей уголовную ответственность за угрозу убийством или причинением тяжкого вреда здоровью.

Анализа эффективности уголовно-правовой нормы выражается в адекватной реализации уголовно-правового запрета правоприменительными органами. В основу данной реализации должен быть положен принцип идейности

---

[1] Эффективность применения уголовного закона: сборник статей / отв. ред. Н. Ф. Кузнецова, И. Б. Михайловская ; [предисл. В. Н. Кудрявцева]. М., 1973. 208 с.

[2] Пудовочкин Ю. Е. Понятие уголовно-правового запрета и проблемы его социально-криминологической обусловленности // Современные проблемы уголовной политики : материалы III Международной научно-практической конференции (г. Краснодар, 28 сентября 2012 года) / под ред. А. Н. Ильяшенко. Краснодар, 2012. Т. 1. С. 152.

[3] Лопашенко Н. А. Эффективное уголовное законодательство: утопия, иллюзия или нереализованные возможности? / Н. А. Лопашенко ; Санкт-Петербургский криминологический клуб URL: https://sartraccc./i.php?filename=Conference%2Foverview_krim_zak.htm &oper=read_file (дата обращения: 25.10.2023).

[4] Коган В. М. Социальный механизм уголовно-правового воздействия / отв. ред. В. Н. Кудрявцев. М., 1983. С. 9—10.

уголовно-правового воздействия. Совпадение морального стандарта поведения с уголовно-правовой нормой усиливает уголовно-правовое воздействие и повышает его эффективность.

Статистические данные Главного информационно-аналитического центра МВД России о динамике выявления и раскрытия преступления, предусмотренного ст. 119 УК РФ за период с 2012 по 2022 год, а также преступлений главы 16 УК РФ в целом[1], свидетельствуют о том, что за последние десять лет намечена тенденция незначительного спада преступности против личности. Указанное обуславливает пропорциональное снижение выявленных и раскрытых преступлений, предусмотренных ст. 119 УК РФ.

Причиной данного спада является трансформация общественных отношений в виртуальную среду, а также переход физического насилия в реальной жизни в психическое, выражаемое посредством средств массовой информации, информационно-телекоммуникационных сетей, в том числе сети «Интернет».

На данный факт указывает появление таких форм психического насилия, выражаемых в цифровом пространстве, как навязчивое преследование в сети «Интернет» (кибersталкинг), травля в сети «Интернет» (кибербуллинг). В этой связи актуальной проблемой выступает адаптация уголовно-правовой нормы, предусматривающей запрет за психическое насилие (ст. 119 УК РФ) к новым преступным угрозам, совершенной с использованием средств массовой информации, информационно-телекоммуникационных сетей, в том числе сети «Интернет»

В настоящее время правоприменители необоснованно сужают сферу реализации уголовно-правовой нормы, предусмотренной ст. 119 УК РФ, сводя ее к семейно-бытовой преступности. Изменилась форма донесения угрозы убийством или причинением тяжкого вреда здоровью, в том числе посредством использованием средств массовой информации, информационно-телекоммуни-

[1] Главный информационно-аналитический центр МВД России : офиц. сайт. URL: https://мвд.рф/folder/101762 (дата обращения: 16.04.2023).

кационных сетей, в том числе сети «Интернет». Однако правоприменители зачастую отказывают в возбуждении уголовного дела, если угроза убийством была выражена в сети «Интернет».

Так, например, из материалов проверки сообщения о преступлении Санкт-Петербургского Линейного Управления МВД России по транспорте следует, что «В ходе проведения проверки было установлено, что заявителю на принадлежащий ему мобильный телефон стали поступать звонки и сообщения с угрозами физической расправой от неизвестных лиц, предположительно коллекторов, по причине того, что его брат взял взаймы денежные средства и не возвращает их. В ходе проведения проверки и оперативно-розыскных мероприятий было установлено, что абонентские номера, с которых поступали звонки и сообщения зарегистрированы на территории Республики Дагестан. установить их принадлежность не представилось возможным».

Как показало проведенное нами исследование, принятие процессуального решения на основании п. 2 ч. 1 ст. 24 УПК РФ органы дознания мотивируют тем, что «В настоящее время звонки заявителю поступать перестали, никто никаких противоправных действий не совершал. Основания опасаться каких-либо противоправных действий в момент звонков и сообщений у заявителя отсутствовали, так как общение происходило опосредовано, через мобильное устройство». Полагаем данную аргументацию необоснованной и не отвечающей современной потребности граждан в уголовно-правовой защите от угроз убийством, поступающим в информационном пространстве.

Уголовно-правовая норма, предусматривающая уголовную ответственность за угрозу убийством по конструкции объективной стороны преступления, является преступлением с формальный составом. В этой связи оно считается оконченным с момента выражения угроз убийством или причинением тяжкого вреда здоровью при наличии оснований опасаться осуществления угроз. В этой связи факта выражения угрозы убийством в сети «Интернет», при наличии оснований опасаться ее осуществления, которыми может выступать продолжаемый характер угроз, достаточно для квалификации деяния по ч. 1 ст. 119 УК РФ.

Так же указание на опосредованный характер угроз, свидетельствующий об отсутствии оснований опасаться их осуществления является некорректным ввиду того, что ст. 119 УК РФ является самостоятельной нормой, предусматривающей уголовную ответственность за причинением вреда обеспеченной законом возможности сохранять имеющийся уровень психического и социального здоровья.

Идентифицировать рассматриваемую норму с институтом обнаружения умысла на совершение преступления является ошибочным. Таким образом, предлагается целесообразным пересмотреть устоявшийся правоприменительной практикой взгляд на ст. 119 УК РФ, и адаптировать ее под современные формы выражения угроз убийством или причинением тяжкого вреда здоровью.

Подводя итог следует отметить, что анализ эффективности уголовно-правовой нормы, предусматривающей уголовную ответственности за угрозу убийством или причинением тяжкого вреда здоровью, совершенную с использованием средств массовой информации, информационно-телекоммуникационных сетей, в том числе сети «Интернет», показывает, что необходимо в дальнейшем совершенствовать практическую реализацию нормы, в целях повышения защиты граждан от психического насилия, аккумулированного в информационной сфере.

УДК 343

С. А. ЮРКОВ

НЕКОТОРЫЕ АСПЕКТЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА НАРУШЕНИЕ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ

Уголовная ответственность за нарушение неприкосновенности частной жизни лица в России установлена относительно недавно, и, по началу, не обращала на себя должного внимания правоохранительных органов и самих граждан.

Однако в последние годы наблюдается увеличение количества регистрируемых преступлений по ст. 137 УК РФ, в связи с чем, высшая судебная инстанция дала ряд разъяснений по применению данной нормы в Постановлении Пленума Верховного Суда Российской Федерации № 46 от 25.12.18 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации).

Объектом преступления, предусмотренного ст. 137 УК РФ, является гарантированное ст. 23 Конституцией Российской Федерации право каждого на неприкосновенность частной жизни, личную и семейную тайну.

Предметом преступного посягательства выступают сведения о частной жизни лица, которые составляют его личную и семейную тайну. Такая формулировка диспозиции ч. 1 ст. 137 УК РФ сводит частную жизнь лица именно к личной и семейной тайне, хотя эти термины не совпадают, а скорее соотносятся между собой как целое и часть, где целое – это сведения о частной жизни, а часть – личная или семейная тайна. В судебной практике и научной литературе определения частной жизни в целом схожи.

Так, Конституционный Суд Российской Федерации неприкосновенность частной жизни определил как предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера[1].

В более позднем определении Конституционного Суда Российской Федерации отмечается, что право на неприкосновенность частной жизни, лич-

[1] Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 9 июня 2005 г. № 248-О. Доступ из справ.-правовой системы «КонсультантПлюс».

ную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера[1].

В. Новиков под неприкосновенностью частной жизни предлагает понимать состояние защищенности от незаконного вторжения посторонних лиц в сферу личной и семейной жизни[2].

А. В. Бриллиантов, к сведениям, составляющим личную или семейную тайну, предлагает относить данные, по мнению лица, которого эти сведения касаются, не подлежащие оглашению[3].

С.П. Гришаев под частной (личной) жизнью понимает все сферы жизни человека: семейную, бытовую, сферу общения, отношения к религии, внеслужебные занятия, увлечения, отдых и иные, которые сам человек не желает предавать гласности[4].

Личная тайна — это сведения, касающиеся только одного лица и сохраняемые им в режиме секретности от других лиц, за исключением сведений, характеризующих публичную, служебную деятельность этого человека[5].

А. С. Озерова полагает, что личная тайна — это сведения о различных сферах частной жизни лица, не носящие противоправный характер, не известные никому, либо известные узкому кругу лиц[6].

---

[1] Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 28 июня 2012 г. № 1253-О. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Новиков В. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности // Уголовное право. 2011. № 1. Доступ из справ.-правовой системы «Консультант-Плюс».

[3] Бриллиантов А. В. Комментарий к ст. 137 УК РФ // Комментарий к Уголовному кодексу Российской Федерации (постатейный). В 4 т. Т. 2. Особенная часть (разделы VII—VIII) / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.] ; отв. ред. В. М Лебедев. М., 2017. 371 с. Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Гришаев С. П. Право на неприкосновенность частной жизни // Гражданин и право. 2012. № 11. С. 11—29.

[5] Новиков В. Указ. соч.

[6] Озерова А. С. Личная и семейная тайна как предмет уголовно-правовой охраны: проблемы судебной практики // Уголовное право. 2022. № 3. С. 36.

Не могут относиться к личной тайне: общедоступная информация (например, сведения о местонахождении); персональные данные, доступ к которым не ограничен для третьих лиц; информация о противоправной деятельности лица и недостоверные сведения[1].

Мы солидарны с автором, что нельзя относить к личной тайне сведения о противоправной деятельности лица и недостоверные сведения. Хотя на практике мы встречали приговор, в котором предметом данного преступления указаны именно данные о судимости. Сведения о совершенном лицом преступлении нельзя признавать личной тайной, даже если судимость была снята или погашена ввиду того, что сам по себе факт судимости носит публичный характер. Приговор выносится публично от имени Российской Федерации и не может засекречиваться.

Сведения о местонахождении лица, о его передвижениях в пространстве, посещение каких-либо мест должны признаваться личной тайной, если лицо не желает их раскрывать.

Даже если человек перемещается в общественных местах, по улицам, но не желает раскрывать для других лиц цели такого перемещения, то такая информация должна признаваться личной тайной, даже в случаях, когда такие передвижения происходят в присутствии посторонних лиц (как наиболее часто и бывает), но не осознающих мотивы, в силу которых лицо это делает.

Персональные данные, доступ к которым не ограничен для третьих лиц, не могут признаваться личной тайной только в случае, если они являются доступными для неопределенно большого числа лиц. Например, лицо выкладывает на страницах социальных сетей свои паспортные данные. Если же человек передает свои персональные данные оператору (например, работодателю), то в этом случае их тайность сохраняется.

Семейная тайна — это групповая тайна, носителями которой являются члены одной семьи, представляющая информацию о взаимоотношениях между ними[2].

---

[1] Там же.

[2] Новиков В. Указ. соч.

В литературе справедливо отмечается, что личная и семейная тайна не одно и тоже. Носителем личной тайны является один человек, носителем семейной – группа лиц, каждый из которых осведомлен о том, что все их них хранят одну тайн. Представляется, что и семейная тайна должна обладать признаком конфиденциальности, т.е. каждый член семьи в силу тех или иных причин не желает ее разглашения. Это может быть информация, касающаяся одного из членов семьи (наличие какого-либо заболевания), некоторых или всех (например, отношение к религии).

Тем не менее на практике предметом данного преступления являются следующие сведения: тайна интимных отношений; о привлечении лица к уголовной ответственности; фамилия, имя и отчество, место рождения лица, место регистрации; видеозапись полового акта; телефонный разговор; информация о телефонных соединениях; видеозапись нахождения лиц в бане (без интимных отношений), которые пили там пиво и нецензурно выражались; семейные фото; информация из индивидуального лицевого счета застрахованного лица в Пенсионном фонде Российской Федерации; о передвижении лица в пространстве. В подавляющем большинстве случаев предмет являлись фотоснимки или видеозаписи интимного характера.

Способами нарушения неприкосновенности частной жизни, по УК РФ, являются: собирание и распространение сведений о частной жизни лица, либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Понятия «собирание» и «распространение» раскрываются в вышеупомянутом Постановлении Пленума Верховного Суда Российской Федерации. В соответствии с п. 3 данного Постановления, под собиранием сведений о частной жизни лица понимаются умышленные действия, состоящие в получении этих сведений любым способом, например, путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения. Под распространением данных сведений следует понимать их сообщение (разглашение) одному или

нескольким лицам в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»).

В практике встречаются следующие формы собирания: запись на телефон видео интимного характера; фотографирование спящего обнаженного человека; фотографирование изображений с чужого ноутбука; съемка на телефон в женском туалете торгового центра женщин, справляющих естественные нужды; видеозапись частной жизни супругов, проживающих на соседнем участке; видеозапись телефонного разговора другого лица в здании суда; запись разговоров сотрудников организации с помощью тайно установленного микрофона; получение информации о телефонных соединениях путем обмана у оператора связи; копирование не флеш-накопитель с чужого ноутбука интимного видео других лиц; вход на чужую электронную почту; незаконный доступ к чужой странице в социальной сети и последующее копирование, хранящихся там фотографий.

Распространение на практике может выражаться в следующих формах: демонстрация видео интимного характера третьим лицам; опубликование персональных данных в группе приложения мессенджера для сотовых устройств «WhatsApp»; размещение в сети «Интернет» фото; отправка другому лицу фото посредством MMS-сообщения; размещение фотоизображений в социальных сетях; отправка фото через мессенджеры другому лицу; размещение видеоролика на сайте видеохостинга «YouTube»; размещение фото в социальных сетях, полученных при их сканировании в фотосалоне, с требованием вернуть излишне уплаченную сдачу; передача тайны в устной форме. Публичным распространением на практике чаще всего является размещение соответствующих сведений в социальных сетях, либо мессенджерах. Полагаем, что общественная опасность публичного и непубличного (личного) распространения сведений является разной. Публичное распространение обладает более высокой степенью общественной опасности, по сравнению с непубличной, и может причинить более существенный вред потерпевшему.

Как сказано ранее, чаще всего на практике распространяются фотографии интимного характера. Тем не менее, возможны случаи, когда распространение сведений о частной и (или) семейной жизни лица может осуществляться в устной или письменной форме. Например, в форме разговора или переписки. Не секрет, что человек — субъект социальный, которому свойственно общаться, коммуницировать с другими людьми на различные темы: профессиональные, деловые, политические, личные, семейные, бытовые, в том числе о других людях.

В процессе такого общения могут рождаться различные слухи и сплетни. В связи с этим возникает вопрос: подлежит ли квалификации по данной статье распространение сведений о частной жизни лица, совершенное в устной форме, в разговоре между двумя или несколькими лицами?

Очевидно, что все люди обсуждают друг друга, своих родственников, соседей, коллег, знакомых и т. д. Делятся в разговорах сведениями, например о том, кто куда ездил, кто куда ходил, кто какую машину купил, у кого какая любовница или любовник и т.д. Если лицо желает сохранить подобные сведения в тайне, по нынешней редакции ст. 137 УК РФ, лица, сообщающие такие сведения другим лицам должны подлежать уголовной ответственности. Однако, представляется, что в таком случае необходимо привлечь девяносто процентов населения, что выглядит весьма проблематично и антисоциально по своей сути.

С субъективной стороны преступление совершается с прямым умыслом, мотивы и цели на квалификацию не влияют.

В практике в приговорах встречаются следующие цели — порочение потерпевшего; ознакомление с личной почтой другого лица; унижение чести и достоинства и др.

Мотивами могут быть: месть на почве личных неприязненных отношений; месть за сожительство с другим человеком; ревность; личная заинтересованность в виде ложно понятых интересов службы (запись угроз работников в адрес своего начальника, которые высказывались в его отсутствие); корысть.

В части 3 ст. 137 УК РФ закреплен самостоятельный состав преступления, предметом которого альтернативно является информация, указывающая на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, или информация, содержащая описание полученных им в связи с преступлением физических или нравственных страданий.

Несомненно, что необходимо ограничивать доступ к такой информации, в целях нормального развития потерпевшего несовершеннолетнего. Однако, отнести такую информацию к личной или семейной тайне невозможно ввиду того, что уголовное право и уголовный процесс — это публичные отрасли права и полностью ограничить доступ к такой информации невозможно.

Объективная сторона данного состава заключается в незаконном распространении такой информации, совершенное в обстановке публичного выступления, либо публично демонстрирующегося произведения, либо в средствах массовой информации, либо в информационно-телекоммуникационных сетях.

В качестве альтернативных последствий указаны причинение вреда здоровью несовершеннолетнего; психическое расстройство несовершеннолетнего; иные тяжкие последствия. Под последними, полагаем можно понимать самоубийство несовершеннолетнего, покушение на самоубийство, оставление образовательного учреждения, переезд в другой населенный пункт и т. д.

Полагаем, что не все из указанных последствий могут находиться в прямой причинной связи с распространением такой информации. Из теории уголовного права известно, что преступные последствия должны закономерно, необходимо вытекать из причины, а именно из совершенного деяния, напрямую. Простой пример, когда при убийстве смерть наступает от удара ножом в жизненно важный орган (сердце). В нашем случае, например, не совсем понятно, каким образом публичное оглашение такой информации может непосредственно причинить вред здоровью. По УК РФ вред здоровью может быть тяжким, средней тяжести и легким.

Как показано выше, в ч. 3 данной статьи предусмотрены альтернативные последствия: либо вред здоровью, либо психическое расстройство. Исходя из

содержания ч. 1 ст. 111 УК РФ, следует, что психическое расстройство — это тяжкий вред здоровью.

Соответственно получается, что для квалификации по ч. 3 ст. 137 УК РФ по признаку вреда здоровья, необходимо, чтобы это был только физический вред (тяжкий, средней тяжести или легкий). Мы не можем представить себе ситуацию, при которой такой вред быть непосредственным следствием публичного оглашения сведений.

Такой вред может быть причинен человеку другим человеком, или самостоятельно. Других вариантов мы не видим. Если такой вред причиняется другим человеком, то необходима квалификация по статьям УК РФ, предусматривающим ответственность за преступления против жизни и здоровья. Если же повреждения причиняются самим несовершеннолетним, то они находятся в причинной связи с его действиями, а не оглашением информации. Точно также необходимо решать вопрос, если наступили последствия в виде самоубийства несовершеннолетнего.

Кроме того, в законе не указана форма вины данного преступления. Соответственно оно может совершаться как с умыслом, так и с неосторожной формой вины. Если преступление совершается с умыслом, то получается, что виновный должен желать наступления либо физического вреда здоровью несовершеннолетнего, либо психического расстройства, либо иных тяжких последствий. Полагаем, что это невозможно, по указанным выше причинам.

Таким образом, нарушение неприкосновенности частной жизни во многих случаях осуществляется в сети «Интернет», либо в иной цифровой среде. Распространение сведений о частной жизни лица, совершаемое в словесной форме, а именно в ходе частных бесед, не должно влечь за собой уголовной ответственности, в связи с чем в ст. 137 УК РФ необходимо ввести соответствующее примечание. Состав преступления, предусмотренный ч. 3 ст. 137 УК РФ несовершенен, трудно доказуем и нуждается в совершенствовании.

II. ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»), В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ

УДК 343

И. И. БАЧО

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБНАЛИЧИВАНИЕМ И ТРАНЗИТИРОВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Обеспечение безопасности экономической системы, в настоящее время является одним из приоритетных направлений государственной политики России.

Для сохранения устойчивого развития финансовой системы, 30.05.2018, Президентом Российской Федерации утверждена «Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[1]. Одной из основных целей данной Концепции являются выявление и пресечение незаконных финансовых операций, осуществляемые в рамках незаконной банковской деятельности.

[1] Концепция развития национальной системы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : утв. Президентом Российской Федерации 30 мая 2018 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Современный мир находится в довольно сложном временном периоде. Кризис экономического развития, повышение дифференциации уровня жизни населения, внешнеполитические проблемы, нестабильная ситуация в мире — все это приводит к разрушению экономики страны, традиционных ценностей, и как следствие, появлению новых видов и способов совершения преступлений, особенно в сфере экономики. На сегодняшний день, одним из основных способов осуществления незаконной банковской деятельности является обналичивание и транзитирование денежных средств. Стоит отметить, что такие преступления имеют сложные схемы совершения, являются многоуровневыми, содержат в себе сопутствующие преступления (ст.ст. 173.1, 174.1, 187, 159 УК РФ) и анализ судебной и следственной практики показывает, что расследование подобных видов преступлений вызывает у правоохранительных органов трудности.

Особую тревогу вызывают преступления, связанные с незаконным обналичиванием и транзитированием денежных средств, совершаемые с использованием информационно-телекоммуникационных сетей. Наряду со «стандартными» способами «обнала», к которым можно отнести заключение договора займа, через фирмы-однодневки путем мнимой сделки, через комиссию по трудовым спорам, снятие наличных денежных средств под отчет либо через корпоративные карты организации и т.д., злоумышленники придумывают все новые, более изощренные способы и схемы обналичивания денежных средств, при этом начиная активно использовать современные технологии и совершать данное преступление в сети «Интернет».

Одним из распространенных способов незаконного обналичивания и транзитирования денежных средств, осуществляемый с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») является обналичивание через криптовалюту.

Стоит отметить, что на сегодняшний день криптовалюта не является средством платежа, но, при совершении преступления, она выступает именно

как «платежное средство» и является средством совершения противоправного деяния[1].

Данный способ привлекает все больше злоумышленников, так, согласно статистическим данным МВД России, за январь—сентябрь 2023 года количество совершенных преступлений данной категории увеличилось на 29,2 % по сравнению с предыдущим периодом[2].

Происходит это ввиду того, что у криптовалюты отсутствует законодательное регулирование и она совершенно лишена контроля со стороны государства. Также нет единого контролирующего центра, отслеживающего транзакции и ведущего их учет.

Регистрация на криптобиржах происходит зачастую анонимно, без указания идентифицирующих данных лица, и к тому же, в большинстве случаях, биржи находятся за пределами РФ, и их деятельность не попадает под российское законодательство. Использование криптовалюты при совершении преступлений, создает у правоохранительных органов трудности в расследовании и в доказывании виновности лиц, причастных к совершению подобных преступлений.

Однако, результат, на которой нацелены злоумышленники, при совершении обналичивания и транзитирования денежных средств — получить денежные средства в наличной форме. И способ с использованием криптовалюты не является исключением. В этом случае, даже при том, что некоторые криптобиржи обеспечивают полную анонимность при их использовании, при совершении транзакций и при переводе виртуальных монет в наличный эквивалент, преступники оставляют определенные следы, по которым их и можно установить.

---

[1] Зарубин А. В., Сапожков А. А. Научно-практический комментарий к Постановлению Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». СПб., 2020. С. 11.

[2] Статистические данные МВД России за январь—сентябрь 2023 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/42989123 (дата обращения: 19.11.2023).

Самой популярной криптовалютой, используемой в качестве платежного средства при совершении преступления выступает биткоин. Биткоин позволяет делать анонимные платежи, то есть при создании биткоин-кошелька на бирже, не нужно указывать персональные (паспортные) данные при регистрации, в отличие от открытия счета в банке. Однако, система биткоин сохраняет информацию обо всех произведенных транзакциях. Сведения о том, куда, когда и сколько переведено виртуальных монет, записываются в блокчейны.

Блокчейн в переводе с английского языка «blockchain» — «цепочка блоков». Именно эти блоки и хранят транзакции, которые происходят в сети. Иными словами, блокчейн — это база данных, содержащая информацию об адресе отправителя (IP-адрес), адрес получателя, сумме транзакции, времени отправки транзакции, количестве подтверждений и хеш-транзакции. Казалось бы, все просто, правоохранительным органам необходимо узнать номер кошелька, который принадлежит злоумышленнику, обычно это устанавливается при производстве обыска, с изъятием компьютерной, мобильной техники и иных электронных носителей.

И уже при производстве компьютерных экспертиз, эксперты могут дать полную информацию о том, какими биржами пользовались злоумышленники, установить их логины и пароли от ученых записей, и номер криптокошелька. По номеру кошелька в системе биткоин, на сайте «blockchain.info» можно узнать всю информацию о проведенных транзакциях, а также об IP-адресах получателя и отправителя, так как блокчейн находится в открытом доступе.

Зная IP-адреса, сотрудники силовых структур могут установить местонахождение устройства, с которого происходил выход в сеть, ну а дальше не трудно выявить и само лицо, виновное в совершении преступления. К тому же, некоторые преступники используют «холодные» криптокошельки (устройства на подобии флешки), которые также могут быть найдены и изъяты при обыске[1].

[1] Зиновьева Н. С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве // Вестник Восточно-Сибирского института МВД России. 2018. № 3 (86). С. 184—189.

Однако злоумышленники придумывают новые схемы и пути запутывания своих следов, в результате чего расследование подобных видов преступлений становится очень затруднительным.

Рассмотрим некоторые схемы, используемые для запутывания следов обналичивания и транзитирования денежных средств через криптовалюту[1]:

1. Подставные криптокошельки. Это самый простой метод избавления от «грязной» крипты. Данный прием обычно используется «новичками» в преступной деятельности, и актуален он лишь на первых этапах совершения преступления. Ведь все транзакции все равно отражаются в Blockchain, и переводы на подставные криптокошельки не спасают от отслеживания переводов. Однако, это неплохой способ для начала запутывания следов, и дробления крупных сумм на мелкие части, как подготовительный этап для дальнейшего отмывания. А если речь идет о крупных финансовых операциях, которые совершаются организованными преступными формирования, то в таком случае могут использоваться тысячи подставных кошельков. Стоит отметить, что по данным исследования «Big Ideas 2023» в мире на сегодняшний день насчитывается около 3,2 млрд криптокошельков.

2. Децентрализованные криптобиржи. Обычно это мелкие криптобиржи, которые предлагают анонимные транзитные услуги, но в таком случае велик риск, что сама криптобиржа может быть мошеннической, и злоумышленник сам потеряет все деньги, ведь цепочка транзакций в Blockchain обрывается, как только криптовалюта заводится на биржу. С одной стороны, это очень удобно для запутывания следов и дальнейшего обналичивания реальных денежных средств, а с другой злоумышленник уже не контролирует свои виртуальные деньги, а доверяет контроль над ними третьи лицам (бирже). Такие криптобиржи работают как крипто отмывочные, через некоторые биржи может ежегодно проходить миллионы долларов. Но, чем больше оборотов наращивает такая криптобиржа, и чем больше «грязной» криптовалюты через нее

[1] Как отмывают криптовалюту: самые популярные способы // Kaspersky : сайт. URL: https://www.kaspersky.ru/blog/crypto-laundering-and-ransomware/35298/ (дата обращения: 22.11.2023).

проходит, то со времен она привлечет к себе внимание правоохранительных органов, и в таком случае можно будет установить информацию о транзакциях, и о лицах, виновных в совершении преступлений.

3. Финансовые «сервисы-матрешки». Данные сервисы выступают как посредники между криптобиржами и злоумышленниками. Они позволяют торговать на криптобирже без создания аккаунта. То есть, злоумышленник обращается к «сервису-матрешке», с ним связывается агент, который будет курировать сделки с криптовалютой, а злоумышленник только дает указание куда, когда и сколько перевести криптовалюты. В данном случае очень сложно связать транзакции с конкретным лицом, и расследование уголовного дела очень затрудняется. Однако подобные сервисы имеют низкий рейтинг безопасности и не популярны в использовании у злоумышленников, потому что риск потерять все деньги очень высок.

4. Криптомиксеры. Представляют собой сервисы, которые позволяют скрыть информацию о транзакциях. Злоумышленник, оказывающий услуги по обналичиванию денежных средств, отправляет криптовалюту на сервис-миксер, где она, посредством транзитных операций соединяется со всеми монетами, которые имеются на сервисе, а дальше, спустя некоторое время, «смешанная» криптовалюта поступает на адрес конечного получателя. Связь между отправителем и получателем скрыта. В последующем получатель уже обналичивает криптовалюту и передает наличные денежные средства клиенту. Стоит отметить, что подобные сервисы находятся под пристальным вниманием правоохранительных органов, и в случае, если обнаруживаются обороты «грязной» (нелегальной) криптовалюты, то посредством проведения определенных следственных действий (обыск, выемка, допросы и т. д.) и оперативно-розыскных мероприятий, правоохранительные органы могут получить информацию о транзакциях и связать их с лицами, причастными к совершению преступлений, связанных с незаконным обналичиванием денежных средств.

5. Даркнет. Не так давно, на просторах «темного интернета» стали появляться сервисы, которые предоставляют услуги по обналичиванию денежных средств через криптовалюту. Для рекламы и поиска клиентов они используют

«черный рынок» (даркнет). Конфиденциальность и анонимность – обязательная часть сделки. Сервисы не уточняют каким образом в действительности они будут работать, но результат их услуги – выход в наличный кэш. Однако, даже учитывая, что даркнет использует скрытые сети, неиндексированные ресурсы, нестандартные протоколы и порты, и позиционируют себя как «неуловимые», правоохранительные органы научились выявлять, расследовать, а самое главное доказывать преступную деятельность, осуществляемую на «черном рынке». Яркий пример тому, прекращение в 2022 году деятельности самого известного даркнет-маркета «HYDRA» («Гидра»), и установление виновных лиц, причастных к организации данной преступной деятельности. Стоит отметить, что, предварительное расследование уголовного дела, в отношении российских граждан, преступная деятельность которых связана с «Гидрой», окончено, и в настоящее время уголовное дело находится на рассмотрении во Всеволожском городском суде Ленинградской области[1].

6. Криптообменники. Напомним, что основной результат незаконного обналичивания и транзитирования денежных средств (в том числе и через криптовалюту) — «выход в кэш». И первоочередная цель преступников, занимающихся незаконным обналом — как конвертировать криптовалюту в фиатные (наличные) деньги анонимно.

После введения законов, контролирующих оборот криптовалюты, все пользователи крупных бирж в обязательном порядке должны подтверждать свои личности, то есть предоставлять паспортные данные. Поэтому получить наличные денежные средства через криптобиржи анонимно невозможно. Для этого злоумышленники пользуются «черными обменниками».

Существует два варианта таких обменников. Первый — онлайн. Они представляют собой сайты, которые не требуют регистрации (в редких случаях необходимо указать адрес электронной почты). Схема работы с данными обменниками довольна проста: на сайте оставляется заявка на получение наличных денежных средств, после ее рассмотрения, дается номер кошелька,

[1] Исследование крупнейшего теневого рынка Hydra // SecurityLab.ru : сайт. URL: https://www.securitylab.ru/news/543799.php (дата обращения: 23.11.2023).

куда переводятся виртуальные монеты. Наличные денежные средства злоумышленник получает через бесконтактную доставку. Посылку оставляют в постамате, и код для получения отправляют злоумышленнику. Стоит отметить, что такие пользоваться такими онлайн-обменниками очень рискованно, существует большая вероятность, что посылка окажется пустой.

Второй вариант — офлайн-обменники. Как правило, они находятся в крупных городах России, таких как Москва и Санкт-Петербург, и представляют собой офисы (помещения), похожие на отделения банковских организаций, где и предоставляются услуги по конвертации криптовалюты.

Наличные деньги можно получить прямо после перевода витруальных монет. Однако, таких обменников очень мало, и они находятся под пристальным вниманием правоохранительных органов, оснащены камерами, и в случае возникновения подозрений, что лицо совершает незаконное обналичивание, установить личность довольно просто.

Поэтому преступники обычно пользуются услугами закрытых обменников. Сделки проходят как правило в квартирах, редко в офисах, сначала происходит перевод виртуальных монет и только потом готовят наличные денежные средства, и через некоторое время злоумышленник получает свой заказ. Это очень небезопасный способ перевода криптовалюты в наличные для злоумышленников, ведь зачастую, такими «закрытыми обменниками» являются сами правоохранительные органы, которые задерживают преступников непосредственно на месте с поличным, что намного упрощает дальнейшее расследование преступления[1].

Стоит отметить, что операции с криптовалютой вовсе не так анонимны, как их позиционируют. Осуществить транзитные операции, а уж тем более конвертировать виртуальные монеты в наличные денежные средства и при этом не оставить никаких следов просто невозможно. Несомненно, расследование подобных преступлений представляет сложность и требует большого количества времени.

[1] Анонимные денежные переводы и подводные камни криптовалютных операций // Хабр : сайт. URL: https://habr.com/ru/articles/587940/ (дата обращения: 25.11.2023).

В первую очередь это связано с плохой технической оснащенностью правоохранительных органов, ведь преступления, совершаемые с использованием информационно-телекоммуникационных сетей, совершаются в большей степени в Интернете, и для установления следообразования преступной деятельности, требуются новые и эффективные технические средства, позволяющие быстро обнаружить данные следы, а самое главное процессуально их оформить, чтобы в соответствии с законом, выявленные сведения смогли стать доказательствами по уголовному делу.

Необходимо выработать единую тактику и методику расследования подобных категорий преступлений, ведь незаконное обналичивание и транзитирование денежных средств, особенно совершаемые с использование информационно-телекоммуникационных сетей представляют угрозу экономической безопасности не только России, но и всего мира.

УДК 343

И. И. ГОЛОВКО

УЧАСТИЕ ПРОКУРОРА В СУДАХ ОБЩЕЙ ЮРИСДИКЦИИ ПО ДЕЛАМ О ДИФФАМАЦИИ

Каждый вправе свободно распространять информацию, не нарушая закон, а также права и свободы других лиц (ч.ч. 1, 4, 5 ст. 29, ч. 3 ст. 17 Конституции Российской Федерации).

Распространение сведений, порочащих честь, достоинство или деловую репутацию гражданина, именуют «диффамацией»[1]. Часть 1 ст. 23 Конституции Российской Федерации гарантирует право на защиту своей чести и доброго имени. Распространение порочащих, а также несоответствующих действительности сведений является основанием ограничения доступа к недосто-

[1] О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц : Постановление Пленума Верховного Суда Российской Федерации от 24 февраля 2005 г. № 3. П. 1. Доступ из справ.-правовой системы «КонсультантПлюс».

верной информации в информационно-телекоммуникационных сетях во внесудебном порядке либо рассмотрения судами спора о защите права по заявлению заинтересованного лица.

Внесудебный порядок ограничения доступа к недостоверной информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», которая порочит честь и достоинство физического лица или подрывает его репутацию и связана с его обвинением в совершении преступления, определен в ст. 15.1-2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации» и осуществляется по заявлению гражданина, которое подлежит направлению в прокуратуру субъекта Российской Федерации.

Прокурор субъекта Российской Федерации (его заместитель) проверяет доводы заявления, составляет заключение о наличии оснований принятия установленных законом мер или уведомляет заявителя об отсутствии таких оснований[1].

Заключение прокурора и материалы заявления гражданина незамедлительно направляются Генеральному прокурору Российской Федерации, который принимает решение либо об обращении в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (далее — Роскомнадзор), с требованием о принятии мер по удалению недостоверной информации и ограничению доступа к информационным ресурсам, распространяющим указанную информацию, в случае ее неудаления, либо не устанавливает оснований для этого. На основании требования прокурора Роскомнадзор незамедлительно принимает меры к удалению такой информации (ограничению доступа к ней).

[1] Об утверждении Инструкции о порядке рассмотрения уведомлений и заявлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет» : Приказ Генерального прокурора Российской Федерации от 26 августа 2019 г. № 596. Доступ из справ.-правовой системы «КонсультантПлюс».

Решение и действия прокурора по результатам проверки заявления гражданина могут быть оспорены в судебном порядке либо вышестоящему прокурору. В связи с этим одним из способов установления законности и обоснованности решения и действий прокурора является рассмотрение судом дела по соответствующему заявлению.

Так, по заявлению гражданина прокуратурой г. Москвы проведена проверка для установления оснований принятия мер по удалению недостоверной информации, ограничению доступа к информации, распространенной в сети «Интернет», как порочащей его честь, достоинство и деловую репутацию. В указанных заявителем материалах отсутствуют сведения о совершении гражданином конкретных преступлений, в связи с чем прокурор не установил необходимость блокировки информации. Решением суда первой инстанции, оставленным без изменения судом апелляционной инстанции, в удовлетворении административного иска о признании ответа на обращение незаконным отказано.

В кассационной жалобе гражданин настаивал, что судами не дана оценка заключению психолого-лингвистической экспертизы, согласно которому на указанных истцом сайтах сети «Интернет» отражена информация, умаляющая честь, достоинство и деловую репутацию конкретного лица в связи с обвинением его в совершении различных преступлений.

Кассационная инстанция согласилась с доводами жалобы; установила, что суды не проверили, имелись ли основания для ограничения доступа к информации; не установили, какая информация проверялась прокурором, соблюден ли порядок рассмотрения заявления. Решения судов первой и апелляционной инстанций отменены, дело направлено на новое рассмотрение в суд первой инстанции[1].

[1] Кассационное определение Второго кассационного суда общей юрисдикции от 18 октября 2023 г. № 88а-27261/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

По другому делу гражданин К. обратился в суд с административным иском о признании незаконным отказа прокуратуры Санкт-Петербурга в принятии мер в порядке ст. 15.1-2 Закона об информации, и об обязании рассмотреть его заявление и принять законное и обоснованное решение.

К. просил прокурора инициировать блокировку сайта, распространяющего недостоверную информацию, связанную с обвинением его в совершении преступлений; просил возбудить уголовное дело, признать его потерпевшим. Прокуратура в ходе проверки установила, что в сети «Интернет» размещена информация, которая не содержит сведения об обвинении лично заявителя в совершении конкретного преступления, отсутствуют основания для инициирования вопроса о принятии мер к удалению информации во внесудебном порядке. Заявление К. в части доводов направлено для рассмотрения прокурорам Московского и Центрального районов Санкт-Петербурга и в ГУ МВД. Суды первой и второй инстанции согласились с прокурором, оставив без удовлетворения доводы К.[1].

Прокурор, осуществляющий деятельность от имени государства, должен строго соблюдать принцип законности. Поэтому участие прокурора в рассмотрении споров о диффамации при оспаривании его решений и действий уместно рассматривать с точки зрения государственного правового механизма защиты прав граждан. Вопросы ответственности прокуратуры являются составляющей основы функциональной деятельности прокуратуры. Отмечают, что в этом случае прокуратура выступает как орган государства[2].

Установленный порядок принятия решения об ответственности органов прокуратуры рассматривается как гарантия законности в деятельности прокуратуры[3].

---

[1] Кассационное определение Третьего кассационного суда общей юрисдикции от 7 декабря 2022 г. № 88а-21292/2022 по делу № 2а-187/2022. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Гражданско-правовой статус органа прокуратуры // Актуальные проблемы прокурорской деятельности: теория прокурорской деятельности в системе наук : монография / Н. А. Васильчикова, И. И. Головко, А. В. Еремин [и др.]. М., 2020. С. 98—99.

[3] Новиков С. Г. К вопросу о гарантиях законности в деятельности прокуратуры СССР // Совершенствование прокурорского надзора в СССР : сборник статей. М., 1973. С. 57—65.

Вопросы участия в гражданском деле прокурора в качестве третьего лица не регулируются действующим законодательством. Участие прокурора в деле в указанном качестве возможно, например, если на досудебном этапе прокурор проводил проверку по заявлению гражданина о совершении другим лицом незаконных деяний, а в дальнейшем спор между указанными лицами разрешается судом.

Так, гражданин М. обратился с иском к П., которая как депутат Совета муниципального образования на бланке Совета направила главе администрации муниципального образования и прокурору заявление о проверке диплома о высшем образовании М. Суд первой инстанции пришел к выводу о том, что изложенные в заявлении ответчика сведения относятся непосредственно к истцу и содержат указание на его незаконное, по мнению П., поведение, текст заявления содержит утверждение о несоответствии истца занимаемой должности в связи с использованием им подложного диплома о высшем образовании.

Суд апелляционной инстанции критично оценил выводы суда первой инстанции, указав, что ответчик в рамках реализации своих полномочий депутата обратилась в компетентные органы за получением достоверной информации и для проведения проверки в отношении сведений об образовании П., ее действия не являются распространением сведений в отношении истца, не имеют оскорбительного характера, отсутствует их публичность и передача третьим лицам.

Кассационная инстанция отменила апелляционное определение и оставила в силе решение суда первой инстанции, с чем не согласилась судебная коллегия по гражданским делам Верховного Суда Российской Федерации, которая пришла к выводу, что определение суда кассационной инстанции принято с нарушением закона, при рассмотрении дела судом апелляционной инстанции не были установлены оскорбительный характер информации и ее передача третьим лицам. Если сведения при рассмотрении жалобы (обращения) не подтвердились, заявитель жалобы не может быть привлечен к гражданско-правовой ответственности на основании ст. 152 ГК РФ.

В противном случае это означало бы привлечение лица к гражданско-правовой ответственности за действия, совершенные им в пределах предоставленных ему конституционных прав, при исполнении им своего гражданского долга. Не является разглашением сведений, содержащихся в обращении, направление письменного обращения в компетентный орган. Судебная коллегия Верховного Суда Российской Федерации поддержала вывод суда апелляционной инстанции, основанный на верном применении норм материального права. Определение кассационного суда отменено, оставлено в силе апелляционное определение[1].

В приведенном судебном постановлении не указано процессуальное положение прокурора в деле, представляется, что прокурор явился третьим лицом без самостоятельных требований.

По одному гражданскому делу прокурор дал заключение по требованию учителя школы к матери ученицы о взыскании компенсации морального вреда[2]. Учитывая, что прокурор не наделен правом участвовать в делах рассматриваемой категории по ч. 3 ст. 45 ГПК РФ, полагаем, что прокурор вступил в указанное дело как третье лицо, не отстаивающее самостоятельных требований.

Как было отмечено ранее, законодательство не определяет особенности участия прокурора в деле в качестве третьего лица. В связи с этим оснований не согласиться с позицией суда о том, что прокурор как третье лицо вправе выступить с заключением, не имеется. Круг полномочий прокурора как лица, участвующего в деле, позволяет ему активно участвовать в исследовании доказательств и способствовать установлению всех обстоятельств по делу.

Участие прокурора в делах по спорам о диффамации в качестве представителя ответчика (органа прокуратуры, прокурора), а также в качестве треть-

[1] Определение Верховного Суда Российской Федерации от 6 июня 2023 г. № 18-КГ23-43-К4. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Решение Канского городского суда Красноярского края от 19 ноября 2020 г. по делу № 2-1146/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

его лица без самостоятельных требований осуществляется на основании общих положений нормативных правовых актов, регламентирующих процессуальную деятельность сторон спора, так как законодательство не регулирует такое направление деятельности прокурора. В целях надлежащей организации работы прокуроров издан приказ Генерального прокурора Российской Федерации от 15.03.2018 № 144 «Об организации работы по обеспечению представительства и защите интересов органов и организаций прокуратуры Российской Федерации в судах»[1], который обязывает принимать участие в рассмотрении судами дел рассматриваемой категории.

Как показывают сведения Судебного департамента при Верховном Суде Российской Федерации, прокурор инициировал рассмотрение судами дел изучаемой категории путем направления исковых заявлений к гражданам и юридическим лицам: за первое полугодие 2023 года рассмотрены 6 дел по заявлениям прокуроров, в 2022 году – 13 дел, в 2021 году – 7 дел, в 2020 году – 5 дел[2].

Представляется, что по указанным спорам прокурор реализовал полномочия по обращению в суд по правилам ч. 1 ст. 45 ГПК РФ в защиту прав, свобод и законных интересов граждан, которые не могут сами обратиться в суд по уважительным причинам (несовершеннолетние, лица с особенностями здоровья, недееспособные и пр.).

Судебная защита нарушенных прав и свобод граждан может быть сопряжена с привлечением лица, распространившего информацию, к ответственности за совершение административного правонарушения, предусмотренного ст. 5.61.1, ст. 5.61 КоАП РФ; либо за совершение преступления, предусмотренного ст. 128.1 УК РФ. Как верно отмечено в п. 6 постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 «О судебной практике

[1] Об организации работы по обеспечению представительства и защите интересов органов и организаций прокуратуры Российской Федерации в судах : Приказ Генерального прокурора Российской Федерации от 15 марта 2018 г. № 144 : текст с изм. и доп. на 15 сент. 2021 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Судебный департамент при Верховном Суде Российской Федерации : офиц. сайт. URL: https://www.cdep.ru/?id=79 (дата обращения: 20.11.2023).

по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» если действия лица, распространившего не соответствующие действительности порочащие сведения, содержат признаки преступления, предусмотренного ст. 128.1 УК РФ, потерпевший вправе обратиться в суд с заявлением о привлечении виновного к уголовной ответственности, а также предъявить иск о защите чести и достоинства или деловой репутации в порядке гражданского судопроизводства. Отказ в возбуждении уголовного дела по ст. 128.1 УК РФ, прекращение возбужденного уголовного дела, а также вынесение приговора не исключают возможности предъявления иска о защите чести и достоинства или деловой репутации в порядке гражданского судопроизводства.

Аналогичным видится порядок защиты прав гражданина с учетом выводов постановления по делу об административном правонарушении. Учитывается преюдициальный характер вступившего в законную силу постановления суда о привлечении к ответственности лица для решения вопроса о защите нарушенных прав гражданина, определенный ч. 4 ст. 61 ГПК РФ.

В числе способов защиты прав граждан по спорам о диффамации на основании соответственно п. 2 ст. 150, пп. 1, 4, 9, 8 ГК РФ следует указать:

— признание судом факта нарушения личного неимущественного права, опубликования решения суда о допущенном нарушении, а также пресечения или запрещения действий;

— опровержение сведений[1];

— удаление соответствующей информации, а также пресечение или запрещение дальнейшего распространения порочащих сведений путем изъятия и уничтожения экземпляров материальных носителей, содержащих указанные сведения, если без уничтожения таких экземпляров материальных носителей

[1] В пункте 4 Постановления Пленума Верховного Суда Российской Федерации от 24.02.2005 № 3 «О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц» указано, что законом не предусмотрено обязательное предварительное обращение с таким требованием к ответчику, в том числе и в случае, когда иск предъявлен к редакции средства массовой информации, в котором были распространены указанные выше сведения.

удаление соответствующей информации невозможно в случаях, когда порочащие сведения стали широко известны и в связи с этим опровержение невозможно довести до всеобщего сведения (п. 4 ст. 152 ГК РФ);

— возмещение убытков и компенсация морального вреда (п. 9 ст. 152 ГК РФ);

— признание распространенных сведений не соответствующими действительности, если установить лицо, распространившее сведения, невозможно (п. 8 ст. 152 ГК РФ).

Отметим, что признание распространенных сведений не соответствующими действительности и порочащими осуществляется по правилам особого производства, все иные способы защиты реализуются в исковом производстве.

Прокурор вступает в процесс и дает заключение по делам, указанным в ч. 3 ст. 45 ГПК РФ, ч. 7 ст. 39 КАС РФ, которые в настоящее время не предусматривают участие прокурора в рассмотрении судами споров о диффамации для дачи заключения.

Во всех рассмотренных ситуациях прокурор не является сторонним наблюдателем процесса рассмотрения дела судом, а активно участвует в судопроизводстве, принимает меры к достижению полноты установления обстоятельств по делу и характеристики правоотношений сторон, установлению подлежащего применению закона. Также участвующий в процессе на всех направлениях прокурор должен изучить постановление суда и прийти к выводу о наличии (отсутствии) оснований для его оспаривания.

Также отметим, что инициирование гражданином ограничения доступа к информации или судебного разбирательства в защиту своих прав может осуществляться с недобросовестными намерениями. В настоящее время злоупотребление правом не является правонарушением. Однако прокурору, участвующему в рассмотрении судами общей юрисдикции споров о диффамации, нельзя не обращать внимание на соответствующие обстоятельства, и не указывать на них в ходе выступления в суде. Этим обеспечивается воспитательная составляющая деятельности прокурора и предупреждение подобного поведения в будущем.

УДК 343

В. С. КАЛАШНИКОВ

РОЛЬ ПРОКУРОРА В ОПРЕДЕЛЕНИИ ТЕРРИТОРИАЛЬНОЙ ПОДСЛЕДСТВЕННОСТИ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В настоящее время редко можно встретить человека, не имеющего смартфона, банковской карты, аккаунта в социальных сетях, электронного почтового ящика или любого другого достижения человеческой цивилизации, упрощающей жизнь. Скорее, наоборот, люди активно ведут свои каналы и блоги, демонстрируя сообществу свою личную жизнь, обмениваются мгновенными сообщениями, приобретают товары несколькими движениями рук, отправляют денежные переводы. И все это при помощи одного устройства.

Вместе с тем научно-технический прогресс облегчает не только повседневную жизнь, но и совершение преступлений. Нетрудно заметить, как за последние 20 лет уголовное законодательство обогатилось новыми составами преступлений или обновленными формулировками прежних преступных деяний. В юридической литературе и в средствах массовой информации слово «кибер» все чаще является составной частью слов «атака», «преступления», «оружие», а информационная безопасность уверенно занимает свою нишу рядом с экономической, экологической и личной безопасностью. Уголовно-правовой охране подвергаются не только привычные виды имущества, но и так называемая «криптовалюта», оборот которой еще не урегулирован на законодательном уровне.

Вместе с тем уголовно-процессуальное законодательство обогатилось разве что электронными носителями информации и порядком их изъятия, да возможностью дистанционно проводить некоторые привычные следственные действия. С одной стороны, универсальность таких процессуальных действий как производство экспертизы или осмотр пока еще позволяют решать значительную часть криминалистических и процессуальных задач, стоящих перед

следователем, а вопросы изъятия и хранения цифровых финансовых активов не носят массового характера, чтобы требовать их законодательного регулирования. С другой стороны, приходится признать, что уголовно-процессуальное законодательство все же не успевает за техническим прогрессом.

Одним из краеугольных камней при расследовании преступлений, совершенных с использованием информационно-коммуникационных технологий, является определение места производства предварительного расследования. Вместо того, чтобы искать и изымать следы преступления, устанавливать лиц, совершивших преступления, органы предварительного расследования нередко занимаются пересылкой сообщения о преступлении из одного территориального подразделения в другое. Это характерно для любых видов преступлений. Однако, когда речь идет о применении информационно-коммуникационных технологий рассматриваемое явление приобретает особое значение. Так называемое информационное пространство стирает границы физического мира, предоставляя возможность преступнику контактировать с жертвой дистанционно, без визуализации друг друга, иногда наугад путем набора случайного телефонного номера или добавления в однодневный чат мессенджера.

Однако каким бы безграничным не было это информационное пространство, уголовно-процессуальное законодательство пытается нас привязать к конкретной точке земного шара, что порождает попытку установления конкретным дознавателем или следователем места совершения преступления и передачу сообщения о преступлении по территориальности.

В настоящее время с использованием информационно-коммуникационных технологий можно совершить преступление из практически любой главы Особенной части УК РФ, начиная от хищений и распространения детской порнографии, и заканчивая доведением до самоубийства при помощи онлайн-игр.

Учитывая, что единственная нормативная дефиниция «информационного пространства» определяет последнюю как сферу деятельности, связанную с формированием, созданием, преобразованием, передачей, использованием,

хранением информации, оказывающей воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[1], применять этот термин для принятия процессуальных решений нецелесообразно.

Когда речь идет о споре, какой территориальный орган должен заниматься расследованием конкретного преступления, указанное выше определение мало чем может помочь, поскольку сфера деятельности не может быть измерена в сантиметрах либо географических координатах. Правильнее было бы рассматривать информационное пространство как набор данных в виде электрических сигналов.

Такое пространство существует одновременно везде, где находятся устройства, подключенные к указанной сети, в то время как нас интересует конкретная точка на поверхности земного шара. И вот тут возникает резонный вопрос: а какая именно точка физического мира, спроецированная из информационного пространства, необходима для установления места производства предварительного расследования? И надо ли его устанавливать на этапе возбуждения уголовного дела?

Например, взлом электронного почтового ящика и копирование оттуда личной информации происходит, как правило, не на конкретных устройствах, принадлежащих пользователям. Почтовый ящик и его содержимое не находится на компьютере или ином устройстве потерпевшего, с которого он осуществляет доступ к своей почте. Равно как и злоумышленник на своем вычислительном устройстве лишь нажимает на клавиши, отправляя команды за пределы устройства и оказывая воздействие на объект, физическое расположение которого ему, скорее всего, не известно.

[1] Соглашение между Правительствами государств — членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности : заключено в г. Екатеринбурге 16 июня 2009 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Следуя за электрическими сигналами, можно добраться до конкретного сервера на материальном носителе. Но определять территориальную подследственность такого преступления по месту нахождения сервера равносильно отмененной практике расследования дистанционных хищений с банковского счета по месту нахождения кредитной организации, в которой этот счет открыт.

Действующая редакция ст. 152 УПК РФ не дает четкого ответ на рассматриваемый вопрос, поскольку отсылает к особенностям окончания каждого отдельного состава преступного деяния.

При этом п. 19 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» говорит, что при определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», и, соответственно, территориальной подсудности уголовного дела судам необходимо учитывать, что доступ к данной сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных). Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления[1].

Рассматриваемая рекомендация трудно применима к мошенническим хищениям, особенно дистанционным, где действия потерпевшего образуют часть объективной стороны состава преступления и выполняются в другом месте, нежели действия злоумышленника. Где будет считаться

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

оконченным склонение к самоубийству, если для привлечения к ответственности не обязательно, чтобы потерпевший даже предпринял неудачную попытку суицида?

Предотвратить необоснованное перенаправление сообщений о преступлениях способен прокурор. По отношению к органу дознания и дознавателю указанное лицо обладает полномочиями по отмене незаконных постановлений, к каковым может быть отнесено и постановление о передаче сообщения по подследственности. Однако уголовно-процессуальное законодательство, в отличие от уголовно-процессуальной науки, не использует термин «территориальная подследственность».

Следовательно, пересылку сообщения о преступлении от одного территориального органа другому нельзя назвать передачей по подследственности. Однако п. 31 Приложения № 1 к Приказу Генерального прокурора Российской Федерации, МВД РФ, МЧС РФ, Минюста Российской Федерации, ФСБ Российской Федерации, Минэкономразвития Российской Федерации и Федеральной службы Российской Федерации по контролю за оборотом наркотиков от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений»[1] прямо предусматривает такую возможность и даже определяет порядок производства подобного действия. В некоторых субъектах Российской Федерации на уровне руководителей правоохранительных органов изданы распоряжения о необходимости согласования с надзирающим прокурором решений о направлении сообщений о преступлении за пределы субъекта Российской Федерации. В пределах же субъекта Российской Федерации передача сообщений о преступлениях осуществляется без каких-либо ограничений, что может породить проблемы как с укрытием

[1] О едином учете преступлений : Приказ Генеральной прокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России и Федеральной службы Российской Федерации по контролю за оборотом наркотиков от 29 декабря 2005 г. № 39/1070/1021/253/780/353/399. Доступ из справ.-правовой системы «КонсультантПлюс».

преступлений, так и с несвоевременным принятием решения о возбуждении уголовного дела.

В отношении решений следователя о передаче сообщений о преступлении в иной территориальный орган расследования прокурор не обладает полномочиями по их отмене. Вносимое в адрес руководителя следственного органа требование об устранении нарушений закона не всегда способно достичь целей надзорной деятельности, поскольку к моменту его рассмотрения материалы по сообщению о преступлении уже не будут находиться в производстве данного органа предварительного следствия. Реагирование в адрес вышестоящего руководителя следственного органа через прокурора субъекта РФ создает не самую продуктивную конструкцию, к тому же работающую только в пределах субъекта Российской Федерации.

Анализ действующих приказов Генерального прокурора Российской Федерации в части организации надзора за деятельностью органов дознания и предварительного следствия показывает, что прокуроры должны пресекать факты необоснованной передачи органами дознания сообщений о преступлениях по территориальности, а при оценке действий следователей только разрешать споры о подследственности. Учитывая, что большая часть преступлений рассматриваемой категории относится к подследственности органов предварительного следствия, напрашивается вывод об отсутствии у прокурора реальной возможности повлиять на правильное определение места производства по уголовному делу на первоначальном этапе рассмотрения сообщения о преступлении.

Однако это не совсем так. Учитывая, что ведомственные приказы правоохранительных органов оперируют термином «территориальная подследственность» возникший спор придется решать прокурору. Однако прокурор может и сам инициировать передачу материалов проверки или уголовного дела в другой территориальный орган расследования, например, при оценке законности принятого решения об отказе в возбуждении уголовного дела

или о возбуждении уголовного дела соответственно. Вместе с тем целесообразной все же представляется конструкция, когда уголовное дело о преступлении рассматриваемой категории возбуждается уполномоченным в соответствии со ст. 151 УПК РФ лицом при наличии повода и основания, проводятся неотложные следственные действия по закреплению следов преступления, а уже потом, с учетом собранных данных решается вопрос о передаче уголовного дела по правилам, предусмотренным ст. 152 УПК РФ.

В этой связи возможны следующие варианты действий. Первое: на уровне субъектов Российской Федерации, а в идеале на федеральном, приказами руководителей правоохранительных органов запретить перенаправление сообщений о преступлениях, когда место его совершения не является очевидным. Например, звонок с телефонного номера, зарегистрированного в соседнем субъекте, не свидетельствует о том, что объективная сторона преступления выполнена по месту регистрации номера телефона. Равно как и перевод денежных средств на счет, зарегистрированный в конкретном банковском отделении. Второе: прокурорам районного звена давать правовую оценку постановлениям о направлении сообщений о преступлении по территориальности, в случае несогласия с ним либо отменять (в отношении органа дознания), либо требовать отмены у руководителя следственного органа. Третье: прокурорам районного звена также давать оценку материалам, поступившим из других территориальных правоохранительных органов и в случае несогласия с решением должностного лица о направлении сообщения по территориальности, во взаимодействии с соответствующим территориальным либо вышестоящим прокурором определять территориальную подследственность. Представляется, что подобный механизм позволит сократить сроки судопроизводства, затрачиваемые на необоснованную передачу сообщений о преступлении от одного территориального органа расследования к другому.

УДК 343

Г. Г. НЕПЕИН

ОСОБЕННОСТИ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ОБЫСКА (ВЫЕМКИ)

Совершенствование информационных технологий, проникающих во все сферы общественной жизни, не только способствуют развитию отношений, но и порождают глобальные проблемы, в частности вооружая преступников новыми орудиями преступлений.

Правоприменительная практика отмечает стремительный рост преступлений, совершаемых бесконтактным, удаленным способом с использованием электронных (цифровых) и информационно-коммуникационных технологий. В доказывании становится все более актуальным использование сведений, о совершенном преступлении, сохраняющихся на электронных носителей информации.

Одно из важных следственных действий, которое осуществляется при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных (компьютерных) технологий, посредством которого добывается необходимая доказательственная информация о причастности лиц к совершенному преступному деянию – производство выемки (обыска, в случае отказа в добровольной выдаче) различных электронных носителей информации.

По смыслу закона, обыск (выемка) осуществляется при наличии достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, а также предметы, документы и ценности, которые имеют значение для уголовного дела.

С криминалистической точки зрения сущность обыска (выемки) заключается в выполнении действий, связанных с принудительным обследованием помещений, транспортных средств и иных объектов. Поскольку целью данного следственного действия является обнаружение и изъятие имеющих отношение

к расследуемому преступлению различных предметов, то в нем присутствует поисковый характер[1].

Для принятия решения о производстве данного следственного действия требуются как фактические, так и процессуальные основания. Фактическими основаниями является наличие информации, позволяющей предположить, что в обследуемом помещении, либо у определенного лица, могут иметься предметы, относящиеся к расследуемому преступлению. При этом, такие сведения могут носить как достоверный характер, так и быть предположительными.

Процессуальным основанием для обыска (выемки) служит постановление следователя, а при обыске жилища — судебное решение.

Вместе с тем, при планировании и производстве данного следственного действия, в ходе которого будет осуществляться поиск и последующее изъятие различных электронных носителей информации, а также иных объектов информационно-телекоммуникационных (компьютерных) технологий, следователю необходимо учитывать разработанные криминалистической наукой тактические приемы обыска помещений, в котором предполагается наличие компьютерной техники.

К иным объектам информационно-телекоммуникационных (компьютерных) технологий, выступающих в качестве орудий преступления, могут относиться: программы ЭВМ, базы данных, информационные системы и (или) сайты в информационно-телекоммуникационной сети «Интернет» или других информационно-телекоммуникационных сетях.

Подготовка к обыску, в ходе которого планируется поиск и последующее изъятие различных предметов (электронных носителей информации), относящихся к расследуемому событию, подразумевает под собой не только принятие решения о производстве данного следственного действия, но и подбор его участников, а также подготовку соответствующих технических средств.

---

[1] Чеботарев Р. А., Челышева О. В. Объективизация доказывания при производстве следственных осмотров и обысков при расследовании убийств // Криминалистъ. 2011. № 1 (8). С. 86.

Участники обыска делятся на обязательных и не обязательных. Так, к обязательным участникам данного следственного действия, помимо следователя, относятся – обыскиваемый или взрослые члены его семьи, а также представитель организации (в независимости от организационно-правовой формы), в помещении которой производится обыск. Проведение обыска в отсутствие этих лиц недопустимо.

Между тем, в ходе производства обыска уголовно-процессуальное законодательство предоставляет право следователю, в целях целесообразности, а также содействия в фото- и видеофиксации, обнаружения, закрепления и изъятия предметов и документов, относящихся к расследуемому преступлению, привлекать к участию различных специалистов.

Так, в ходе производства обыска помещений, в котором предполагается наличие компьютерной техники, и последующее изъятие электронных носителей информации, а также иных объектов информационно-телекоммуникационных (компьютерных) технологий, рекомендуется привлекать к данному следственному действию специалистов в области компьютерных средств и систем.

Задача такого специалиста — оказание помощи следователю в выявлении следов преступления и преступника. Г. М. Шаповалова такие следы, оставляемые при совершении преступлений в сфере использования информационно-телекоммуникационных (компьютерных) технологий обозначила как информационные – «изменение информационной среды в виде сигналов и кодов на электронных и иных физических носителях»[1].

Такие информационные следы могут отобразиться в программном обеспечении компьютера, компьютерной сети или сложной автоматизированной системе управления. При их выявлении они позволяют в совокупности с другими доказательствами сделать вывод о механизме преступления и иных обстоятельствах расследуемого события[2].

---

[1] Шаповалова Г. М. Возможность использования информационных следов в криминалистике : автореф. ... канд. юрид. наук. Владивосток, 2006. С. 7.

[2] Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001. С. 60.

В рамках подготовительного этапа следователю совместно со специалистом необходимо подготовить технику, предназначенную для считывания и хранения информации (ноутбук, различные съемные накопители информации — флешка, внешний жесткий диск и т. д.) [1].

Обыск начинается с фотофиксации места расположения и внешнего вида компьютерных средств. При этом, каждое действие специалиста комментируется им в слух и отражается следователем в протоколе.

Основными объектами, подлежащими осмотру и последующему изъятию в ходе производства данного следственного действия, являются:

— отдельные компьютеры, как не подключенные к сети, так и рабочие станции, входящие в сеть;

— серверы (управляющие компьютеры);

— телекоммуникационные устройства;

— различные запоминающие устройства (USB-накопители, карты памяти в телефонах и фотоаппаратах, SSD, SDRAM и т. д.)

В ходе осмотра компьютеров и периферийных устройств, накопителей информации устанавливается и описывается в протоколе: конфигурация компьютера (с четким описанием всех устройств); номера моделей и серийные номера каждого из устройств; прочая информация, имеющаяся на фабричных ярлыках или этикетках.[2] Кроме того, отмечается наличие, либо отсутствие подсоединенных к компьютерной технике каналов проводной, либо беспроводной связи (wi-fi роутеры).

Если в ходе выполнения обыска установлено, что компьютера включен в сеть, то необходимо описать и произвести фотофиксацию изображения, имеющегося на экране, определить какая программа выполняется в данный момент.

---

[1] Зинин А. М., Семикаленова А. И., Иванова Е. В. Участие специалиста в процессуальных действиях : учебник / под общ. ред. А. М. Зинина. М., 2016. С. 65—69.

[2] Иванов Н. А. Транснациональные преступления, совершаемые с использованием компьютерных и телекоммуникационных технологий (квалификация, теория и практика расследования). Саратов, 2007. С. 94.

При необходимости сохранения информации, имеющейся на компьютерном устройстве, от ее уничтожения от различного рода устройств, специалист может вскрыть кожух системного блока и визуально определить конфигурацию ЭВМ, описать месторасположение электронных плат[1].

Так как, основной задачей специалиста является помощь следователю в выявлении следов преступления и преступника, отображающегося в программном обеспечении компьютера, а также просмотр и изъятие информации, содержащейся в файлах компьютера, то ему необходимо просмотреть содержание дисков, имеющихся в запоминающем устройстве произвольного доступа компьютера (HDD-диск), зафиксировать название файлов и их содержание, а также последние работавшие на устройстве компьютерные программы.

Изъятие информации из оперативной памяти компьютера осуществляется путем ее копирования на заранее приготовленные носители информации, как установленные на имеющиеся у специалиста технические средства (внешний жесткий диск, флеш-карта и т. д.). На месте обыска, рекомендуется распечатать содержимое файлов, записанных на жесткие диски компьютера. Распечатка оформляется в виде приложения к протоколу следственного действия. В ней указывается, на каком типе и виде печатающего устройства, с помощью каких программных средств она выполнена[2].

При изъятии оборудования, специалист завершает работу компьютера и отключает от питания. После отключения от электропитания соединительные кабели и разъемы маркируются, одновременно с этим опечатываются все технические входы и выходы, устройства для ввода информации (устройство для чтения лазерных оптических дисков — CD-диск, флеш-карт и т. д.).

По результатам следственного действия – обыска, следователем составляется протокол следственного действия. В соответствии со ст. 166 УПК РФ в нем должны быть указаны: все технические средства, применение при производстве следственного действия; объекты, к которым эти средства были

[1] Нехорошев А. Б. Компьютерные преступления: квалификация, расследование, экспертиза. Саратов, 2004. С. 85.

[2] Зинин А. М., Семикаленова А. И., Иванова Е. В. Указ. соч.

применены, и полученные результаты. Кроме того, в протоколе должны быть отметки о том, что лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств.

К указанному протоколу прилагаются: фотографические негативы и снимки, киноленты, диапозитивы, фонограммы допроса, кассеты видеозаписи, чертежи, планы, схемы, а также электронные носители информации, полученной или скопированной с других электронных носителей информации в ходе производства следственного действия.

По окончании обыска, протокол подписывается следователем и лицами, участвовавшими в следственном действии.

УДК 343

Л. П. ПИСКУН

АЛГОРИТМ ПОДГОТОВКИ ИСКОВОГО ЗАЯВЛЕНИЯ О ВЗЫСКАНИИ НЕОСНОВАТЕЛЬНОГО ОБОГАЩЕНИЯ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Под преступлениями в сфере информационно-телекоммуникационных технологий в широком смысле следует понимать общественно опасные деяния, запрещенные под угрозой наказания действующим уголовным законом, которые совершены непосредственно с использованием информационных технологий, т.е. приемов, способов и методов применения средств вычислительной техники.

К ним относится более 20 составов преступлений, предусмотренных действующим УК РФ. Спектр таких преступных посягательств «колеблется» от распространения вредоносных компьютерных программ, совершения мошенничеств и краж до распространения противоправной информации, товаров и услуг при помощи сети «Интернет», до преступлений против основ конституционного строя Российской Федерации.

Обновленный Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации, уточнил количество составов преступлений данной направленности[1].

Мошенничества и кражи, совершенные посредством информационных технологий, характеризуются ярко-выраженным корыстным характером.

В связи с этим, жертв таких преступлений, которыми являются в основном пожилые люди, как показывает правоприменительная практика, волнуют не вопросы изобличения виновных лиц и их справедливого наказания, а вопрос возмещения причиненного преступлением имущественного ущерба.

Одним из механизмов такого возмещения может являться возмещение неосновательного обогащения по некоторым уголовным делам данной категории, при соблюдении нескольких обязательных условий, таких как:

— следование требованиям, закрепленным в ст. 45 ГПК РФ;

— установление банковских реквизитов, на которые были перечислены денежные средства, а также лиц (потенциальных ответчиков), на которых они оформлены;

— установление добросовестности (недобросовестности) установленных потенциальных ответчиков.

Согласно ч. 1 ст. 1102 ГК РФ, лицо, которое без установленных законом, иными правовыми актами или сделкой оснований приобрело или сберегло имущество (приобретатель) за счет другого лица (потерпевшего), обязано возвратить последнему неосновательно приобретенное или сбереженное имущество (неосновательное обогащение).

Таким образом, неосновательное обогащение, согласно сформулированной законодателем норме, может выражаться в двух формах: сбережение либо приобретение чужого имущества. Применительно к рассматриваемым в дан-

[1] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : Указание Генеральной прокуратуры Российской Федерации № 401/11, МВД России № 2 от 19 июня 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

ной статье составам преступлений, представляется, что злоумышленники могут неосновательно обогащаться только в одной из представленных форм – приобретение чужого имущества.

В рассматриваемых ситуациях именно прокурор, руководствующийся ст. 45 ГПК РФ, выступает в защиту прав, свобод и законных интересов граждан, которые по состоянию здоровья, возрасту, недееспособности и другим уважительным причинам (неграмотность, отсутствие юридического образования и пр.) не могут сами обратиться в суд с исковым заявлением.

При подготовке такого искового заявления прокурорским работником и сотрудникам поднадзорных правоохранительных органов проделывается тщательная работа, которую кратко можно описать в следующих сменяющих друг друга этапах.

1. Установление дел данной категории в производстве поднадзорного органа.

В момент возбуждения уголовного дела по соответствующим частям ст. 159 УК РФ, а также по п. «г» ч. 3 ст. 158 УК РФ, и поступления копии данного процессуального решения прокурору, прокурорскому работнику, осуществляющему надзор на указанном направлении, необходимо оценивать гипотетическую возможность заявления такого иска. Если потерпевшим по данному уголовному делу является лицо, перечисленное в ст. 45 ГПК РФ, такое уголовное дело подлежит незамедлительному включению в соответствующий реестр уголовных дел прокуратуры района.

2. Заявление потерпевшего.

Без заявления потерпевшего подготовка данной категории исков невозможна. Рекомендуется разработать единый шаблон такого заявления на имя прокурора района в целях упорядочивания всего процесса подготовки иска, который помимо основных данных потерпевшего должен содержать контактные номера телефонов его близких родственников, что особенно актуально по уголовным делам, потерпевшими по которым являются весьма пожилые люди.

Представляется, что регистрация такого заявления в прокуратуре района и порядок его рассмотрения должны осуществляться по общим правилам, установленным Инструкцией о порядке рассмотрения обращений и приема граждан в органах прокуратуры Российской Федерации утв. Приказом Генеральной прокуратуры Российской Федерации от 30.01.2013 № 45.

3. Установление данных ответчика.

Указанная стадия подготовки искового заявления невозможна без активного участия поднадзорного органа. Данные потенциального ответчика устанавливаются на основании ответов на запросы и поручения органа предварительного расследования. В ходе осуществления прокурорского надзора необходимо контролировать своевременное направление таких запросов и поручений следователями и дознавателями незамедлительно после проведения допроса потерпевшего.

В случае необходимости рекомендуется ориентировать следователей и дознавателей на повторное направление таких требований и поручений в случае длительного неполучения ответов на них.

4. Подготовка текста искового заявления.

Как и большинство иных исковых заявлений, данный вид также содержит все основные его части (как правило, вводная, описательная, мотивировочная, просительная и заключительная).

Вводная часть такого искового заявления в обязательном порядке должна отражать полные установочные данные потерпевшего и ответчика, один из их идентификаторов (страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика, серия и номер документа, удостоверяющего личность, серия и номер водительского удостоверения), что предусмотрено ч. 2 ст. 131 ГПК РФ.

Описательная часть иска обычно содержит кратко изложенные обстоятельства уголовного дела, а также сведения, полученные в ходе предварительного расследования (показания потерпевшего, свидетелей и пр.), которые можно подтвердить копиями материалов уголовного дела.

Мотивировочной части искового заявления также не следует быть пространной, что и его описательная часть, но, вместе с тем, представляется обязательным указание на некоторые статьи гражданско-процессуального законодательства, в частности на принцип генерального деликта (ст. 1064 ГК РФ), понятие обязательства (ст. 307 ГК РФ), неосновательное обогащение (ст. 1102 ГК РФ).

Просительная часть искового заявления содержит уточнение требований (сумма, подлежащая взысканию), а также указание на возможное взыскание неустойки за пользование чужими денежными средствами (ст. 395 ГК РФ).

Заключительная часть иска о взыскании неосновательного обогащения представлена сведениями о должностном лице, подписывающем данное исковое заявление, а также оформленным приложением, которое включает копии заявления потерпевшего, а также материалов уголовного дела.

Составной частью иска является приложение, которое представляет собой заверенные копии материалов уголовного дела (протоколы допросов, объяснения, ответы операторов сотовой связи и банковских организаций и пр.), а также расчет неустойки за пользование чужими денежными средствами.

5. Направление искового заявления в суд.

По общему правилу это суд по адресу (месту жительства) ответчика (одного из ответчиков), что предусмотрено положениями ст. 35 Административно-процессуального кодекса Российской Федерации, ст. 28 ГПК РФ.

В настоящее время прокуратурой г. Санкт-Петербурга продолжается работа по внесению гражданских исков в порядке ст. 45 ГПК РФ о возмещении причиненного преступлением вреда в рамках расследования уголовных дел. Аппаратом прокуратуры города также разработаны рекомендации по подготовке исков данного вида (Информационное письмо прокуратуры г. Санкт-Петербурга от 15.11.2023 № 16-21-2023 о направлении типовых искового заявления и протокола разъяснения права на предъявление гражданского иска).

Районные прокуроры ориентированы на ведение такой работы; на сегодняшний день достигнуты определенные результаты. Так, за 10 месяцев

2023 года подготовлено 33 иска данной категории, по 2 из которых имеется 2 заочных решения суда.

Представляется, что развивающийся в настоящий момент механизм взыскания неосновательного обогащения является весьма эффективной мерой, способствующей возмещению ущерба по уголовным делам данной категории.

УДК 343

И. С. ХОВАНОВ

РОЛЬ ПРОКУРАТУРЫ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ В СЕТИ «ИНТЕРНЕТ»

Развитие информационных технологий и глобальной сети «Интернет» открыло практически неограниченные возможности для распространения любой информации. К сожалению, наряду с полезным и познавательным контентом, в киберпространстве активно распространяются материалы экстремистского и террористического характера.

Согласно порталу правовой статистики Генеральной прокуратуры Российской Федерации, в 2022 было зафиксировано беспрецедентное количество правонарушений экстремистской направленности — 1566, что на 509 больше аналогичного показателя предыдущего периода. Эксперты отмечают, что значительная часть экстремистских преступлений приходится на онлайн-пространство и выражается в призывах к агрессии и насилию в интернете[1].

Активное внедрение интернет-технологий, наблюдаемое в последние два десятилетия, принесло как очевидные преимущества в виде доступности информации, так и серьезные проблемы. По мнению В.Л. Назарова и П.Е. Суслонова особо стоит обратить внимание на распространение экстремистских идей среди молодежи, поскольку молодые люди наиболее уязвимы для негативного информационно-психологического воздействия экстремистски

[1] Показатели преступности России // Генеральная прокуратура Российской Федерации. Портал правовой статистики : сайт. URL: https://crimestat.ru/offenses_chart (дата обращения: 14.10.2023).

настроенных лиц и групп[1]. Так, шестнадцатилетний подросток был привлечен прокуратурой Набережных Челнов по ст. 20.29 КоАП РФза размещение двух электронных книг и рисунка, которые были признаны судом запрещенными для распространения на территории Российской Федерации[2].

Контент таких сайтов, как правило, включает историю организации, биографии лидеров, описание целей и врагов, а также новостные разделы. Информация подается в простой и доступной форме, чтобы привлечь как можно больше сторонников. Экстремисты позиционируют себя как борцов за справедливость и свободу, а государство представляют врагом, с которым необходимо бороться. Для этого используются современные интернет-технологии: социальные сети, онлайн-игры, мобильные приложения. Контент адаптируется специально для молодежи — это музыка, видеоролики, мемы.

Одним из способов распространения материалов, содержащих в себе признаки экстремистской направленности, является интернет, который дает людям возможность анонимно выражать любые взгляды, в том числе экстремистские, что снижает ответственность и раскрепощает. В сети легко найти единомышленников и создавать закрытые сообщества, где радикальные взгляды усиливаются. Это создает эффект «эхо-камеры», что может приводить к радикализации[3].

Активно используется личное общение в закрытых чатах и группах. Большую роль в распространении экстремистских материалов играют мессенджеры и социальные сети из-за широкого охвата аудитории и слабых механизмов контроля. Наиболее популярным каналом распространения запрещенного контента является мессенджер «Telegram».

---

[1] Назаров В. Л., Суслонов П. Е. Профилактика экстремизма в молодежной среде : учебное пособие. Екатеринбург, 2018. С. 10.

[2] Прокуратура Набережных Челнов привлекла юношу к ответственности за распространение экстремистских материалов в Интернете // Прокуратура Республики Татарстан : сайт. URL: https://epp.genproc.gov.ru/web/proc_16/mass-media/news?item=77877222 (дата обращения: 23.11.2023).

[3] Хованов И. С. О некоторых проблемах противодействия прокуратурой Российской Федерации экстремизму в сети «Интернет» // Вопросы российской юстиции. 2023. № 26. С. 461.

Сеть «Интернет» играет ключевую роль в пропаганде идеологии экстремизма и вербовке новых сторонников, эта проблема требует пристального внимания и принятия мер со стороны государства.

Одним из основных органов, отвечающим за противодействие экстремизму в сети «Интернет», является прокуратура.

В докладе Генерального прокурора Российской Федерации по вопросам противодействия экстремизму за 2022 год подведены следующие результаты работы прокуратуры Российской Федерации в сфере противодействия экстремизму[1].

Так по итогам работы за 2022 год признаны нежелательными 23 иностранные некоммерческие организации, деятельность еще 17 запрещена как экстремистская, осуществлен ежедневный мониторинг сети «Интернет», который выявил противоправный контент на 180 тыс. страниц, все они заблокированы, прекращено вещание теле- и радиоканалов, распространявших противоправную информацию. Также в докладе отмечается рост количества преступлений с участием несовершеннолетних, что требует усиления профилактики вовлечения молодежи в экстремизм, подчеркнута важность принятия дополнительных мер по противодействию распространению в России экстремизма из-за рубежа.

Правовую основу прокурорского надзора в рассматриваемой сфере составляют ст. 13 Конституции Российской Федерации, которая запрещает деятельность в целях насильственного изменения основ конституционного строя и нарушения целостности Российской Федерации, подрыва безопасности государства, создания вооруженных формирований, разжигания социальной, национальной и религиозной розни, Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 18.12.2022) «О противодействии экстремистской деятельности», Федеральный закон от 17.01.1992 № 2202-1 (ред. от 24.07.2023) «О прокуратуре Российской Федерации» и Федеральный закон от 27.07.2006

[1] Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/gprf/mass-media/news?item=87329761 (дата обращения: 08.08.2023).

№ 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации».

Согласно ст. 15.3 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 02.11.2023) «Об информации, информационных технологиях и о защите информации» Генеральный прокурор РФ и его заместители уполномочены принимать меры по ограничению доступа к интернет-ресурсам экстремистской направленности. Кроме того, ст. 25 Закона о прокуратуре регламентирует порядок объявления предостережения и вынесения предупреждения о недопустимости осуществления экстремистской деятельности.

Прокуроры осуществляют постоянный мониторинг интернет-пространства с целью выявления противоправного контента. При обнаружении экстремистских материалов прокуратура обращается в Роскомнадзор с требованием о блокировке сайта или удалении конкретной информации. Также проводится работа с провайдерами и владельцами ресурсов по недопущению размещения запрещенной информации.

Однако на практике реализация данных полномочий наталкивается на ряд проблем. В частности, в соответствии с приказом Генерального прокурора Российской Федерации от 26 августа 2019 г. № 596, сообщение о противоправном контенте поступает в региональную прокуратуру, где проводится проверка с привлечением экспертов. Лишь затем готовится заключение в Генпрокуратуру для направления требования о блокировке ресурса в Роскомнадзор.

Такой громоздкий механизм замедляет реагирование на угрозы информационной безопасности. К тому же заблокированные сайты нередко создают «зеркала» на других ресурсах, меняя незначительные детали, что усложняет работу правоохранительных органов.

В то же время, как справедливо отмечают Б.В. Андреев и О.А. Инсаров, единые стандарты разработки и эксплуатации информационных систем в прокуратуре отсутствуют, а автоматизация контрольно-надзорной деятельности находится на недостаточном уровне[1].

[1] Инсаров О. А., Андреев Б. В. Цифровая трансформация органов прокуратуры Российской Федерации // Вестник университета прокуратуры Российской Федерации. 2018. № 5. С. 36—41.

Важную роль играет взаимодействие прокуратуры с оперативными подразделениями МВД, ФСБ и другими ведомствами, которые проводят комплексную разведку киберпространства, выявляют экстремистские сообщества, пресекают их деятельность. Совместно с данными органами необходимо продолжать практику информационно-просветительских мероприятий, которые направлены на информирование граждан, а в особенности молодого поколений, с целью донести опасность участия и осуществления экстремистской деятельности в цифровой среде.

Для повышения эффективности прокурорского надзора в сфере противодействия экстремизму в сети «Интернет», которые позволят усилить информационную безопасность и снизить распространенность преступлений экстремистского характера в виртуальном пространстве предлагаются следующие меры:

1. Расширить полномочия региональных прокуроров по направлению требований о блокировке противоправного контента напрямую в Роскомнадзор, минуя Генпрокуратуру.

2. Внедрить автоматизированные системы выявления «зеркал» уже заблокированных сайтов для упрощения процедуры их блокировки.

3. Усилить взаимодействие прокуратуры с Интернет-провайдерами для оперативного установления владельцев IP-адресов, с которых распространяются запрещенные материалы.

4. Необходимо совершенствование статистического учета преступлений экстремистской направленности, совершаемых с использованием сети «Интернет».

5. Создать в структуре прокуратуры специализированные подразделения для мониторинга Интернет-ресурсов и фиксации фактов экстремистской деятельности в сети.

6. Разработать методические рекомендации для повышения эффективности анализа информационных ресурсов на предмет содержания признаков экстремизма.

Подводя итог, можно сделать вывод, что проблема распространения экстремизма в сети «Интернет» становится серьезнее. Особенности онлайн-пространства создают благоприятную среду для пропаганды радикальных идей и вербовки сторонников, несмотря на принимаемые со стороны государства меры, все еще существует ряд проблем, которые снижают эффективность противодействия кибер-экстремизму.

В связи с этим, по нашему мнению, необходима выработка нового комплексного подхода, включающая совершенствование технических средств мониторинга, налаживание взаимодействия государственных органов, активную профилактическую работу с целью повышения кибербезопасности пользователей, что позволит существенно усилить борьбу с распространением экстремистских материалов в сети «Интернет».

УДК 343

А. В. ХОЛОПОВ

СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ВИЗУАЛИЗАЦИИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

С точки зрения познания события преступления, совершенного с использованием электронных или информационно-телекоммуникационных сетей, одной из основных проблем его расследования, является исследование доказательств, представляющих собой большой массив данных (компьютерной, цифровой информации), содержащих информацию (цифровые следы) о деятельности преступника (преступников), например, как на отдельном цифровом устройстве (компьютер, планшет, смартфон, роутер и т. д.), так и на сетевых ресурсах.

Сложность расследования преступлений такого рода, заключается в том, что изъятые большие массивы цифровых данных как доказательственная информация, фактически, представляет собой списки, программные коды, содержащие сведения о деятельности на локальных или сетевых ресурсах, которые невозможно изучить без использования специальных знаний, например, назначение компьютерно-технической экспертизы.

По этой же причине, заключение компьютерно-технической экспертизы, также может быть трудно воспринимаемо, как для следователя на досудебной стадии, так и для присяжных на судебной стадии уголовного судопроизводства. Другими словами, для восприятия и познания такого рода доказательственной информации субъектам уголовного судопроизводства (следователю, прокурору, судье, защитнику, присяжным) необходимо обладать специальными знаниями, позволяющими сформировать в сознании визуальный образ (мысленную модель), воспринимаемой информации, не представленной в наглядной форме.

В этом смысле, доказательственную информацию в виде цифровых (компьютерных) данных необходимо визуализировать, т.е. придать им такую наглядную форму (схемы, графики, диаграммы, модели, инфографика), которая позволит субъектам уголовного судопроизводства познать событие преступления в части деятельности преступника в цифровом пространстве.

Такой процесс визуализации можно рассматривать как переход от отсутствия наглядности (не наглядности) к наглядности, что позволяет субъекту познания чувственно воспринять свойства объекта для формирования в сознании его образа, например, квантовых явлений в физике, и поэтому процесс визуализации заключается в переводе «ненаглядного» в наглядное.

Термин «визуализация», можно рассматривать как синоним наглядности, т.к. наглядность, например, в английском языке, передается следующими словами: visuality, visibility, visual.

Говоря об обеспечении наглядности, отметим, что визуализация является сложным процессом, заключающимся в формировании наглядного образа объекта (предмета, явления, процесса, события, ситуации и т. д.), так называемой визуальной модели в виде информации (схемы, графики, компьютерные модели), отражающей его различные характеристики, т. к. объект невозможно изучить путем прямого наблюдения и восприятия органами чувств субъекта познания.

Если говорить о технологическом понимании термина «визуализация», как о способах и приемах формирования конечного зрительно воспринимаемого образа, то «речь идет о визуальном представлении результатов научных исследований с помощью средств компьютерной графики. Научная визуализация переводит результаты научных исследований, выраженные в численной форме, в видимые, наглядные образы. (…) Главная цель — увидеть то, что раньше нельзя было увидеть. Иначе говоря, увидеть невидимое»[1].

Центральное место в визуализации занимает процесс формирования так называемого визуального или аудиовизуального образа. Различают внешнюю визуализацию как процесс создания и демонстрация с помощью различных научно-технических средств визуальных (аудиовизуальных) образов и внутреннюю визуализацию, связанную с психологическими процессами формирования в сознании субъекта познания визуальных образов в результате восприятия какой-либо информации органами чувств.

Рассматривая уголовное судопроизводство как процесс познания, визуализация, предполагает не только наглядное представление доказательственной информации, например, в виде схем аналитического характера, но и ее систематизацию, т.е. организацию, классификацию и ранжирование массивов данных.

[1] Бондарев А. Е., Галактионов В. А. Анализ развития концепций и методов визуального представления данных в задачах вычислительной физики // Институт прикладной математики им. М. В. Келдыша Российской академии наук : сайт. URL: https://library.keldysh.ru/preprint.asp?id=2009-53 (дата обращения: 30.11.2023).

Систематизация представляет собой «мыслительную деятельность, в процессе которой изучаемые объекты организуются в определенную систему на основе выбранного принципа»[1], а также «деятельность, заключающаяся в научно-обоснованной классификации и ранжировании совокупности конкретных объектов»[2]. Исходя из данного определения, деятельность следователя по формированию уголовного дела, в целом, можно назвать результатом систематизации доказательственной информации на досудебных стадиях уголовного судопроизводства, в которой содержатся данные о событии преступления.

Необходимость систематизации и анализа доказательственной информации может возникнуть на досудебных стадиях для исследования и анализа результатов больших массивов данных, например, информации, предоставленной оператором сотовой связи, а именно детализации телефонных соединений (биллинга); информации, предоставленной провайдером; результатов компьютерно-технической экспертизы и т.д. Заметим, что в процессе предварительного расследования преступления доказательственная информация может быть систематизирована в виде списков-классификаций без использования наглядных форм представления в виде графических схем и т.д.

Полагаем, что визуализации, т.е. придание доказательственной информации наглядных форм, прежде всего, актуальна и значима на судебных стадиях, т. к. согласно ч. 5 ст. 246, ст. 273 и 274 УПК РФ, на государственного обвинителя возложена обязанность представления материалов уголовного дела участникам судебного разбирательства, в особенности с участием присяжных.

---

[1] Новый словарь методических терминов и понятий (теория и практика обучения языкам). М., 2009. // Академик : сайт. URL: https://methodological_terms.academic.ru/1815 (дата обращения: 30.11.2023).

[2] Справочник технического переводчика. – Интент. 2009–2013 // Академик : сайт. URL: https://technical_translator_dictionary.academic.ru/229761 (дата обращения: 30.11.2023).

Так, в 1993 году в письме Генеральной прокуратуры Российской Федерации «О методических рекомендациях об участии прокурора в исследовании доказательств в судебном разбирательстве» отмечалось, что «имеющиеся доказательства, особенно такие, как письменные документы, вещественные доказательства, заключения экспертов, должны быть продемонстрированы в суде наглядно, убедительно, чтобы значение их было понятно не только профессиональным судьям, но и неспециалистам»[1].

Как уже отмечалось визуализация, предполагает и систематизацию информации о чем отмечает Р. А. Мухаметжанова «присяжным заседателям доказательства должны представляться в системе, во взаимосвязи, в заранее определенной последовательности»[2]. В этом смысле, на стадии судебного разбирательства перед сторонами обвинения и защиты может стоять задача наглядного представления сложной системы данных аналитического характера в виде отображения причинно-следственных связей, структур, классификаций, а также различных сравнений и сопоставлений цифровых данных.

На досудебных и судебных стадиях может возникнуть необходимость на основе биллинговой информации, предоставленной оператором сотовой связи провести анализ и наглядно представить его результаты, например, отобразить на карте местности точки перемещения и звонков абонента или отобразить в виде графической схемы круг общения лица или группы лиц и т.д. Также может возникнуть необходимость наглядного сопоставления этих данных с предварительно систематизированной и визуализированной информацией о деятельности лица или группы лиц в интернете, например, в социальных сетях.

---

[1] О методических рекомендациях об участии прокурора в исследовании доказательств в судебном разбирательстве : Письмо Генеральной прокуратуры Российской Федерации от 12 марта 1993 г. № 12/13-93. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Мухаметжанова Р. А. Особенности участия государственного обвинителя в судебном следствии в присутствии присяжных заседателей // Следственная практика : научно-практический сборник / гл. ред. А. Ф. Козусев. М., 2012. Вып. 187. С. 80.

Как уже отмечалось, одна из основных проблем визуализации заключается в том, что необходимо анализировать большой массив данных, для исследования которых необходимо использовать программное обеспечение, позволяющее осуществлять такую обработку, анализ, систематизацию с наглядным отображением в автоматизированном режиме.

Для решения проблем автоматизированной обработки больших массивов данных с последующей визуализацией результатов такой систематизации информации аналитического характера, представляет интерес отечественное специальное программное обеспечение (далее – СПО) «Следопыт» и «Октопус» производства ООО «БалтИнфоКом» г. Санкт-Петербург[1].

СПО «Следопыт» позволяет производить автоматизированный анализ объектов в географической, социальной и событийной среде на основании загруженных данных следующего вида: 1) Биллинг сетей сотовой, спутниковой и иной связи; 2) Данные о принадлежности идентификаторов (учетные данные); 3) Данные систем контроля доступа; 4) Данные треккинговых систем; 5) Данные АИС ГИБДД; 6) Данные о покупке и использовании билетов (Розыск Магистраль); 7) Журналы доступа к серверам; 8) Данные подключения мобильных устройств к Wi-Fi точкам доступа (собранные как со стороны мобильного устройства при криминалистическом анализе, так и со стороны оператора Wi-Fi точек доступа); 9) Данные местоположения камер видеофиксации; 10) Данные местоположения банкоматов/автоматов платежных систем и т. д.

Функциональные возможности СПО «Следопыт» заключаются в следующем: 1) Локализация и классификация мест пребывания; 2) Выявления общих мест пребывания для 2 более объектов анализа; 3) Построение маршрутов передвижения; 4) Прогнозирование поведения; 5) Выявления и отображение смежных телефонных номеров и их хронологии; 6) Исследование динамики поведения; 7) Поиск тесно связанных групп номеров; 8) Сравнение и работа со списками идентификаторов.

[1] БалтИнфоКом : сайт. URL: https://baltinfocom.ru (дата обращения: 30.11.2023).

СПО «Следопыт», прежде всего, ориентирован на проведение анализа биллинговой информации, на основе исследования которой возможно получить полную и наглядную картину о передвижении и поведении исследуемого объекта (лица или группы лиц)[1].

СПО «Октопус» предоставляет собой систему ручной и автоматизированной регистрации, приоретизации и анализа информации о связях сущностей.

СПО «Октопус» может проводить анализ информации на основе таких источников как социальные сети, доски объявлений, платежные транзакции, справочники, внутренние базы данных, новостные ленты, геопривязанные, данные и иных предоставленных на исследование массивов данных.

Функциональные возможности СПО «Октопус» заключаются в следующем: 1) Структурирование и анализ данных в виде графа объектов и связей между ними; 2) Подключение к ведомственным базам; 3) Сбор и обработка данных из открытых источников (госданные, соцсети, новости, объявления); 4) Поиск и непрерывный мониторинг сведений из всех подключаемых (сопрягаемых) ресурсов; 5) Поиск связей и выявление цепочки связанных собеседников; 6) Определение пересекающихся контактов; 7) Построение досье; 8) Построение аналитических отчетов.

Данное СПО предоставляет возможность создать единое пространство связанных данных, полученных из разнородных источников информации, а также позволяет получить полную картину исследуемой предметной области вне зависимости от размытости на временном отрезке и природы входных данных[2].

В уголовном судопроизводстве процессуальной формой закрепления процесса и результатов систематизации и анализа доказательственной информации может являться информационно-аналитическая экспертиза, проводимая в экспертно-криминалистических подразделениях Следственного комитета Рос-

[1] Семейство программных продуктов «Следопыт» // БалтИнфоКом : сайт. URL: https://baltinfocom.ru (дата обращения: 30.11.2023).

[2] Там же.

сийской Федерации. Предметом данной экспертизы является анализ цифровых массивов данных, содержащих сведения о деятельности цифровых систем, устройств, отдельных индивидуумов, в целях поиска взаимосвязей отдельных элементов указанных массивов данных[1].

Отметим, что рассмотренное выше СПО используется экспертами при производстве информационно-аналитических экспертиз.

Как отмечает эксперт экспертно-криминалистического отдела управления криминалистики ГСУ СК РФ по г. Санкт-Петербургу М.А. Гудкова «возможными результатами проведения информационно-аналитической экспертизы (исследования) являются, в том числе: обнаружение общих признаков у ряда преступлений; выявление общих групповых признаков у исполнителей для обобщения серий и исключения случаев, не относящихся к серии преступлений; определение возможного состава соучастников преступления, их информационных связей; выявление информации о событиях и их участниках, скрытых от следствия; помощь в идентификации объекта исследования (например, криминальной сети), понимании природы его деятельности, определении последовательности событий, связанных с этой деятельностью (например, выявление схемы финансовых транзакций для вывода украденных денежных средств за рубеж и т. п.), а также помощь в оценке роли и места каждого события; определение маршрутов передвижения участников преступления; подтверждение или опровержение показаний участников или свидетелей преступления об их действиях, местонахождениях и передвижениях»[2].

Визуализация результатов информационно-аналитического экспертного исследования в зависимости от решаемой задачи может быть представлена в виде: «иллюстрационных таблиц с изображениями графов связей абонентов;

[1] Судебная информационно-аналитическая экспертиза // Судебно-экспертный центр Следственного комитета Российской Федерации : сайт. URL: https://sec.sledcom.ru/categories/iae.html (дата обращения: 30.11.2023).

[2] Гудкова М. А. Актуальные вопросы информационно-аналитических исследований // Расследование преступлений: проблемы и пути их решения. 2018. № 3 (21). С. 156—157.

приложений с графическими изображениями участков местности с нанесенными маршрутами и направлениями перемещения устройств между зонами приема сигнала базовых станций; сведений о направлениях перемещения устройств между зонами приема сигнала базовых станций, зафиксированные в виде видеозаписи рабочего окна специализированного программного обеспечения, используемого для построения графической модели перемещения устройства на местности в интерактивном режиме; приложений, содержащие данные в табличном виде»[1].

Возможности информационно-аналитической экспертизы в части визуализации результатов анализа больших массивов цифровых данных о деятельности лица или группы лиц в информационном (кибернетическом) пространстве (сотовая связь, интернет, данные на локальных носителях) могут быть использованы на стадии судебного разбирательства, в особенности с участием присяжных заседателей.

В заключение отметим, что использование современных возможностей визуализации преступной деятельности, совершаемой с использованием электронных или информационно-телекоммуникационных сетей, следует рассматривать как один из способов моделирования события преступления с целью обеспечения его познания профессиональными и не профессиональными субъектами уголовного судопроизводства.

[1] Там же. С. 159.

МАТЕРИАЛЫ СЕКЦИИ «ТРИБУНА МОЛОДОГО УЧЕНОГО»

УДК 343

А. А. АБДУЛКАДИРОВ[1]

ТРЕШ-СТРИМИНГ КАК СОЦИАЛЬНО ОПАСНОЕ ЯВЛЕНИЕ В СЕТИ «ИНТЕРНЕТ»

В настоящее время благодаря использованию телекоммуникационного пространства люди могут взаимодействовать друг с другом, передавать между собой важную информацию, быть активными участниками современного цифрового общества, прежде всего посредством социальных сетей и мессенджеров.

Однако социальные сети, кроме коммуникативной функции, могут создавать новые угрозы и риски для безопасности граждан и общества в целом: сбор личных данных для последующего шантажа, психологическое давление, распространение информации деструктивного содержания (сведений, способных нанести вред конечным их потребителям).

В сети «Интернет» все чаще можно встретить онлайн-трансляции, пропагандирующие насилие и унижение человеческого достоинства. Одной из разновидностей подобной деструктивной активности является треш-стриминг. Согласно проведенным исследованиям около 54 % мужчин в возрасте от 18 до 24 лет ранее слышали о треш-стримах. Каждый пятый интернет-пользователь лично сталкивался с треш-стримами (20 %) или участвовал в них, при этом более 24 % опрошенных из указанного числа относятся к подросткам и молодежи[2].

---

[1] Научный руководитель — АБДУЛАЗИЗОВА Патимат Гасановна, доцент кафедры государственно-правовых дисциплин, Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук.

[2] «Треш-стримы» в Интернете и как с ними бороться, 22 декабря 2021 г. // ВЦИОМ Новости : сетевое издание. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/tresh-strimy-v-internete-i-kak-s-nimiborotsja (дата обращения: 05.10.2022).

В СМИ неоднократно освещались инциденты, связанные с трансляцией аморального контента на видеохостингах. Так, 4 декабря 2021 г. Раменским судом был вынесен приговор в отношении одного из треш-стримера Станислава Решетняка (Reeflay).

Стример в прямом эфире по просьбам подписчиков оскорблял и наносил неоднократные удары своей девушке, вынес ее в бессознательном состоянии на мороз, в результате чего она скончалась. Обвинение было выдвинуто по ч. 4 ст. 111 УК РФ (умышленное причинение тяжкого вреда здоровью, повлекшее по неосторожности смерть человека).

Подобный инцидент не единичен, на просторах сети «Интернет» можно найти большое количество видео трансляций, которые может посмотреть любой пользователь (в том числе и несовершеннолетние или лица, имеющие проблемы ментального характера). При этом действующим законодательством не предусмотрена какая-либо ответственность за сам факт проведения подобных стримов.

В настоящее время к юридической ответственности стримеры привлекаются только после наступления определенных негативных последствий с участниками подобных стримов.

В рамках заседания временной комиссии по информационной политике и взаимодействию со СМИ, посвященного теме совершенствования российского законодательства, с целью противодействия треш-стримам обсуждалась возможность введения уголовной ответственности за сам факт проведения подобных стримов — в частности, предлагалось дополнить ст. 282 УК РФ следующими положениями: «действия, содержащие унижение человеческого достоинства, с применением насилия и использованием сети «Интернет» в режиме реального времени, а также с целью извлечения материальной выгоды от трансляции подобных действий»[1].

[1] Роскомнадзор поддержал введение уголовной ответственности для организаторов треш-стримов // ТАСС : информационное агентство. URL: https://tass.ru/obschestvo/10513357 (дата обращения: 06.10.2022).

Введение в уголовный закон отдельной нормы, связанной с привлечением к уголовной ответственности лиц, транслирующих в прямом эфире сцены насилия, унижений человеческого достоинства и иных противоправных действий, обязывает дать определение треш-стримингу и установить характерные особенности данного явления.

Сейчас треш-стрим можно охарактеризовать как одну из разновидностей видеотрансляций, в ходе которой неограниченный круг лиц может заплатить ведущему за совершение им действий, явно противоречащих нормам морали и нравственности, а также содержащих сцены насилия, унижений и оскорбления человеческого достоинства. Дискуссионным является вопрос, связанный с определением предмета уголовно-правового запрета в треш-стриминге.

Привлечение к уголовной ответственности за трансляцию с места события нецелесообразно. Ответственность наступает в случае демонстрации сюжета, содержащего сцены насилия и жестокого обращения, например, нанесение побоев за материальное вознаграждение (за поощрения зрителей стрима), причинение вреда здоровью, истязание.

Однако за перечисленные деяния уголовная ответственность уже предусмотрена положениями действующего уголовного законодательства. В условиях проведения треш-стрима, общественная опасность подобных действий увеличивается, и это обусловлено рядом факторов, среди которых можно выделить: 1) распространение контента на неограниченный круг лиц; 2) возможность анонимного пособничества в совершении деяния, когда пользователь регистрируется под чужим «никнеймом» и переводит денежные средства за действия, совершаемые в рамках онлайн-трансляции; 3) основная аудитория треш-стримеров — несовершеннолетние; и просмотр подобных трансляций оказывает деструктивное воздействие на психику подростков, а также преподносит подобную девиацию как норму.

Указанные положения свидетельствует о необходимости введения ответственности в отношении лиц, занимающихся трансляцией в прямом эфире контента, направленного на унижение чести и достоинства человека и содержащего сцены насилия.

Следует отметить, что совершенные в рамках треш-стрима действия аморального характера в большинстве случаев рассматриваются в порядке частного и частно-публичного обвинения. Это означает, что уголовное преследование может быть инициировано только по заявлению потерпевшего (например, по ст. 115 УК РФ).

Для некоторых стримов авторы могут использовать в качестве жертв маргинальные слои населения, которые в полной мере не могут осознавать, что с ними происходит, или сознательно допускают, что с ними могут производиться различные негативные действия (например, участвуют в стримах «за еду», алкоголь или материальное стимулирование).

В последующем, треш-стримеры, чувствуя свою безнаказанность за совершение подобных действий, могут транслироваться наиболее изощренные формы унижения человеческого достоинства. В целях противодействия указанному явлению мы поддерживаем законодательную инициативу Совета Федерации, направленную на привлечение к юридической ответственности лиц, организующих незаконные стрим-трансляции, направленные на уничижение человеческого достоинства и общественной нравственности, а также предлагаем также рассмотреть вопросы о привлечении лиц, принимающих в них участие в качестве целевой аудитории или оказывающих материальную поддержку онлайн-трансляций.

Привлечение к юридической ответственности организаторов и активной аудитории трэш-стримов остается одним из наиболее актуальных вопросов в противодействии распространению деструктивного контента в сети.

Основной вопрос также встает к отнесению новых административно-правовых норм к конкретной норме закона, — прежде всего КоАП РФ: либо к правонарушениям, посягающим на здоровье населения, либо к составам, предусматривающим административную ответственность за незаконные действия в информационно-телекоммуникационных сетях.

Принимая во внимание, что, в случае причинения вреда жизни или здоровью участников трэш-стримов, стример несет ответственность за причаст-

ность к ним как к оконченному составу, то дополнительного отнесения указанных составов к правонарушениям, посягающим, на здоровье населения, предусмотренным главой 6 КоАП РФ, не требуется.

В данном контексте базовую ответственность виновные лица несут за фактическую организацию и участие в трэш-стримах, независимо от наступивших последствий для их участников.

На основании изложенного предлагаем рассмотреть и внесение новых норм в главу 13 КоАП РФ — например, дополнить Кодекс статьей 13.37.1, предусматривающей административную ответственность за распространение владельцем аудиовизуального ресурса информации социально-деструктивного характера, а также оказание помощи в ее организации и распространении.

При этом целесообразным будет и привлечение к уголовной ответственности за совершение описанных выше деяний в тех случаях, когда лицо, в течение года уже привлекалось к административной ответственности по указанной статье, однако продолжило совершать указанные действия, или было замечено за совершением иных действий, потворствующих социально-деструктивному поведению в сети «Интернет».

УДК 343

А. П. АГАРКОВА[1]

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ СУБЪЕКТОВ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

В настоящее время одной из главных угрозой со стороны технологического прогресса, по нашему мнению, следует считать все возрастающую зависимость человека от самой техники. Каждый день новая техника — это лозунг современных реалий. Без технического оснащения современное общество уже

[1] Научный руководитель — АЛЕШИНА-АЛЕКСЕЕВА Екатерина Николаевна, старший преподаватель кафедры уголовного права Санкт-Петербургского университета МВД России.

не представляет своего существования. Работа, досуг, да, почти вся жизнь сконцентрирована в технике. Несмотря на зависимость людей, техника значительно упростила жизнь общества. Если прогресс наступил в сфере технологий, то не стоит забывать, что преступность также не стоит на месте и так же уходит в сферу сети «Интернет». В связи с высокой скоростью ее развития, органы власти не успевают идти с ней в ногу. В результате этого возникают пробелы в праве и отсутствие должного законодательного развития в сфере сети «Интернет».

Множество преступников, остаются безнаказанными или вовсе не найденными в силу своих способностей в сфере новых технологий, им удается обходить систему и избегать наказания.

Преступность в сети «Интернет», как правило не одиночная, чаще всего совершаемая группой или вовсе организованной группой. Однако, согласно нашему законодательству, уголовной ответственности за определенные противоправные действия подлежит лишь то лицо, которое распространило противозаконную информацию.

Среди противоправных действий, в которых предметом выступает информация следует отметить деяние, предусмотренное ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан». Данное преступление включает ответственность за действия, выраженные в виде публичного распространения информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан начально не соответствующая действительности.

Проанализировав судебную практику, было отмечено, что чаще всего вышеуказанная информация распространяется в сети «Интернет» нанося вред общественной безопасности, создавая панику среди населения.

Публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств.

Согласно примечания к ст. 207.1 УК РФ под «обстоятельствами, представляющими угрозу жизни и безопасности граждан, признаются чрезвычайные ситуации природного и техногенного характера, чрезвычайные экологические ситуации, в том числе эпидемии, эпизоотии и иные обстоятельства, возникшие в результате аварий, опасных природных явлений, катастроф, стихийных и иных бедствий, повлекшие (могущие повлечь) человеческие жертвы, нанесение ущерба здоровью людей и окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности населения».

Не стоит недооценивать важность данного общественного опасного деяния в наше время. Ведь тема COVID по сути своей является волнующей нас также как и пару лет назад. Ведь не ясно, какие последствия для организма наступают для людей, переболевших данной болезнью. Соответственно и количество дезинформации, которая вызывает сильную реакцию общественности, не мало, что может повлечь тяжелые последствия для государства и всего общества.

К уголовной ответственности по ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан», могут привлекаться лица, достигшие шестнадцатилетнего возраста, однако, как показывает судебная практика решения в отношении их исключают наступления уголовной ответственности, не смотря на серьезную санкцию данной статьи. Если провести параллель со ст. 207 УК РФ «Заведомо ложное сообщение об акте терроризма», необходимо отметить, что по данной статье субъектом может выступать лицо, достигшее четырнадцатилетнего возраста.

Таким образом, возникает вопрос о возрасте субъектов в представленных статьях. Ведь, в каждой из них говориться о распространении заведомо ложной информации, которая представляет угрозу жизни и безопасности граждан. Так почему же возраст субъектов отличается и как показывает судебная практика по ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан», не смотря на заявленный возраст субъекта, они уходят от наказания. Чем это обусловлено и как аргументировано?

Помимо данного вопроса, необходимо сказать и о том, что преступления, совершаемые с использованием средств массовой информации, значительно усложнили процесс выявления субъекта совершившего преступления. Таким примером, может послужить самое первое уголовное дело по ст. 207.1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан».

Некий пользователь «Петренко» разместил в Twitter видео, где утверждал, что COVID-19 изобрели в Новосибирском государственном научном центре «Вектор» и путем взрыва рассеяли его в России и Китае[1]. Таким образом, «лицо публично распространило под видом достоверных сообщений заведомо ложную информацию об обстоятельствах, представляющих угрозу жизни и безопасности граждан».

По вышеуказанному общественно опасному деянию лицо, совершившее преступление до сих пор, не установлено. Как нам кажется, для повышения уровня раскрываемости уголовных дел связанных с использованием средств массовой информации, следует рассмотреть изменение способа регистрации в информационной сети.

Для регистрации в ней, лицу, будет необходимо указать свои персональные данные, при помощи которых будет легче вычислить преступника. Этот способ уменьшит уровень преступности в сети «Интернет» и средствах массовой информации и повысит уровни раскрываемости данных уголовных дел. Однако, возникнет вопрос о безопасности персональных данных граждан, но учитывая наличие, такого справочно-информационного интернет-портала, как «Госуслуги», то можно говорить о том, что способы защиты персональных граждан уже изучены и проблем с этим не должно возникнуть при грамотном подходе к ним.

[1] Что необходимо изменить в статье 207.1 УК РФ по мнению адвоката // Судебный адвокат : сайт. URL: https://www.advo24.ru/publication/novaya-statya-ob-ugolovnoy-otvetstvennosti-za-rasprostranenie-feykovykh-novostey-o-koronaviruse-nuzh.html (дата обращения: 09.11.2023).

УДК 343

В. В. АДАМОВИЧ[1]

ВОПРОСЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

В современном обществе с развитием информационных технологий также развивается и преступность. Определенную долю в структуре преступности занимают преступления в сфере компьютерной информации, закрепленные в главе 28 УК РФ.

Общественная опасность указанной группы преступлений заключается в посягательстве на особый объект уголовно-правовой охраны в виде компьютерной информации, а также причинении вреда информационной безопасности личности, обществу и государству. Одним из общественно опасных деяний, посягающих на компьютерную информацию, стало создание, распространение и использование вредоносных компьютерных программ.

Данная тенденция подтверждается статистическими данными МВД России, согласно которым в 2020 году было зарегистрировано 510 396 преступлений, совершенных с использованием информационных технологий, в 2021 году — 517 772 преступления, в 2022 году — 522 065 преступлений, из них раскрыто в 2022 году только 142 384 преступления, остальные 73 % совершенных преступлений остались нераскрытыми.

Однако у правоохранительных органов существуют определенные трудности при квалификации подобных преступлений, что не позволяет в полной мере оказывать эффективное уголовно-правовое противодействие киберпреступности.

Объективная сторона рассматриваемого деяния включает в себя обязательный признак в виде деяния, которым является создание, распространение

[1] Научный руководитель — ОГАРЬ Татьяна Андреевна, начальник кафедры уголовного права Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент.

и использование вредоносных компьютерных программ либо иной компьютерной информации. Данные действия по смыслу закона заведомо направлены на несанкционированное копирование, блокирование, уничтожение и модификацию компьютерной информации или нейтрализацию средств защиты компьютерной информации.

Характеристика объективной стороны состава преступления, предусмотренного ст. 273 УК РФ, свидетельствует о том, что моментом окончания рассматриваемого преступления будет являться момент создания вредоносной компьютерной программы, предполагающий завершение кода, направленного на причинение вреда компьютерной информации и создание условий по ее уничтожению, блокированию, копированию, модификации, что препятствует ее нормальному использованию правомерным владельцем такой информации.

В связи с указанным обстоятельством преступление, предусмотренное ст. 273 УК РФ по конструкции является деянием с формальным составом. Некоторые ученые-правоведы указывают на несовершенство объективной стороны преступления, предусмотренного ст. 273 УК РФ, и ее поверхностный характер[1].

Так, даже неглубокий анализ диспозиции ст. 273 УК РФ свидетельствует об отсутствии возможности привлечения лица к уголовной ответственности за приобретение вредоносного программного обеспечения. В случае приобретения лицом вредоносной программы его действия подлежат квалификации как приготовление к совершению иного преступления, посягающего на компьютерную информацию, поскольку в данном случае лицо осуществляет приискание средств и орудий совершения преступления[2].

Однако ввиду того, что преступление, предусмотренное ст. 273 УК РФ, относится к преступлениям категории средней тяжести, то приготовление

---

[1] Кшнякина А. Е. Актуальные проблемы применения ст. 273 Уголовного кодекса Российской Федерации // E-Scio. 2022. № 1. С. 18—19.

[2] Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // Правопорядок: история, теория, практика. 2022. № 4 (35). С. 102—108.

к совершению указанного общественно опасного деяния не является уголовно наказуемым, что создает потенциальные условия по дальнейшему использованию и распространению вредоносных программ. Правоприменительная практика по рассматриваемому преступлению свидетельствует об оценке судами момента приобретения вредоносного программного обеспечения и изучения информации по его эксплуатации, однако указанные действия не влияют на квалификацию, поскольку преступление будет оконченным в момент совершения одного из действий, указанных в ст. 273 УК РФ. Приобретение вредоносного программного обеспечения в данной ситуации остается вне сферы действия ст. 273 УК РФ.

Так, Карпов был признан виновным в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ в том что он реализуя преступный умысел, направленный на противоправные уничтожение, блокирование, модификацию, копирование компьютерной информации и нейтрализацию средств защиты компьютерной информации в целях получения материальной выгоды, приобрел в информационно-телекоммуникационной сети «Интернет» вредоносную программу, предназначенную для нейтрализации средств защиты компьютерной информации, а также установил на свой ноутбук еще несколько вредоносных программ, которые заведомо были предназначены для уничтожения, блокирования, модификации или копирования.

После совершения указанных действий Карпов использовал вредоносную компьютерную программу в целях нейтрализации средств защиты компьютерной информации, а также программы, предназначенные для уничтожения, блокирования, модификации и копирования компьютерной информации, в результате чего на экране потерпевшего появлялась надпись, содержащая предложение о разблокировке заблокированной компьютерной информации за денежное вознаграждение[1].

[1] Приговор Череповецкого федерального городского суда Вологодской области от 13 января 2020 г. по делу № 1-95/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.03.2023).

Различные рекомендации по созданию вредоносных программ содержатся в информационно-телекоммуникационной сети «Интернет», а также существует отдельный «черный» рынок вредоносного программного обеспечения, что свидетельствует о значительном количестве предложений по приобретению вредоносного кода.

Данное обстоятельство указывает на широкую общественную опасность приобретения вредоносных компьютерных программ, поскольку после приобретения указанных программ может быть осуществлено их использование в целях противоправного уничтожения, блокирования, модификации или копирования компьютерной информации. Кроме того, результат от создания указанных программ и их приобретении является сходным – появление у лица вредоносной программы, которая может быть использована для нанесения ущерба компьютерной информации.

Основное различие в действиях по созданию и приобретению вредоносной программы заключается в том, что процесс создания вредоносной программы требует от лица применение определенных знаний в области программирования, когда процесс приобретения может быть осуществлен и без наличия указанных навыков, что расширяет перечень возможных субъектов совершения общественно опасного деяния.

Также создание вредоносный программы заключается в получение как результата противоправных действий качественно нового кода, когда приобретение вредоносной компьютерной программы предполагает получение лицом уже существующего кода.

Однако важно отметить, что в случае, когда лицо использует инструкции по созданию вредоносного программного обеспечения, оно не получает качественно новую программу, а лишь модифицирует уже существующую, однако такие действия лица подлежат квалификации по ст. 273 УК РФ[1].

[1] Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // Правопорядок: история, теория, практика. 2022. № 4 (35). С. 105—106.

Таким образом, деяние лица по приобретению вредоносной программы имеет определенную степень общественной опасности, поскольку данные действия лица создают условия по дальнейшему распространению таких программ и их использованию, которые обладают большими характером и степенью общественной опасности, ввиду чего необходимо внести законодательные изменения в ст. 273 УК РФ посредством включения в нее такого признака объективной стороны как приобретение вредоносной компьютерной программы.

Данное законодательное изменение предназначено для дифференциации уголовной ответственности за приобретение вредоносных компьютерных программ и их создание, распространение или использование посредством выделения в ч. 1 ст. 273 УК РФ общественно опасного деяния по приобретению вредоносных компьютерных программ с категорией преступления небольшой тяжести, в части второй рассматриваемой статьи действий по их созданию, использованию или распространению с категорией преступления средней тяжести.

Отдельным вопросом доктрины уголовного права является вопрос относительно субъективной стороны состава преступления, предусмотренного ст. 273 УК РФ. Существуют разные точки зрения относительно формы вины в рассматриваемом преступлении. Ввиду того, что по смыслу закона преступление, предусмотренное ст. 273 УК РФ по конструкции состава преступления является формальным, то оно может быть совершено исключительно с прямым умыслом.

Однако п. 11 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» указывает на то, что использование вредоносных компьютерных программ предпо-

лагает совершение лицом действий по применению указанных программ, в результате которых происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты, что по смыслу охватывает и общественно опасные последствия, в связи с чем состав преступления в форме использования исходя из рассматриваемой формулировки приобретает материальных характер.

Например, В.Н. Черкасов и В.М. Быков считают, что общественно опасное деяние, предусмотренное ст. 273 УК РФ может быть совершено исключительно с прямым умыслом. По их мнению, лицо, совершающее преступление, предусмотренное ст. 273 УК РФ, должно осознавать фактический характер и общественную опасность своих действий и желать их совершить[1]. При оценке действий лица, совершившего общественно опасное деяние, предусмотренное ст. 273 УК РФ, следует установить уровень его фактической осведомленности о вредных свойствах компьютерной программы.

Иной точки зрения придерживаются такие ученые-правоведы как В.И. Гладких, И.Н. Мосечкин, которые считают, что общественно опасное деяние, предусмотренное ст. 273 УК РФ может быть также совершено с косвенным умыслом помимо прямого. Они указывают, что лицо, совершающее преступление, предусмотренное ст. 273 УК РФ, должно осознавать фактический характер и общественную опасность своих действий по созданию, использованию или распространению вредоносного программного обеспечения, предвидеть возможность наступления общественно опасных последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации, желать или не желать наступления таких последствий, но сознательно допускать наступление таких последствий, либо относиться к ним безразлично[2].

---

[1] Быков В. М. Черкасов В. Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ // Российский судья. 2012. № 7. С. 36—37.

[2] Гладких В. И., Мосечкин И. Н. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации // Всероссийский криминологический журнал. 2021. № 2. С. 232—233.

Поскольку указанное преступление по своей конструкции является преступлением с формальным составом, то косвенный умысел в таких составах просто невозможен. На наш взгляд видится верной позиция, которая допускает совершение преступления, предусмотренного ст. 273 УК РФ исключительно с прямым умыслом.

Данное обстоятельство обуславливается тем фактом, при котором лицо целенаправленно создает, использует и распространяет компьютерную программу, являющуюся вредоносной, предназначенную для уничтожения, блокирования, модификации, копирования компьютерной информации. В данном случае вредоносный характер программы свидетельствует о стремлении лица к совершению с вредоносной программой действий, которые приведут к неправомерному уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации.

Характеризуя субъективную сторону преступления, предусмотренного ст. 273 УК РФ, необходимо отметить, что диспозиция рассматриваемой статьи содержит указание на такой признак как «заведомость». Данный признак предполагает достоверное знание лица о предназначении создаваемых, используемых или распространяемых им компьютерных программ для уничтожения, блокирования, модификации или копирования компьютерной информации. Также признак «заведомости» предполагает осведомленность лица о вредоносном характере компьютерной программы. Так, согласно позиции Т.М. Лопатиной, лицо, которое заблуждалось относительно вредоносных свойств компьютерной программы, не подлежит привлечению к уголовной ответственности, в связи с чем имеет место ошибка[1].

В связи с указанным обстоятельством из-за отсутствия единого понимания дефиниции «заведомость» возникает правовой пробел, который используют киберпреступники при совершении преступлений. Предлагается заме-

[1] Каражеляскоv Б.А., Карпушева Л.Н., Юнусов М.Ф. Проблемы уголовной ответственности в сети «Интернет» // Образование и право. 2022. № 11. С. 290-291.

нить признак «заведомо» на понятие «заведомо предназначенных для». Данная корректировка позволит исключить возможность обхода действующего уголовно-правового запрета.

Таким образом, преступление, предусмотренное ст. 273 УК РФ, обладает достаточно высокими характером и степенью общественной опасности, однако норма, регламентирующая ответственность за создание, использование и распространение компьютерных программ имеет определенные пробелы, не позволяющие использовать ее эффективно в полной мере. В частности, не охватываются сферой действия уголовного закона действия лица по приобретению вредоносной компьютерной программы, а также остается неурегулированной форма вины, с которой может быть совершено преступление, предусмотренное ст. 273 УК РФ. Решение данных проблем позволит создать единообразную судебную практику, а также повысить эффективность применения ст. 273 УК РФ.

УДК 343

А. Д. АДОВСКОВА,
О. С. ГРИЦАЕВА[1]

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Мошенничество — одна из наиболее динамично развивающихся форм корыстной преступности. Изменчивость конъектуры рынка, политической и экономической ситуации не только в Российской Федерации, но и на международной арене предопределяет совершенствование существующих и появление новых способов совершения мошенничества, в том числе в сфере компьютерной информации. Мошенничеству как криминологическому и уголовно-правовому типу корыстной преступности не присуща статичность и однообразность.

[1] Научные руководители — ДВОРЖИЦКАЯ Марина Андреевна, старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук; ПИСАРЕВСКАЯ Елена Анатольевна, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

В УК РФ целых шесть статей посвящены регламентации уголовной ответственности за мошенничество (ст.ст. 159—159.6 УК РФ). Данный факт обусловлен своевременной реакцией законодателя на появляющиеся новые формы совершения такого традиционного деяния как мошенничество. Криминализацию новых форм мошенничества можно оценить как своевременную. Однако следует отметить, что на практике остается наиболее востребованной «классическая» статья о мошенничестве, которая также не исключает возможность применения анализируемых технологий.

Согласно статистике МВД России, в 2022 году количество преступлений, связанных с информационно-телекоммуникационными технологиями и компьютерной информацией, выросло на 0,8 % по сравнению с предыдущим годом, достигнув отметки в 522 тыс. случаев. Данный факт означает, что преступления в сфере IT и компьютерной информации составили 26,5 % от общего числа зарегистрированных преступлений. Из них было зарегистрировано 257 606 мошенничеств, предусмотренных ст.ст. 159, 159.3, 159.6 УК РФ, совершенных с использованием указанных технологий или в обозначенной сфере. Темп прироста по указанным видам мошенничеств в 2022 года по отношению к 2021 году составил +3,4 %. При этом большинство из этих деяний — 244 984 составили мошенничества, предусмотренные ст. 159 УК РФ, 7 288 — это деяния, предусмотренные ст. 159.3 УК РФ, 334 — это преступления, предусмотренные ст. 159.6 УК РФ.

Этот рост преступности в сфере информационных технологий может быть связан с быстрым развитием цифровой экономики и все большей зависимостью общества от компьютерных систем. Современные технологии предоставляют множество возможностей, но также открывают двери для новых видов преступлений, таких как кибермошенничество, хакерские атаки, онлайн-воровство личных данных и другие.

Однако необходимо отметить, что рост числа зарегистрированных преступлений в данной сфере также может быть связан с увеличением осведомленности и готовности жертв сообщать о преступлениях. Сегодня все больше

людей осознают важность кибербезопасности и знают, куда обратиться в случае преступления. В целом, борьба с преступлениями в сфере информационных технологий остается приоритетной задачей для правоохранительных органов. Необходимо продолжать развивать сотрудничество между государством, компаниями и обществом, чтобы эффективно противостоять киберпреступности и обеспечить безопасность в онлайн-среде.

Приведем также другие статистические данные. По статистике Центрального банка Российской Федерации 3 квартал 2022 года охарактеризовался снижением регистрации кибермошенничества по сравнению с аналогичным периодом 2021 года.

Так, количество зарегистрированных случаев мошенничества в указанный период снизилось на 10,3 %, до 229,8 тыс. Тем не менее сокращение численности самой преступности не говорит о снижении общего размера ущерба. Согласно «Обзору отчетности об инцидентах информационной безопасности при переводе денежных средств» размер ущерба составил почти 4 млрд рублей, а значит по сравнению с 2021 годом он вырос на 23,9 %[1].

Экстраполируя тенденцию возрастания регистрации преступлений данной категории, можно предположить, что в последующие пять лет будет происходить их дальнейшее увеличение. Этому будут способствовать внедрение в преступные схемы новых технологий социальной инженерии и использование современных IT-средств (SIMBOX; средства IP телефонии)[2].

Выделим детерминанты анализируемых видов мошенничеств. Следует отметить, что они в ряде аспектов схожи с классическими детерминантами мошенничества, но также имеют свои специфические особенности. К уникальным детерминантам мошенничества с использованием компьютерной информации можно отнести следующее:

---

[1] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за 2022 год. URL: https://cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 20.11.2023).

[2] Молчанова Т. В., Аксенов В. А. Факторы, обуславливающие мошенничество, совершенное с использованием информационно-телекоммуникационных технологий // Вестник экономической безопасности. 2020. № 2. С 50—55.

— современные технологии предоставляют возможность анонимного ведения деятельности в сети «Интернет»;

— сетевые технологии — это средство массового воздействия, а значит, субъекту преступления не составляет труда найти потенциальную жертву;

— недостаточность социально-правового контроля со стороны общества за процессами информатизации;

— некоторые недостатки правового регулирования в области электронной торговли и защиты прав потребителей;

— неустраненные недостатки правоохранительной системы.

Кроме того, С.В. Ямашкин обоснованно указывает на то, что одним из факторов, способствующих увеличению числа преступлений в сфере высоких технологий, является недостаточное использование современных компьютерных систем защиты и использование устаревших средств защиты со стороны коммерческих организаций[1].

С каждым годом процесс цифровизации становится более интенсивным и люди вынуждены приспосабливаться к новым технологиям независимо от своего желания. Интернет и соцсети стали неотъемлемой частью жизни практически каждого человека. С одной стороны, в этом есть большое количество плюсов, таких как удобство и доступность любой информации. С другой стороны, из-за столь тесного соприкосновения всемирной паутины с жизнью человека, он становится более уязвимым. «Несмотря на виртуальность всемирной сети жертвы мошенничества несут реальные экономические потери»[2].

Стоит выделить наиболее важные, по нашему мнению, существующие проблемы противодействия анализируемым видам мошенничества:

Первой проблемой можно назвать трудности выявления самого факта преступления. Сложности в его выявлении обуславливаются прежде всего тем, что в большинстве случаев потерпевшие не обращаются в полицию, по-

[1] Ямашкин С. В. Организованное мошенничество: уголовно-правовой и криминологический аспекты : дис. … канд. юрид. наук. Самара, 2010. С. 15.

[2] Стеценко Ю. А., Холодковская Н. С. Мошенничество в сети «Интернет» // Вестник Таганрогского института имени А. П. Чехова. 2021. № 2. С. 76.

нимая, что установить личность преступника будет практически невозможной. По данным ЦБ, в III квартале 2022 году россияне перевели мошенникам денежные средства 258 097 раз, на сумму почти 3,3 млрд рублей[1]. И это только известная сумма ущерба, а о реальной сумме, которая была переведена мошенникам, остается только догадываться.

Второй проблемой, уже немного затронутой в ходе рассмотрения первой, являются трудности, возникающие при обнаружении и установлении личности, совершившее преступление. Сегодня любой человек, используя компьютерные технологии, может оставаться анонимным как в соцсетях, так и в сети «Интернет» в общем. Этот фактор и придает мошенникам большую степень уверенности в их безнаказанности. Ведь действительно, найти в современном мире некое лицо, не зная о нем никаких правдивых персональных данных — не представляется возможным.

Следующей проблемой является динамичность развития информационных технологий и способов их использования в преступной деятельности мошенников, что обуславливает необходимость постоянного совершенствования механизмов противодействия данным деяниям.

Мошеннические схемы в этой сфере придумываются и совершенствуются практически ежедневно. Этот факт не позволяет выделить единые наиболее действенные мероприятия, посредством постоянного проведения которых можно эффективно воздействовать на детерминанты, им способствующие.

Наличие наиболее уязвимых категорий населения, которые в силу возраста и других факторов не способны самостоятельно учитывать существующие и возникающие риски в анализируемой сфере, к которым следует отнести пенсионеров, несовершеннолетних и др. Указанные категории населения не всегда понимают многие информационные, компьютерные и социальные процессы, и их неграмотность может быть использована мошенниками под

[1] Статистика Банка России за 3 квартал 2022 г. // Центральный банк Российской Федерации : офиц. сайт. URL: https://www.cbr.ru/ (дата обращения: 20.11.2023).

предлогом соответствующей помощи[1]. К сожалению, даже несмотря на ежедневное информирование населения в СМИ об имеющихся случаях совершенных преступлений, где подробно рассказывается о способе мошенничества с целью предотвращения появления новых жертв, люди продолжают попадаться на «крючки» мошенников.

Таким образом, можно с уверенностью утверждать, что анализируемые преступления являются одной из наиболее распространенных разновидностей хищения имущества и неправомерного получения прав на него, которое совершается с использованием совершенно разных способов и наличия сведений о потенциальном потерпевшем. Существенное увеличение числа указанных преступлений объективно обусловлено наличием конфиденциальности в сети «Интернет», которая и позволяет злоумышленникам оставаться инкогнито.

Существующая на сегодняшний день система противодействия мошенничеству, как нам представляется, недостаточно эффективна и требует совершенствования механизмов противодействия.

УДК 343

В. С. АЛФЕЕВА[2]

ДЕТЕРМИНАНТЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО ЧАСТЬЮ 2 СТАТЬИ 280 УК РФ

На уровне международного уголовного права понятие экстремизма определено в Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом. Согласно статье 1 данного документа «экстремизм» —какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных

[1] Синявская С. П. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Криминалистъ. 2020. № 4. С. 3—7.

[2] Научный руководитель — КАДЫРОВА Надежда Николаевна, доцент кафедры уголовно-правовых дисциплин Челябинского государственного университета, кандидат юридических наук, доцент.

вооруженных формирований или участие в них[1]. Сам факт закрепления данного деяния качестве конвенционного преступления свидетельствует о его высокой общественной опасности.

Понятие экстремистской деятельности является нормативно закрепленным и в Российский Федерации. Оно содержится в статье 1 Федерального закона от 25.07.2002 № 114-ФЗ (ред. от 15.07.2023) «О противодействии экстремистской деятельности».

Под призывами к осуществлению экстремисткой деятельности следует понимать действия, так или иначе направленные на призывы к данным деяниям. Они будут проявляться во влиянии на сознание и волю с целью побудить людей к совершению определенных действий.

Как указывает Стратегия противодействия экстремизму в Российской Федерации**,** информационно-телекоммуникационные сети, включая сеть «Интернет»[2], стали основным средством связи для экстремистских организаций, которое используется ими для привлечения в свои ряды новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии.

Кроме того, среди основных направлений государственной политики данная стратегия называет проведение мониторинга средств массовой информации, совершенствование мер по ограничению доступа к информационным ресурсам на территории Российской Федерации, координацию мер, направленных на информационное противодействие распространению экстремистской идеологии в сети «Интернет» и многое другое.

Сам факт наличия данных направлений свидетельствует об определенном состоянии обеспокоенности государства. Действительно, широкая распро-

[1] Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом : подписана 15 июня 2001 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Стратегия противодействия экстремизму в Российской Федерации до 2025 года : Указ Президента Российской Федерации от 29 мая 2020 г. № 344. Доступ из справ.-правовой системы «КонсультантПлюс».

страненность данных деяний в последние годы не может не вызывать беспокойство. Однако до сих пор не выработано каких-либо эффективных мер по борьбе с данным видом преступности. Те способы, которые существуют сейчас, например, специальные алгоритмы в социальных сетях, имеют слишком широкую сферу действия и не могут использоваться, в связи с этим в той мере, в которой это необходимо.

В последние годы наблюдается тенденция публикаций в социальных сетях той информации, которая прямо или косвенно содержит призывы к осуществлению экстремистской деятельности. На данную тенденцию, по нашему мнению, влияют два основных фактора:

Текущая обстановка в мире, которая не может не сказываться на сознании людей, внося определенные изменения. Эти психологические процессы приводят к тому, что люди начинают высказываться подобным образом. Это приводит к повышению общественной опасности, в результате чего срабатывает простой механизм уголовного права: чем выше опасность от преступности того или иного деяния, тем более востребованной становится норма, определяющая ответственность за данное деяние.

Развитие техники и, как следствие, развитие и расширение информационно-телекоммуникационной сети «Интернет». Данная сеть уже не первый десяток лет охватывает многие области жизни людей и лишь расширяет свою важность, в связи с чем сейчас медиа-пространство можно смело приравнивать реальной жизни по своему значению. Конечно, у данного явления есть и преимущества, но они неразрывно связаны с осознанностью потребления. Нас в данном случае интересует негативная сторона данного процесса.

В первую очередь, в качестве средств совершения данных преступлений выступают социальные сети. Это обусловлено рядом признаков, характерных именно для социальных сетей. Самым глобальным, по нашему мнению, является наличие специальных алгоритмов. Они предлагают ту информацию, на источники которой у пользователя даже не имеется подписки. Следовательно,

распространение такой информации не имеет точного круга адресантов и может быть просмотрено широким кругом пользователей. Вторым по масштабу являются быстро набирающие популярность в данный момент мессенджеры. Они не настолько удобны как социальные сети ввиду отсутствия ленты, комментариев и прочего. Однако наибольшее количество пользователей сосредоточено именно там. Кроме того, для обсуждения каких-либо действий, в том числе агитации, удобны именно они.

Вторым признаком является удобство использования и интерфейса. Для того, чтобы разместить запись или видеоматериал необходимо лишь нажать на несколько клавиш, что не занимает много времени. А яркие изображения будут привлекать внимание пользователей, что также способствует распространению.

Третьим признаком можно выделить условную анонимность. Для регистрации аккаунта не требуется указание каких-либо связанных с личностью данных, будь то фамилия или номер телефона. Исходя из этого, пользователи убеждены в своей анонимности и, как следствие, безнаказанности.

Ввиду ранее сказанного, можно выделить внешние и внутренние детерминанты. Внешние детерминанты связаны с доступностью сети «Интернет». Практически у всех смартфон находится всегда под рукой, в связи с чем нажать на несколько значков не представляет трудностей.

Также, поскольку медиа-пространство уже практически неотделимо от реальности, часть жизни сосредоточена именно там. В особенности это касается подростков и молодежи в целом. В связи с этим такой процесс как выражение своей позиции также переходит в интернет.

Это связано прежде всего с тем, что высказывание в сети имеет намного больший охват, чем даже выражение в местах массового скопления людей. Элемент удобства также играет свою роль: не нужно совершать никаких действий по выходу из дома, тратить время и ресурсы. Кроме того, общество в целом устроено так, что выражать свое мнение, прячась за набором букв, намного легче. Все эти установки вкупе и образуют внешние детерминанты.

При анализе приговоров можно выявить определенное сходство: достаточно большое количество – это несовершеннолетние и молодежь. Именно они, как известно, являются основными и наиболее активными пользователями социальных сетей. Их личность еще не сформирована окончательно, посему для этой группы характерно желание так или иначе выделиться. Причем, разница между выделением из толпы и совершением противоправных поступков для них не является ощутимой.

Внутренние детерминанты связаны с психологическими особенностями личности. Как уже было сказано, обстановка довольно сильно влияет на сознание людей, что побуждает в людях агрессию и ненависть, которая выливается в социальных сетях. Кроме того, в данный момент существует такое отношение к праву как правовой инфантилизм, выражающийся в пренебрежительном отношении к законодательству, в том числе и к нормам УК РФ. Людям становятся безразличны предписания уголовного законодательства.

К этому фактору также добавляется низкая правовая культура и отсутствие патриотического воспитания в сознании людей. В связи с этим у человека теряется понимание того, что даже нечто незначительное по его меркам, будь то комментарий или пост в социальной сети, может привести к определенным последствиям. В том числе, к уголовной ответственности.

Исходя из приговоров можно вывести и основные направления экстремисткой деятельности, призывы к которой осуществляются. В основном, это касается расовой и религиозной ненависти и вражды.

Так, например, Ленинский районный суд г. Махачкалы Республики Дагестан вынес приговор в отношении лица, которое разместило в социальной сети «Instagram»[1] видеоматериал, на котором имеются призывы к осуществлению экстремисткой деятельности. Причем, размещение такого материала носило

[1] Instagram принадлежит компании Meta, признанной экстремистской организацией и запрещенной в Российской Федерации.

не разовый характер. Данным лицом было размещено сразу несколько видеоматериалов, что позволяет говорить о системности совершения такого деяния[1]. У человека явно сформированы определенные радикальные взгляды, которые он стремится транслировать в массы при помощи сети «Интернет».

«Несмотря на то, что уже осталось две недели, работу нужно усилить изо всех сил. Агитируем в массовых скоплениях людей про революцию 5-го ноября», — с таких слов начался пост лица в социальной сети «ВКонтакте» согласно приговору Волжского районного суда[2].

Основной причиной в данной ситуации является отсутствие либо неэффективность патриотического воспитания. Поскольку призыв к осуществлению подобной деятельности в контексте интересов государства говорит о том, что у лица присутствует низкий уровень правовой культуры и, как следствие, полное неуважение к своему государству. И если предыдущий пример можно рассматривать с точки зрения необдуманных импульсивных поступков, то данное деяние явно носит осознанный характер. И, как следствие, опасность для общества становится значительно выше.

Таким образом, подводя итог детерминантам ч. 2 ст. 280 УК РФ можно разделить их на две категории: внешние и внутренние. Внешние даже нашли свое отражение в диспозиции данной части. Сеть «Интернет» все плотнее входит в повседневную жизнь, в связи с чем растет число преступлений, совершаемых с его использованием. То есть сама по себе причина совершение подобного деяния – информационно-телекоммуникационная сеть «Интернет», глобализация является непреодолимым процессом.

Однако остаются также и внутренние причины, связанные с взглядами самой личности на окружающую действительность. Именно с этой позиции и

[1] Приговор Ленинского районного суда г. Махачкалы от 11 ноября 2022 г. по делу № 1-713/2022 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 09.10.2023).

[2] Приговор Волжского районного суда от 12 ноября 2018 г. по делу № 1-220/2018 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 09.10.2023).

возможна профилактика совершения данного рода преступлений. В первую очередь, это потребует усилий со стороны самого государства. Например, разработка и реализация разного рода программ по правовому просвещению и воспитанию в гражданах патриотизма и толерантности. Целевой аудиторией для реализации таких программ должны стать преимущественно несовершеннолетние, поскольку именно они в силу своих возрастных особенностей наиболее подвержены воздействию со стороны. И будет правильно, если это воздействие будет позитивным и исходить от государства.

УДК 343

А. В. БАРСУКОВА[1]

ПРИЗНАКИ ОБЪЕКТИВНОЙ СТОРОНЫ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 159.6 УК РФ

Президент Российской Федерации Владимир Путин на расширенном заседании коллегии МВД 20 марта 2023 года отметил, что преступления в сфере информационных технологий в 2022 году составили четверть от общего количества совершенных преступлений (510 тысяч), и уточнил, что в таких условиях борьба органов правопорядка с информационной преступностью является одной из первостепенных задач[2].

Подобная тенденция складывается в виду цифровизации всех сфер жизни общества: сейчас благодаря компьютеру можно получить не только доступ к информации, но и, например, заказать продукты, записаться на прием ко врачу, подать заявление в государственные органы и много другое. При этом цифровизация не является исключительно положительным явлением, поскольку для совершения всех вышеуказанных действий необходимо

[1] Научный руководитель — БЕЗБОРОДОВ Дмитрий Анатольевич, профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

[2] Число киберпреступлений в России // Tadviser : сайт. URL: https://www.tadviser.ru/index.php/ (дата обращения: 02.11.2023).

предоставление данных о личности, например, номера телефона, места жительства, реже – паспортных данных и иной информации.

На данный момент имеется множество развитых форм хищения денежных средств с помощью информационных технологий: фишинг, мошенничество на платформах интернет-магазинов, мошенничество с использованием платежных карт, скимминг и некоторые иные виды. Особо развитыми представляются мошеннические схемы.

В виду постоянного развития и появления новых схем использования компьютерной информации при мошенничестве УК РФ дополняется новыми статьями и изменениями в уже существующие. Тем не менее это не решает всех проблем квалификации, судебная практика также все еще далека от совершенства.

В связи с вышеуказанным, в виду интенсивного распространения компьютерной преступности существует необходимость рассмотреть положения ст. 159.6 УК РФ и вносимые в нее изменения в целях разработки предложений по совершенствованию данной уголовно-правовой нормы.

Статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации» впервые была введена Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». До момента принятия закона данный вид мошенничества квалифицировался по совокупности норм об имущественных преступлениях и преступлениях в сфере компьютерной информации, например, фишинг или хищение средств с банковских счетов благодаря получению логина и пароля путем направления SMS-сообщений гражданину квалифицировались по совокупности мошенничества и неправомерного доступа к компьютерной информации[1]. Данный подход к квалификации хоть и применялся, однако приводил к ошибочной оценке деяния и к размытости разграничения смежных составов преступлений, ввиду разрозненности практического применения.

[1] Приговор Старооскольского городского суда Белородской области от 12 мая 2011 г. // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

Тем не менее, по мнению некоторых ученых введение специальной статьи не решило проблемы квалификации информационного мошенничества, а в некоторых случаях, даже наоборот, усугубило некоторые коллизии[1]. Так, например, В.И. Гладких считал, что нововведенная норма по своему составу не соответствует основным признакам мошенничества, следовательно, не может называться «мошенничество»[2].

По мнению Р.Ю. Шергина применение новой нормы на практике приводит к размытости разграничения преступлений, в которых компьютерная информация является средством обмана потерпевшего гражданина, и преступлений, когда компьютерная информация является лишь способом устранения препятствий для совершения иных форм хищения[3].

Кроме того, сравнивая с ранее приятным подходом к квалификации можно говорить о том, что в нем нормы главы о преступлениях сфере компьютерной информации как бы дополняли нормы главы об имущественных преступлениях при их совместном вменении, однако после введения ст. 159.6 УК РФ такое дополнение стало применяться намного реже, а в большинстве случаев нормы главы о компьютерных преступлениях создают конкуренцию норм с составом мошенничества.

На практике единый подход также не был сформирован — зачастую одни и те же деяния, например, мошенничество с помощью SMS-сообщений о переводах со счета или выполнении входа в приложение банка с другого устройства, благодаря которым злоумышленники получали настоящие данные о логине и пароле лица, разными судами квалифицировались и как кража, и как простое мошенничество, и как компьютерное мошенничество.

---

[1] Чернякова А. В. Актуальные аспекты уголовной ответственности за хищения, совершаемые с использованием информационно-коммуникационных технологий // Юридическая наука и правоохранительная практика. 2019. № 3 (49). С. 125.

[2] Гладких В. И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. № 22. С. 28.

[3] Шергин Р. Ю. Уголовная ответственность за компьютерное мошенничество: новое не всегда лучшее // Законность. 2017. № 5 (991). С. 47—48.

Для формирования единого правоприменительного подхода в 2017 году было принято Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». В данном Постановлении признаком, разграничивающим компьютерное мошенничество с иными формами хищения, являлось использование при совершении мошенничества такого способа как вмешательство в функционирование средств, хранения, обработки и передачи компьютерной информации или информационно-телекоммуникационных сетей, имеющее целенаправленное воздействие (ссылка).

В части данное положение помогло в формировании единообразного подхода и разъяснило судам, что следует считать вмешательством, однако при этом вопрос о том, является ли данной способ совершения хищения мошенничеством, разрешен не был и дискуссия в научных кругах продолжилась[1].

В 2018 году Федеральным законом от 23.04.2018 № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в ст. 159.6 УК РФ было внесено следующее дополнение: «с банковского счета, а равно в отношении электронных средств платежа».

В связи с данными изменениями в научных кругах возникла дискуссия о том, так ли необходимо было признавать хищение с банковского счета или в отношении электронных средств платежа тяжким преступлением, еще и вне зависимости от суммы похищенного. Законодатель такую необходимость обосновывал ростом количества совершаемых хищений данного вида. Однако многие ученые с такой позицией не согласились, так как, по их мнению, рост количества преступлений и особая (электронная) форма денежных средств не могут явно свидетельствовать о повышении степени общественной

[1] Шарапов Р. Д. Актуальные вопросы квалификации новых видов мошенничества // Проблемы квалификации и расследования преступлений, подследственных органам дознания : материалы Всероссийской научно-практической конференции / Тюменский институт повышения квалификации сотрудников МВД России. Тюмень, 2013. С. 4.

опасности и изменении ее характера, следовательно, отнесение таких преступлений к категории тяжких нарушает принцип справедливости[1].

С приведенным мнением следует не согласиться, поскольку согласно Постановлению Пленума Верховного Суда Российской Федерации от 22.12.2015 № 58 (ред. от 18.12.2018) «О практике назначения судами Российской Федерации уголовного наказания» степень общественной опасности определяется судами исходя из конкретных обстоятельств дела и характера наступивших последствий, а также некоторых других условий, а характер общественной опасности определяется судами исходя из направленности преступного посягательства, то есть его объекта, и причиненного вреда.

Кроме того, объект преступления кроме общественных отношений, на которые направлено посягательство, включает в себя также и предмет посягательства, которым в данном случае являются безналичные денежные средства, то есть, основываясь на разъяснении постановления Пленума, можно говорить о том, что предмет также влияет на характер общественной опасности. Следовательно, законодатель путем конкретизации предмета компьютерного мошенничества указывает на возросшую значимость безналичных денежных средств как предмета преступления и необходимость повышения степени их уголовно-правовой защиты.

К тому же, степень общественной опасности определяется также исходя из объективной стороны преступления, которая в данном случае выражается в особом способе совершения хищения электронных денежных средств, который отличается от хищения наличных денежных средств, поскольку при хранении средств, например, на банковском счете лицо предполагает, что принял достаточные меры для сохранения своего имущества и свободный доступ к ним ограничен. Так, при хищении безналичных средств свободно их получить невозможно: можно украсть телефон или банковскую карту, однако

[1] Архипов А. В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 6—7.

это не означает получения свободного доступа к безналичным денежным средствам.

Стоит также отметить, что Постановлением Пленума Верховного Суда Российской Федерации от 22.12.2015 № 58 (ред. от 18.12.2018) «О практике назначения судами Российской Федерации уголовного наказания» аналогичный квалифицирующий признак был введен в ст. 158 УК РФ, следовательно, имеет место рассмотрение разграничения составов преступлений по п. «г» ч. 3 ст. 158 и ст. 159.6 УК РФ[1].

Данный вид кражи и «компьютерное» мошенничество являются формами хищения и как следствие имеют единый объект преступления и субъективную сторону, выраженную прямым умыслом и корыстной целью.

Различие прослеживается в способе совершения хищения: при краже используется тайное хищение, а при мошенничестве – обман и злоупотребление доверием лица. Однако по смыслу такого способа хищения обман может быть совершен только при непосредственном контакте двух людей[2], что делает такой способ мошенничества почти не применимым к ст. 159.6 УК РФ.

На современном этапе развития интересным фактом является то, что с момента введения в действие ст. 159.6 УК РФ, исходя из анализа судебной практики, совершение «компьютерного» мошенничества всегда совершается либо в отношении электронных денежных средств, либо с банковского счета, следовательно, такие виды хищения являются основными.

Таким образом, подводя итог, можно говорить о том, что характер и степень общественной опасности мошенничества с безналичными денежными средствами выше общественной опасности хищений наличных денежных средств, следовательно, ужесточение уголовной ответственности законодателем представляется обоснованным. Однако предпринятые в данном направлении действия являются недостаточно эффективными и требуют дальнейшего совершенствования, в том числе и для унификации судебной практики.

---

[1] Иванова Л. В. Хищение с использованием информационных технологий: проблемы квалификации // Юридическая наука и правоохранительная практика. 2020. №1 (51). С. 30.

[2] Шестало С. С. Новое в уголовном законодательстве о хищении безналичных денежных средств // Юрист. 2018. № 8. С. 41.

Так, по мнению некоторых ученых, в виду схожести положений п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ их следует исключить из УК РФ и ввести новый состав преступления «Хищение с использованием информационных технологий»[1]. При этом, существуют недостатки и в предлагаемой учеными редакции такой статьи, поскольку она почти полностью повторяет положения ст. 159.6 УК РФ, что может повлиять на ограничение распространения положений такой статьи на иные формы хищения.

Другие ученые, например М. Д. Фролов, предлагают внести изменения в ст. 159.6 УК РФ и сформулировать ее как «Хищение, совершенное с использованием информационно-телекоммуникационных технологий», под которым понимается хищение чужого имущества или приобретение права на чужое имущество, совершенное посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[2].

Однако в данном случае очевидной становится подмена понятийного аппарата, поскольку автор смешивает такие понятия как информационно-телекоммуникационная сеть и информационные технологии, чего не допускает современное законодательство.

В связи с вышеуказанным, возможным и логичным путем совершенствования уголовно-правовой нормы о «компьютерном» мошенничестве является объединение положений п. «г» ч. 3 ст. 158, ст. 159.3 и ст. 159.6 УК РФ в одну статью, при условии, что она дословно не будет повторять диспозицию ст. 159.6 УК РФ, а будет являться именно консолидацией положений, указанных выше статей. Такой подход позволит исключить ошибки правоприменения и унифицировать судебную практику.

---

[1] Иногамова-Хегай Л. В. Квалификация преступлений против личности и «компьютерных» преступлений по правилам совокупности преступлений и конкуренции уголовно-правовых норм // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 5 (55). С. 9.

[2] Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : автореф. дис. ... канд. юрид. наук. М., 2019. С. 15—17.

УДК 343

Ю. С. БЕЗУГЛОВА[1]

ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Двадцать первый век считается веком высоких технологий. Многие из этих технологий применяются для обработки, передачи и хранения информации. Компьютерная информация сегодня является одним из предметов преступного посягательства наряду с традиционными материальными и нематериальными благами. Поэтому ответственные органы все больше внимания уделяют задаче уголовно-правовой защиты информации, действия с которой осуществляются посредством компьютерных систем. Однако решение обозначенной задачи невозможно без установления особенностей данной группы преступлений.

Каждый год как в странах зарубежья, так и в Российской Федерации количество совершаемых компьютерных преступлений увеличивается. Согласно сведениям МВД РФ в январе—сентябре 2023 года 489 тыс. преступлений были зарегистрированы как совершенные с использованием информационных технологий или в сфере компьютерной информации, что на 29,2 % больше по сравнению с 2022 года[2].

Приведенные статистические данные не позволяют в полной мере судить об уровне глобальности проблемы, поскольку преступления в сфере компьютерной информации обладают высокой латентностью, то есть многие из них остаются неизвестными для ведомств и как следствие не учитываются в отчетах. Это происходит потому, что рассматриваемая группа преступлений сложно раскрывается. Кроме того, имеет место быть сложность сбора улик в случае, если преступление совершил профессионал.

---

[1] Научный руководитель — БЕРЕСТОВОЙ Андрей Николаевич, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

[2] Сборник о состоянии преступности в России за январь—сентябрь 2023 г. // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/42989123/ (дата обращения: 10.10.2023).

Обеспечение состояния защищенности, неуязвимости компьютерной информации имеет большое значение как для государства в целом, так и для отдельного субъекта в частности. Эффективная работа по недопущению совершения любых преступлений (в том числе рассматриваемых в статье) возможна только при наличии соответствующих уголовно-правовых норм.

В статье под преступлениями в сфере компьютерной информации понимаются предусмотренные уголовным законом общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности производства, хранения, использования либо распространения информации или информационных ресурсов. В основу определения положена информация.

Любая информация, попадающая в память компьютера, становится данными, которые некоторые исследователи называют компьютерной информацией. Такая информация представлена в виде электрических сигналов. Человек воспринимает ее с помощью аппаратного и программного обеспечения. Согласно УК РФ средства, при помощи которых можно совершать основные действия с информацией (информационные процессы), могут быть разными.

Акты поведения человека, расцениваемые как преступления в сфере компьютерной информации, приводятся в главе 28 УК РФ. Нарушение доступа к компьютерной информации, создание, использование и распространение вредоносных программ, нарушение правил использования компьютерной информации, нарушение правил управления техническими средствами для обеспечения безопасности и стабильности функционирования сети «Интернет» и общедоступных сетей связи, неправомерное воздействие на критическую информационную инфраструктуру государства — деяния, запрещенные в Российской Федерации.

Создание вредоносных программ (ст. 273 УК РФ) является актуальной проблемой современности, которая берет свои корни еще в двадцатом веке. Преступное деяние направлено на разработку и использование программного

обеспечения, которое нейтрализует средства компьютерной защиты или модифицирует, блокирует, копирует или уничтожает без возможности восстановления данные.

В существующей судебной практике достаточно примеров привлечения к ответственности лиц, совершивших преступления, относящиеся к ст. 273 УК РФ. Примером являются деяния В.А. Он использовал компьютерные программы, нейтрализующие средства защиты компьютерной информации. Впоследствии признан виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, Октябрьским районным судом г. Красноярская[1].

Следующим общественно опасным деянием, которое относится к разряду преступлений в сфере компьютерной информации, является нарушение правил хранения компьютерной информации (ст. 274 УК РФ). Объективная сторона описываемого преступного деяния заключается в нанесении ущерба пользователю путем уничтожения, блокировки или изменения компьютерной информации, которая охраняется законом. Компетентные органы, разработчики программного обеспечения, собственники или законные пользователи программы устанавливают правила хранения информации, нарушение которых влечет уголовную ответственность, которая закреплена в ст. 274 УК РФ.

Воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1. УК РФ). Уголовная ответственность наступает за неправомерный доступ к информационным системам, сетям, автоматизированным системам управления, функционирующим в таких сферах, как энергетика, здравоохранение, оборонная промышленность и т. д. Данная статья введена в УК Федеральным законом от 26.07.2017 № 194-ФЗ. Преступление включает в себя различные формы преступных действий, таких как незакон-

[1] Приговор Октябрьского районного суда г. Красноярска от 16 октября 2017 г. по делу № 1-423/2017 // Sud-Praktika.ru : сайт. URL: https://sud-praktika.ru/precedent /456504.html (дата обращения: 10.11.2023).

ный доступ, создание вредоносных продуктов, уничтожение или блокирование критической информационной инфраструктуры в различных сферах общества[1]. За совершение любого из обозначенных в диспозиции статьи действий может быть назначено наказание до 10 лет лишения свободы.

В качестве примера можно привести приговор Первомайского районного суда г. Владивостока. В феврале 2018 года А.С., С.В. и М.А. вступили между собой в преступный сговор. Действия лиц были направлены на извлечение финансовой выгоды в результате неправомерного использования компьютерной информации различных организаций. А.С., С.В. и М.А. осуждены по ч. 4 ст. 274.1 УК РФ[2].

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Статья 272 УК РФ устанавливает уголовную ответственность за доступ к компьютерной информации лицами без согласия правообладателя. Объективная сторона преступления характеризуется доступом к информации лицами, не обладающими соответствующими правами, и последствиями в виде изменения или копирования информации.

Стоит отметить, что характерной особенностью рассматриваемой группы преступлений является ее субъект. В основном преступления в сфере компьютерной информации совершают лица, обладающие узкопрофильными знаниями, умениями и навыками – программисты, специалисты в области информационной безопасности, инженеры по обслуживанию технических систем безопасности, работники спецслужб. Указанный фактор существенно затрудняет расследование преступлений в связи с легкостью устранения улик и скрытия местоположения преступниками.

В результате проведенного исследования сделан вывод: преступления в сфере компьютерной информации сложны в обнаружении и расследовании,

---

[1] Рафиков И. Н., Алышев Ю. В. Преступления в сфере компьютерной информации // EScio. 2020. № 23. С. 1—6.

[2] Приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-376/2019. // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 10.11.2023).

что является отличной почвой для многократного увеличения количества совершаемых противоправных деяний.

Сегодня в Российской Федерации отсутствует достаточный объем следственной практики по расследованию преступлений в сфере компьютерной информации. Видится необходимым увеличение количества квалифицированных кадров, обладающих знаниями как в области юридических наук, так и в области компьютерных технологий.

В юридическом сообществе ведутся дискуссии об отнесении к разряду компьютерных преступлений всего массива преступных деяний, которые совершаются с использованием в каком-либо виде компьютерной техники, телекоммуникационных сетей или сети «Интернет». Технологический прогресс обуславливает появление новых форм преступных проявлений, в которых используется компьютерная техника. Необходимо обеспечить быстрое реагирование со стороны правоохранительной системы государства.

УДК 343

М. Ш. БИСУЛТАНОВА[1]

СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ» КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

Развитие технологий открывает широкие возможности для человечества, однако в современных реалиях наблюдается рост информационного обмена, который не обеспечивается достаточным уровнем защиты информации, что создает благоприятные возможности для совершения компьютерных преступлений.

В уголовном законе отсутствует определение термина «способ совершения преступления», однако в науке уголовного права в широком смысле под способом совершения преступления понимаются действия или система дей-

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

ствий, которые обладают важными свойствами, а именно — они должны совершаться в процессе преступления и быть направленными на достижение преступного результата.

Особенная часть УК РФ предусматривает такой признак объективной стороны, как использование информационно-телекоммуникационных сетей, включая сеть «Интернет». Так законодателем был урегулирован вопрос отнесения сети «Интернет» к способам совершения преступления, применяемых на всех его стадиях: приготовление, покушение, оконченное общественно опасное деяние.

Согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть — это «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники».

Сайт в сети «Интернет» представляет собой «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет». Страница сайта в сети «Интернет» — это «часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет».

В том случае, когда Интернет используется как средство для совершения действий второстепенного плана, можно говорить о совершении преступлений с использованием Интернета. А когда само преступное деяние совершается с помощью Интернета, следует говорить о собственно совершении преступления посредством Интернета».

Законодатель уделяет особое внимание публичности, упрощению совершения деяния, анонимности преступников, а также массовости, быстроте и глубине проникновения негативного информационного воздействия на общество.

В связи с этим уголовный закон относит совершение преступления с использованием сети «Интернет» не только к основным признакам состава преступления, но и к квалифицирующим, что значительно повышает степень общественной опасности содеянного и влечет усиление наказания виновного.

Так, в ряде статей Уголовного кодекса Российской Федерации содержится неоднократное упоминание квалифицирующего признака «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». В настоящее время Особенная часть УК РФ насчитывает 20 норм, содержащих использование данного признака.

УДК 343

В. В. БОРОВИКОВ,
Е. В. СТОЛЯРСКИЙ[1]

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ», КАК СПОСОБ СОВЕРШЕНИЯ РАЗВРАТНЫХ ДЕЙСТВИЙ

В мае-июне 2022 года компанией «Online Interviewer» по заказу «Лаборатории Касперского» среди родителей и их детей школьного и дошкольного возраста был проведен опрос на тему использования несовершеннолетними интернета. Так, в возрасте 7–10 лет у 88 % детей есть собственный смартфон с выходом в интернет.

При этом 68 % используют ресурсы глобальной сети для общения с друзьями в социальных сетях (в основном – «ВКонтакте»). Почти половина опрошенных в графе «личные данные» указывают свой реальный возраст, рассказывают о своих увлечениях, 27 % указывают номер своего образова-

[1] Научный руководитель — ФЕДЫШИНА Полина Викторовна, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации.

тельного учреждения, 13 % выкладывают фотографии, на которых видно обстановку квартиры, 12 % указывают имена родителей, 10 % делятся своим номером телефона[1].

Результаты исследования позволяют сделать тревожный, но однозначный вывод: дети оставляют достаточный «цифровой след» в сети, позволяющий даже без установления контакта с ними выяснить многие подробности их личной жизни. В силу весьма юного возраста данная категория населения не может полностью осознавать опасность публикации своих персональных данных в общий доступ. Данный вывод усугубляется тем, что треть родителей не знают, какую информацию о себе публикуют их дети.

Все вышеперечисленные факторы являются основой формирования плодородной почвы для распространения такого опасного явления, как «онлайн-груминг» или «кибер-груминг».

Костромской областной институт развития образования определяет онлайн-груминг как криминальную онлайн-активность по установлению дружеских отношений и эмоциональной связи с ребенком или подростком для завоевания его доверия с целью сексуальной эксплуатации[2]. Такие действия, предпринимаемые «грумерами», как разговоры на циничные темы, просьбы прислать фотографии или видеозаписи откровенного характера, предложения встретиться для вступления в половую связь и пр. образуют собой объективную сторону преступления, предусмотренного ст. 135 УК РФ.

Общественная опасность развратных действий в кибер-пространстве, обосновывается рядом факторов.

---

[1] «Взрослые и дети в интернете»: исследование «Лаборатории Касперского» / Альянс по защите детей в цифровой среде. URL: https://internetforkids.ru/projects/vzroslye-i-deti-v-internete-issledovanie-laboratorii-kasperskogo (дата обращения: 20.11.2023).

[2] Онлайн-груминг. Памятка для педагогических работников / О. В. Тайгин, И. В. Адоевцева // Серия памяток по профилактике деструктивного поведения несовершеннолетних / Костромской областной институт развития образования, Факультет воспитания и психологического сопровождения. 2020. URL: https://www.eduportal44.ru/koiro/RMIKPU/SPEZ/DocLib/11_Груминг.pdf (дата обращения: 20.11.2023).

Основным фактором, по нашему мнению, выступает анонимность лица, осуществляющего преступный умысел. Социальные сети позволяют взаимодействовать с лицами и при этом не раскрывать своих фактических данных. В таких условиях преступник с целью введения в заблуждение и установления контакта способен каждый раз подстраиваться под конкретного ребенка и «менять» свою внешность, возраст и даже пол. Стоит отметить, что в Российской Федерации осуществляются меры по деанонимизации пользователей в социальных сетях.

Так, например, для установки более надежной защиты своей страницы пользователь может связать свой аккаунт в «ВКонтакте» с аккаунтом в «Госуслугах», а для регистрации необходимо в обязательном порядке указать свой номер телефона. К сожалению, этих мер недостаточно, поскольку у пользователей существует возможность регистрировать несколько аккаунтов без обязательной привязки к «Госуслугам».

Кроме того, общественная опасность данного преступления обуславливается оказанием негативного воздействия на ребенка. Причем это воздействие может выражаться как в психическом вреде: разговоры на циничные темы сексуального характера, обмен фото и видеоматериалами эротического и порнографического характера, демонстрация половых органов; так и в физическом, когда преступник договаривается с несовершеннолетним лицом о встрече и «сексуальное знакомство» перерастает в сексуальный контакт.

Не стоит забывать и о высоком уровне латентности данного преступления. Так, согласно данным вышеупомянутого исследования об активности несовершеннолетних в сети «Интернет», треть родителей не знают, какая информация об их ребенке находится в открытом доступе в социальных сетях и с кем общаются там их дети. Зачастую злоумышленники с целью сокрытия преступления используют шантаж, который особенно эффективно действует по отношению к еще не созревшему детскому сознанию. Ребенок попросту боится, что родители или друзья узнают о том, что он отправлял определенные фотографии незнакомому взрослому человеку.

Так, диспозиция ст. 135 УК РФ предусматривает наказание за совершение развратных действий без применения насилия лицом, достигшим восемнадцатилетнего возраста в отношении лица, не достигшего шестнадцатилетнего возраста. Постановление Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности» в п. 17 выделяет так называемые «интеллектуальные» развратные действия — при которых отсутствует какой-либо физический контакт, в том числе совершенные с использованием сети «Интернет» и иных информационно-телекоммуникационных сетей.

Способ совершения преступления — это внешняя форма, в которой выражаются преступные действия, т. е. конкретные приемы и методы, применяемые в процессе преступного посягательства. В рассматриваемом составе способ совершения преступления включает в себя использование информационно-телекоммуникационных сетей (включая сеть «Интернет). Развитие социальных сетей выступило подспорьем для совершения указанного деяния в сети. Указанный фактор обуславливает особое внимание законодателя относительно роли использования информационно-телекоммуникационных сетей (включая сеть «Интернет) как зачастую особо квалифицированного способа совершения преступления.

Ненасильственный характер преступления является ключевым фактором для разграничения развратных действий с насильственными действиями сексуального характера, предусмотренными ст. 132 УК РФ. Другим критерием является возраст потерпевшего, определенный как в диспозиции статей главы 31 УК РФ, так и в Постановлении Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности», конкретизированный также примечанием к ст. 131 УК РФ. Совершение развратных действий в отношении малолетнего лица (т.е. не достигшего 12-летнего

возраста) без вступления с ним в сексуальный контакт, требует квалификации по п. «б» ч. 4 ст. 132 УК РФ.

Так, Московским городским судом М. был осужден за совершение преступления, предусмотренного п. «б» ч. 4 ст. 132 УК РФ. Установлено, что 21-летний М. познакомился с 10-летней жительницей г. Казани, вступил с ней в интернет-переписку, после чего направлял ей материалы порнографического характера с целью побудить ее к сексуальным действиям путем психологического воздействия[1].

Данный приговор стал одним из первых в России в отношении развратных действий в сети «Интернет» и положил начало правоприменительной практике квалификации деяний интернет-грумеров. Ранее перспектива уголовных дел по таким преступлениям была сомнительна, поскольку правоохранительными органами под действиями сексуального характера понималось нечто реальное, нежели виртуальное. Меньше, чем через год позиция относительно «интеллектуальных» развратных действий была закреплена в Постановлении Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности».

Несмотря на наличие разъяснений Постановления Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности», в правоприменении возникают вопросы, требующее пристального внимания.

Согласно разъяснениям Постановления Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы лично-

[1] В России впервые осудили за непристойное поведение в интернете / Российская газета. 2014. 19 февр. URL: https://rg.ru/2014/02/19/internet-site.html (дата обращения: 20.11.2023).

сти», квалификация преступлений, предусмотренных ст. 131–135 УК РФ возможна только тогда, когда виновный знал или допускал, что потерпевшим является лицо, не достигшее возраста, указанного в диспозициях соответствующих статей.

Таким образом если преступник выполнил объективную сторону развратных действий по отношению к 14-летней девушке, указавшей в своем профиле в социальной сети, например, 17-летний возраст, его действия не могут быть квалифицированы по ст. 135 УК РФ? Данный вопрос находит свою актуальность в том, что несовершеннолетние зачастую пытаются либо выглядеть в глазах других старше своего возраста, либо определенными действиями стараются соответствовать поведению взрослых. Сеть «Интернет» предоставляет отличные возможности для «преображения» таких детей.

Представляется, что все зависит от конкретных обстоятельств: сообщала ли девушка о своем настоящем возрасте в ходе переписки, делилась ли своими фотографиями, на которых отчетливо видно, что она не достигла 16-летнего возраста, выходила на контакт с лицом путем использования видеосвязи. Если в ходе предварительного следствия будет установлено, что лицо не знало и не могло предполагать о реальном возрасте своего собеседника, такое лицо не может подлежать уголовной ответственности за совершение развратных действий.

В дополнение к вышеуказанному примеру стоит отметить, что применение совершеннолетним лицом в ходе переписки шантажа, угроз, психологического давления, иных методов воздействия, свидетельствующих о насильственном характере деяния, целью которого является удовлетворение сексуальных потребностей преступника и возбуждение у потерпевшего сексуального интереса, по смыслу закона, может быть квалифицировано по п. «б» ч. 4 ст. 132 УК РФ.

Так, К. был осужден за совершение преступления, предусмотренного ч. 1 ст. 135 УК РФ. Установлено, что К., являясь лицом, достигшим 18-летнего воз-

раста, осуществил ряд телефонных звонков 15-летней Л., в ходе которых предлагал встретиться для вступления в сексуальную связь, а также высказал иные слова и выражения, направленные на вызывание у Л. интереса к сексуальным отношениям. Кроме того, в ходе телефонных разговоров Л. неоднократно сообщала К. о своем 15-летнем возрасте.

Квалификация деяния К. по ч. 1 ст. 135 УК РФ представляется нам обоснованной, поскольку К. не оказывал на Л. давления, не пытался угрожать, т.е. не проявлял психологического насилия.

Кроме того, как в научной, так и в практической среде, зачастую возникает вопрос о разграничении ст. 135 УК РФ и п. «б» ч. 3 ст. 242 УК РФ, предусматривающей ответственность за распространение, публичную демонстрацию или рекламирование порнографических материалов среди несовершеннолетних с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет).

Оба состава являются формальными: для выполнения объективной стороны не обязательно возникновение сексуального интереса или ознакомления с порнографическими материалами. Оба преступления характеризуются прямым умыслом, а также в ряде случаев тождественным способом его совершения (с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет).

Объектом преступления, предусмотренного ст. 135 УК РФ выступает нормальное половое и нравственное развитие и половая неприкосновенность личности, в то время, когда объектом ст. 242 УК РФ является общественная нравственность.

В данном контексте интересно исследование Сучковой В.В., определившей общественную нравственность как сложную систему норм и ценностей, определяющих модель поведения человека в обществе, одним из элементов

которой является общественная нравственность в сфере сексуальных отношений (половая мораль)[1]. Полагаем, что объект ст. 242 УК РФ является более широким по отношению к объекту ст. 135 УК РФ, поскольку нормальное половое развитие включено в систему норм и ценностей в сфере сексуальных отношений.

Однако, говоря о субъективной стороне преступления, предусмотренного ч. 2 ст. 242 УК РФ стоит устанавливать и цель такого деяния. Известно, субъективная сторона обладает как обязательным элементом – виной, так и факультативными элементами – мотивом и целью. Осуждая лицо по ч. 2 ст. 242 УК РФ правоприменитель устанавливает, знало или догадывалось ли лицо о возрасте «получателя, очевидца» демонстрации порнографических материалов. Если лицо объективно полагало, что лица, которым он демонстрирует порнографический материал совершеннолетние, то в таком случае нельзя говорить об уголовной ответственности по ч. 2 ст. 242 УК РФ. Из этого следует, что по ч. 2 ст 242 УК РФ, обязательным элементом субъективной стороны выступает не только вина, но и цель (в данном случае целью является распространение, демонстрация порнографических материалов среди несовершеннолетних).

По нашему мнению, ключевым фактором разграничения будет выступать направленность умысла лица. При совершении развратных действий лицо преследует цель удовлетворения собственного сексуального влечения, или на вызывание сексуального возбуждения у потерпевшего лица (п. 17 Постановления Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности»).

[1] Сучкова В.В. Общественная нравственность в сфере половых отношений как объект уголовно-правовой охраны : дис. ... канд. юрид. наук. М., 2004. С. 7.

При выполнении объективной стороны преступления, предусмотренного ст. 242, лицо преследует цели непосредственного распространения, публичной демонстрации или рекламирования порнографических материалов, в том числе с получением дохода.

В научной литературе предлагается дополнить ч. 3 ст. 135 УК РФ квалифицирующим признаком «с использованием информационно-коммуникационной сети (включая сеть «Интернет»)»[1].

Соответствующий законопроект даже был внесен в Государственную Думу 24.06.2015 г. Данная мера представляется авторам избыточной, поскольку уголовная ответственность за «интеллектуальные» развратные действия конкретизируется в п. 17 Постановления Пленума Верховного Суда Российской Федерации от 04.12.2014 № 16 «О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности». Кроме того, в таком случае нарушается принцип справедливости, предусмотренный ст. 6 УК РФ, поскольку по смыслу закона, объективная сторона развратных действий в сети «Интернет» предусмотрена ч. 1 ст. 135 УК РФ, предусматривающей более мягкую санкцию, нежели ч. 3 указанной статьи. Так, на основании заключения Правового управления Государственной Думы вышеуказанный законопроект был отклонен[2].

Таким образом, развратные действия, совершенные с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет), получили мощный толчок к распространению в связи с активным развитием социальных сетей и роста количества их несовершеннолетних пользователей.

---

[1] Амирова Д. К., Гильмутдинов Д. Д. Уголовная ответственность за развратные действия, совершенные в отношении несовершеннолетних с использованием информационно-коммуникационной сети «Интернет» // Ученые записки Казанского юридического института МВД России. 2021. Т. 6, № 2 (12). С. 124.

[2] О внесении изменений в статьи 135 и 242.1 Уголовного кодекса Российской Федерации в целях уточнения норм об уголовной ответственности за преступления сексуального характера в отношении несовершеннолетних, совершенные с использованием информационно-телекоммуникационных сетей : Законопроект от 24 июня 2015 г. № 822714-6. URL: https://sozd.duma.gov.ru/bill/822714-6 (дата обращения: 20.11.2023).

Общественная опасность данного преступления обуславливается множеством факторов, свидетельствующих о необходимости активной профилактической работы правоприменителя, а также проведению качественной работы по выявлению и расследованию развратных действий в сети «Интернет».

Рассматриваемый способ совершения преступления обладает рядом особенностей, которые необходимо учитывать при квалификации. Такими особенностями выступают осведомленность преступника о возрасте потерпевшего, направленность умысла, характер его действий.

УДК 343

М. В. ВАЖЕНИНА[1]

КИБЕРПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ВИДЫ, ОСОБЕННОСТИ КВАЛИФИКАЦИИ

Современное общество постоянно развивается, но вместе с ним развивается и преступная среда, а значит, появляются новые виды, формы преступлений и способы их совершения. Одним из таких видов являются киберпреступность.

Киберпреступность является относительно новой, но очень опасной и быстро развивающейся разновидностью преступлений. Как отметил председатель судебного состава коллегии по уголовным делам Верховного Суда Российской Федерации Геннадий Иванов: «с каждым годом количество осужденных за преступления в сфере компьютерной информации стабильно растет — в 2019 году таких было 165 человек, в 2021 — 225 человек. Число осужденных за преступления, где использование Интернета вменяется как признак, заметно превышает количество преступлений в сфере компьютерной информации. В 2019 году осужден 6 041 человек, в 2021 — 6 726 человек»[2].

[1] Научный руководитель — АЛЕШИНА-АЛЕКСЕЕВА Екатерина Николаевна, старший преподаватель кафедры уголовного права Санкт-Петербургского университета МВД России.

[2] Верховный суд научит рассматривать дела о киберпреступлениях // Парламентская газета. 2022. 8 нояб. URL: https://www.pnp.ru/social/verkhovnyysud-nauchit-rassmatrivat-dela-o-kiberprestupleniyakh.html (дата обращения: 11.11.2022).

Киберпреступность охватывает большой спектр общественно-опасных деяний, которые могут причинить вред как отельной личности, так и национальной безопасности страны в целом. Поэтому особенности квалификации данного вида преступлений остаются главной проблемой в борьбе с преступностью в сфере защиты компьютерной информации.

На современном этапе развития уголовного законодательства нет четкого определения киберпреступности. Ученые по-разному трактуют понятие «киберпреступления»[1]. Так, по мнению большинства правоведов, «киберпреступность — это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов»[2].

К основным видам киберпреступлений можно отнести:

— Финансово-ориентированные киберпеступления. Это такие преступления, главной целью которых является получение коммерческой выгоды. Это, прежде всего, кибервымогательство, кибермошенничество и фишинг;

— Киберпреступления, связанные с вторжением в личную жизнь. Это, прежде всего, такие преступления, как шпионаж и кража персональных данных;

— Нарушение авторских прав. Данные преступления в первую очередь связаны с распространением музыки, фильмов сериалов и др.;

— Спам;

---

[1] Хусяинов Т. М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования : материалы Всероссийского круглого стола, Иркутск, 20 марта 2015 года. Иркутск, 2015. С. 120–125; Цимбал В. Н., Клюев С. Г. Понятие киберпреступления и его содержательная часть // Вестник Московского университета МВД России. 2021. № 1. С. 129–132 ; Антонов А. Г., Алешина-Алексеева Е. Н., Соколова А. В. К вопросу о понятии и видах киберпреступлений // Вестник Пермского института ФСИН России. 2023. № 1 (48). С. 5–10.

[2] Что такое защита от преступности? // Kaspersky : сайт. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 18.11.2023).

— Социально и политически мотивированные киберпреступления и др.

Условно, к преступлениям в сфере компьютерной информации можно отнести широкий круг преступлений, направленных на различные правоохраняемые отношения, ценности, права и свободы в сфере компьютерной безопасности, защиты персональных данных и других сфер интернет-безопасности.

Стоит отметить, что объектами преступлений данной области являются общественные отношения в сфере защиты жизни, здоровья, нравственного и физического развития несовершеннолетних, а также собственность, причем как материальная, так и интеллектуальная, защиты конституционного строя и государственной безопасности и др.

Особенностью преступлений в сфере компьютерной безопасности является то, что информация и информационно-телекоммуникационные технологии могут выступать как предметом преступления, так и орудием и средством совершения общественно опасного деяния[1].

Так, киберпреступления совершаются в виртуальном пространстве, что позволяет преступнику находиться в любой части мира, а значит, создает сложности в поиске преступника[2]. Также создание таких программ, как VPN, wh.exe, которые позволяют преступнику не оставлять следы, поиск преступника делает невозможным.

Законодатель на данном этапе развития уголовного закона выделяет киберпреступность в отдельный вид преступлений и определяет некоторые способы совершения этих преступлений, но совершенствование этих способов позволяет уйти преступникам от ответственности.

---

[1] Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. №1. URL: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-klassifikatsiya-mezhdunarodnoe-protivodeystvie (дата обращения: 19.11.2023).

[2] Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416-425.

Таким образом, Российское законодательство нуждается в усовершенствовании уголовного закона в области компьютерной и цифровой информации. Широкий круг объектов преступлений, совершаемых в данной сфере, создает определенные сложности при квалификации. Именно поэтому первым этапом может стать включение в обстоятельства, отягчающие наказание (63 статью УК РФ) совершение преступления с использованием информационно-телекоммуникационных средств. Также необходимо проводить мониторинг криминологической среды, целью которого является выявление новых видов преступлений и способов совершения.

УДК 343

Э. Г. ГАБИБОВА,
Е. В. КОЛОШИНА[1]

ПРОБЛЕМЫ КВАЛИФИКАЦИИ РАЗВРАТНЫХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

На современном этапе развития общества сеть «Интернет» стала незаменимым элементом обучения, работы и коммуникации. Человек уже не представляет свою повседневную жизнь без его использования. Но наряду с инновационным развитием появляется преступная деятельность, которая совершается с использованием компьютеров, систем и компьютерных сетей и Интернета.

Дестабилизирующее воздействие преступной деятельности наиболее «остро» отражается на уязвимых слоях населения, к числу которых относятся и несовершеннолетние. Вызывает опасение наметившаяся тенденция увеличения числа преступлений в отношении несовершеннолетних - число детей и подростков, пострадавших от преступлений, за последние три года увеличилось почти на 20 тыс. — с 94,8 тыс. в 2020 году до 113,3 тыс. в 2022-м.

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

Особого внимания требует факт увеличения доли половых преступлений, совершенных с использованием сети «Интернет». По данным СК России, за девять месяцев 2022 года свыше 900 преступлений сексуального характера в отношении несовершеннолетних было совершено с использованием информационно-телекоммуникационных технологий.

Половым преступлением, совершение которого не всегда связано с нарушением физической неприкосновенности, являются развратные действия (ст. 135 УК РФ). Статья 135 существенно изменена в результате внесения изменений в УК РФ Федеральным законом от 27.07.2009 № 215-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». Но даже несмотря на длительный период существования, на практике возникает много вопросов относительно данной статьи.

Во-первых, остается нерешенным вопрос о толковании термина «развратные действия» — сущность таких действий не раскрывается в уголовном законе, а также на уровне актов официального судебного толкования. Осложняет ситуацию отсутствие в диспозиции ст. 134 УК РФ указания на «иные действия сексуального характера».

Упоминание о развратных действиях встречается в приказе Минздравсоцразвития Российской Федерации «Об утверждении Порядка организации и производства судебно-медицинских экспертиз в государственных судебно-экспертных учреждениях Российской Федерации».

Обозначенный Порядок организации и производства судебно-медицинских экспертиз в государственных судебно-экспертных учреждениях Российской Федерации содержит в себе указание об установлении признаков развратных действий. Согласно положениям данного нормативно-правового акта, при развратных действиях могут совершаться различные противоестественные сексуальные манипуляции, поэтому в задачу эксперта входит установление возникающих при этом объективных признаков.

Затруднительным является установление перечня деяний, входящих в круг так называемых интеллектуальных развратных действий, т.е. совершаемых путем определенных поступков, выражающихся в разговорах на сексуальные темы, демонстрации различного рода порнографических изображений и материалов.

По мнению Оберемченко А.Д., имеются основания полагать, что такие развратные действия зачастую остаются без соответствующей реакции в форме уголовного преследования ввиду относительно невысокого уровня общественной опасности. Данная точка зрения нам не представляется убедительной, особенно с учетом возможности использования информационно-телекоммуникационных сетей, позволяющих преступнику действовать анонимно, коммуницируя сразу с большим количеством лиц, не достигших совершеннолетия. Кроме того, интеллектуальные развратные действия могут носить трансграничный характер, а также обеспечивают высокую латентность совершаемых преступных деяний.

Вторым аспектом, касающимся ответственности за совершение интеллектуальных развратных действий, является зафиксированное в примечании к ст. 131 УК РФ правило об отнесении к преступлениям, предусмотренным п. «б» ч. 4 ст. 131 УК РФ, а также п. «б» ч. 4 ст. 132 УК РФ деяний, подпадающих под признаки преступлений, предусмотренных ч. 3–5 ст. 134 УК РФ и ч. 2–4 ст. 135 УК РФ, если они совершены в отношении лица, не достигшего 12-летнего возраста.

Часть авторов высказываются о невозможности квалификации интеллектуальных развратных действий по п. «б» ч. 4 ст. 132 УК РФ. Уравнивание таких развратных действий к преступлениям, предусмотренным п. «б» ч. 4 ст. 131 и п. «б» ч. 4 ст. 132 УК РФ, представляется некорректным, поскольку указанные деяния обладают несовпадающими объективными характеристиками и различной общественной опасностью. Ответственность за такого рода деяния, по их мнению, следует предусмотреть в квалифицированном составе статьи 135 УК РФ.

Другие авторы стоят на позиции, что состав преступления, предусмотренного ст. 135 УК РФ, должен охватывать исключительно развратные действия интеллектуального характера, а включение данной нормы в сферу действия примечания к ст. 131 УК РФ является излишним.

Законодательного урегулирования требует ситуация, складывающаяся в связи с отнесением к преступлениям против половой неприкосновенности несовершеннолетних, не достигших четырнадцатилетнего возраста, развратных действий (в том числе интеллектуальных) - исходя из содержания ст. 73 УК РФ следует, что условное осуждение за такие деяния не назначается. Такой запрет представляется некорректным, поскольку характер совершенного деяния и характер уголовно-правовых последствий не является соразмерным.

Ряд авторов считают целесообразным дополнить ст. 135 УК РФ квалифицирующим признаком, предусматривающим ответственность за совершение развратных действий с использованием компьютерных систем или телекоммуникационных сетей.

Представляется, что в условиях динамичного развития сети «Интернет», сопутствующей инфраструктуры, обеспечивающей доступ практически к любому ресурсу детям любого возраста, такое нововведение отвечает запросам защиты половой свободы и неприкосновенности несовершеннолетних.

Проблемы применения ст. 135 УК РФ возникают при конкуренции со ст. 242 УК РФ. Всегда ли при совершении развратных действий в форме демонстрации потерпевшему (или нескольким потерпевшим) порнографической продукции будет иметь место идеальная совокупность с ч. 2 ст. 242 УК РФ в форме распространения порнографических материалов и предметов или их публичной демонстрации?

Объекты составов преступлений, ответственность за которые предусмотрена ст. 135, 242 УК РФ, различны. Потерпевший является обязательным признаком и того, и другого составов, однако, для ст. 135 УК РФ потерпевшим является лицо, не достигшее шестнадцатилетнего возраста, а для ч. 2 ст. 242 УК РФ потерпевшим является несовершеннолетний. Соответственно,

не во всех случаях вменения ч. 2 от. 242 УК РФ будет идти речь о вменении развратных действий.

Под распространением порнографических материалов и предметов понимают «в нарушение установленных правил или без соответствующего разрешения доведение до сведения других лиц материалов и предметов порнографического характера».

Но, если потерпевший не достиг шестнадцатилетнего возраста, то будет ли идеальная совокупность рассматриваемых составов в случае, когда, скажем, совершеннолетний продает такому потерпевшему порнографический материал? А если это происходит посредством интернета, когда виновный даже не видит потерпевшего? Тем более, что признак заведомости недостижения потерпевшим возраста согласия из диспозиций ст.ст. 134, 135 УК РФ исключен.

В приведенных примерах отсутствует направленность действий виновного на удовлетворение собственных половых потребностей и (или) сексуальное возбуждение и (или) удовлетворение половых потребностей потерпевшего. По крайней мере, последняя цель безразлична для виновного. Ст. 135 УК РФ не предусматривает в качестве обязательных признаков субъективной стороны состава ни целей, ни мотивов. Вменение совершения развратных действий в приведенных примерах было бы абсурдным, однако, исходя из буквального понимания рассматриваемых норм уголовного закона, такая ситуация возможна.

Представляется, что половая неприкосновенность может рассматриваться как факультативный объект преступления, предусмотренного ч. 2 ст. 242 УК РФ. С учетом того, что по общему правилу лица, достигшие шестнадцатилетнего возраста, не обладают половой неприкосновенностью, состав ч. 2 ст. 242 УК РФ в отношении несовершеннолетнего, достигшего шестнадцати лет, вполне можно рассматривать, как преступление, посягающее только на общественную нравственность.

Основываясь на вышеизложенных фактах, представляется возможным сделать вывод о необходимости законодательного усовершенствования ст. 135 УК РФ. Так, необходимо раскрыть сущность развратных действий; дополнить состав квалифицирующим признаком, указывающим на использование в ходе совершения преступления информационно-телекоммуникационных сетей; а также разрешить вопрос об исключении состава из сферы действия примечания к ст. 131 УК РФ.

УДК 343

А. Г. ГАДЖИЕВА[1]

ПАРТНЕРСТВО СБЕРБАНКА И УНИВЕРСИТЕТА МВД РОССИИ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Современное общество имеет высокий уровень информационного развития и проникновения технологий в повседневную жизнь. Важные тренды - цифровизация и виртуализация - оказывают значительное влияние на социальные изменения, имеющие как положительные, так и отрицательные последствия, включая новые риски и угрозы, с которыми правовое регулирование не всегда успевает справиться.

Важность исследуемой проблемы подчеркнул и Владимир Путин на встрече 4 октября 2023 в Сириусе со школьниками и студентами из разных стран, в ходе которого были обсуждены важные вопросы по формированию международных правовых систем по обеспечению кибербезопасности. Внимание на создание такой системы обратил один из участников форума из Индии, подчеркнув, что до сих пор нет сотрудничества между странами в области кибербезопасности. В свою очередь, Президент отметил, что Россия в

[1] Научный руководитель — РАМАЗАНОВА Пати Казихановна, заведующий кафедрой гуманитарных и социально-экономических дисциплин Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции, кандидат филологических наук, доцент.

2017 г. уже внесла в ООН предложения по созданию Конвенции о сотрудничестве в сфере противодействия информационной преступности.

Однако распространение технологий имело не только положительные последствия, но и негативные, такие как рост киберпреступности. Становиться киберпреступником выгодно. Сегодняшние грабители и мошенники не орудуют ножами и ломами, которые опасны и чреваты предсказуемыми последствиями, а используют щелчки мыши или телефонные звонки и методы социальной инженерии для кражи средств граждан. Этот вид преступлений более «привлекателен», чем обычные преступления: современные технологии позволяют совершать преступления, не выходя из дома, рассматриваемый нами киберпреступности.

МВД РФ опубликовало отчет о состоянии преступности в стране, где указывается на рост количества киберпреступлений в 2023 году и его распределение по регионам. Лидером по приросту преступлений в информационной среде стала Ингушетия, а в Чечне этот показатель упал более чем на 50 %. За период январь–май 2023 года министерство выявило 261 тысячу киберпреступлений, что на 27,5 % больше, чем за тот же период 2022 года. Основная часть преступлений совершается через интернет, а также киберпреступники стали чаще использовать мобильные средства связи. Случаи мошенничества с электронными средствами платежа при этом сократились на 32 %. На данный момент в России активно ведется борьба с киберпреступностью на всех уровнях: от административной и уголовной ответственности за утечки информации до принудительной блокировки счетов подозреваемых в мошенничестве[1].

Сбербанк, как крупнейшее кредитно-финансовое учреждение страны непосредственно ощутил изменения в векторе атак киберпреступников. Их целями являются клиенты, системы банковской автоматизации и самая разветвленная сеть банкоматов в России. Они стараются активно защищать вступив-

[1] Статистические данные 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/кет/12167987/ (дата обращения: 08.09.2018).

шие активы, включая клиентов и системы. Однако предупреждение, выявление, раскрытие и расследование преступлений, а также розыск преступников являются прерогативой правоохранительных органов. Согласно действующему законодательству, только они имеют право принимать меры по расследованию бизнеса, процедуры и следственные действия.

И для того, чтобы переломить ситуацию с расследованием киберпреступлений и помочь нашим правоохранительным органам успешнее бороться с киберпреступлениями в финансовой сфере, в июле 2016 года банк подписал соглашение о стратегическом партнерстве с Московским университетом МВД имени В.Я. Кикотя. Основная цель — объединить усилия представителей бизнеса, имеющих успешный опыт в обеспечении кибербезопасности, и государства в борьбе с киберпреступностью.

Первое, что необходимо было сделать, — оптимизировать парадигму обучения, которая должна учитывать особенности киберпреступлений и их расследования. Банк провел на своей территории цикл лекций по актуальным темам кибербезопасности. Слушателями были курсанты факультета информационной безопасности, Института подготовки сотрудников для органов предварительного расследования, действующие следователи, дознаватели и оперативники. В течение учебного года по выходным дням или вечерам пятницы сотрудники различных подразделений Службы кибербезопасности Сбербанка и приглашенные лекторы-практики рассматривали теорию защиты информационных ресурсов от различных атак, типовые схемы компьютерного мошенничества, особенности расследования киберпреступлений.

Осознавая это, банк помог Университету Министерства внутренних дел создать полигон и лабораторную базу, на которых можно закрепить полученные знания. Эти базы созданы в колледже подготовки специалистов в области информационной безопасности и Институте подготовки

сотрудников органов предварительного следствия.

Один из таких объектов — «Лаборатория информационной безопасности в экономической сфере» — предназначен для повышения практических навыков по защите систем, обрабатывающих финансовую информацию.

Лаборатория оснащена специализированным программным обеспечением для дистанционного банковского обслуживания и другим оборудованием. На практических занятиях курсанты приобретают навыки в обнаружении «цифровых следов» в системах дистанционного банковского обслуживания, знакомятся и работают с различным банковским оборудованием. Объектами исследования выступают в основном «виртуальные следы» и электронные носители информации.

Другой объект, предназначенный для подготовки будущих следователей, было создано в виде модели филиала Сбербанка Российской Федерации. Там установлены банкоматы, оборудование самообслуживания и персональные компьютеры. С помощью этого объекта учащиеся могут не только обнаружить, осмотреть и описать внешние повреждения терминала, полученные во время классической хакерской атаки, но и обнаружить, осмотреть и описать вредоносное программное обеспечение, инициированное злоумышленником.

Обучаемые получают навыки по снятию образа жесткого диска с банкомата и направлению его на компьютерную экспертизу без выведения банкомата из рабочего состояния и нарушения функционирования отделения финансово-кредитного учреждения. Курсанты отрабатывают проведение таких процессуальных действий, как обыск, изъятие и упаковка электронных носителей информации, выемка, осмотр предметов и документов. Кроме того, обучаемые знакомятся с системой видеонаблюдения банкоматов и отделений банка, получают навыки по обнаружению и изъятию имеющихся фото- и видеозаписей совершенных преступлений, получают изображения преступников[1].

[1] Калиниченко И. А. Начинаем с разборки «железа» // Полиция России. 2017. № 8. С. 18—21.

Для успешной борьбы с киберпреступниками необходимо постоянно отслеживать последние достижения технологий и прогнозировать потенциальные угрозы, которые они могут нести. Для этого необходимо постоянно поддерживать высокий уровень знаний сотрудников правоохранительных органов.

Для выполнения этого условия специалисты из различных подразделений Министерства внутренних дел должны систематически проходить переподготовку и повышение квалификации. Поэтому в 2017 и на сегодняшний день в учебном году при активной поддержке Сбербанка действующие операторы и следователи прошли переподготовку в новой лаборатории и полигоне Университета Министерства внутренних дел.

Цель состоит в подготовке квалифицированных специалистов для органов внутренних дел, которые противодействуют преступлениям, совершаемым финансовым сектором в области информационных технологий.

Сотрудники Службы кибербезопасности Сбербанка часто принимают участие в различных мероприятиях Университета МВД — круглых столах, конференциях по актуальным вопросам противодействия киберпреступлениям, а также участвуют в заседаниях научного общества курсантов и слушателей, членами которого являются наиболее активные представители различных факультетов.

Достижениями уже сейчас можно сказать, что проделанная работа принесла определенные результаты. Поэтому во второй половине прошлого года следователи, прошедшие переподготовку в Университете МВД, успешно расследовали уголовное дело в Москве по факту подделки платежных карточек для оплаты проезда в метро в рамках борьбы с преступлениями в сфере компьютерной информации, совершенными против собственности[1].

[1] Тарчоков Б. А. Тенденции развития киберпреступности в глобальном информационном пространстве // Проблемы экономики и юридической практики. 2021. Т. 17, № 1. С. 198—201.

Используя эмпирических данные, полученные от специалистов банка, курсанты пишут курсовые и дипломные работы, отмечаемые руководством МВД России. Так, в 2017 году в конкурсе на лучшую научно-исследовательскую работу студентов образовательных организаций системы МВД России победителем в номинации «Теория и практика противодействия преступности» была признана работа на тему «Деятельность следователя по расследованию хищений денежных средств из банкоматов и с их использованием», разработанная с использованием материалов лекций по кибербезопасности Сбербанка.

Помимо подготовки квалифицированных кадров, сотрудники банков и университетов Министерства внутренних дел обмениваются актуальной информацией о состоянии современной киберпреступности в режиме реального времени, совместно формулируют поправки к нормативно-правовым актам и рецензируют научные статьи.

Совместная деятельность Сбербанка и Университета Министерства внутренних дел Российской Федерации по борьбе с киберпреступностью будет продолжена. Однако для того, чтобы в полной мере бороться с киберпреступностью, все университеты Министерства внутренних дел должны участвовать в этом процессе. Достижения Сбербанка Российской Федерации, которые используются в сотрудничестве с Университетом Министерства внутренних дел в процессе обучения, могут быть переданы всем учебным заведениям, осуществляющим подготовку и переподготовку кадров правоохранительных органов. Было бы полезно создать больше полигонов и лабораторий для борьбы с киберпреступностью, по аналогии с киберпреступностью, созданной университетами с помощью банков. При необходимости банк готов оказать содействие в организации этих веб-сайтов.

Но и этого мало — те курсанты, которые учатся сейчас, приступят к расследованию киберпреступлений только через три—четыре года. В условиях растущей киберпреступности ждать так долго невозможно. Многие следователи, эксперты и оперативники регионального управления погрузились в тему

противодействия киберпреступлениям, в том числе мошенничествам, совершенным с использованием методов социальной инженерии. На рабочей встрече в центре противодействия мошенничеству Сбербанка сотрудники УМВД рассмотрели эффективные способы взаимодействия правоохранителей с банком, познакомились с актуальными схемами дистанционных мошенничеств, задали вопросы тем, кто находится на «первой линии» борьбы с банковскими мошенниками, ознакомились с высокотехнологичными решениями, которые использует Сбербанк для предотвращения зафиксированных попыток мошенничества.

Рабочие встречи получают положительные отзывы от коллег из Министерства внутренних дел разных городов и областей. Это подтверждается важностью распространения такой информации, поскольку это позволит значительно оптимизировать механизмы раскрытия и расследования многих финансовых и кредитных преступлений.

Сбербанк совместно с Университетом МВД продолжают работу по улучшению качества подготовки правоохранителей, чтобы снизить до минимума количество киберпреступлений. Руководство и сотрудники Сбербанка уверены, что участие в обучении и подготовке грамотных, вооруженных знаниями последних достижений науки и техники специалистов правоохранительных органов, — это основа успеха в борьбе с киберпреступностью и, как следствие, гарантия безопасности средств всех клиентов.

В целях защиты борьбы с киберпреступностью мы предлагаем применить следующие меры:

1. Необходимо повышать уровень государственного контроля. Так, Правительство России укрепляет государственный контроль в области кибербезопасности с помощью различных инструментов, таких как аудиты, лицензирование и сертификация, а также введение обязательных требований к защите информации для критической информационной инфраструктуры.

2. Развивать национальную систему образования и подготовки кадров в области кибербезопасности. Усиление требований к кибербезопасности приводит к возрастанию спроса на квалифицированных специалистов в этой сфере. В России необходимо развивать образовательные программы и научные исследования для подготовки высококлассных экспертов в области кибербезопасности.

Опираясь на подписанное соглашение и совместную работу Сбербанка и университета МВД, можно применять методики защиты от кибермошенников и рекомендации по совершенствованию системы минимизации кибер-рисков в банковской сфере, включающие следующие направления:

1. Повышение качества образования подготовки технических и юридических кадров.

Необходимо повысить привлекательность специальностей, связанных с информационными технологиями, выделять больше бюджетных мест по данным направлениям, а также увеличить часовую нагрузку по предметам, связанным с обучением информационным технологиям студентов всех специальностей. Это необходимо, так как киберпреступность развивается абсолютно во всех отраслях, поэтому экономисты, доктора, инженеры и др. также должны быть «подкованы» в основах IT, чтобы избежать кибератак, происходящих вследствие человеческих факторов.

Также важно уделить внимание подготовке сотрудников органов внутренних дел (ОВД). Необходимо разрабатывать новые темы, разделы, спецкурсы, посвященные расследованию преступлений в сфере информационных технологий, кибербезопасности и информационной безопасности.

2. Развитие механизма страхования кибер-рисков. Страхование от кибер-рисков как отдельный продукт – редкость для отечественного рынка. Например, программы страхования от кибер-угроз предлагают «АльфаСтрахование», «Сбербанк Страхование», «Согаз», «Альянс» и еще нескольких крупных игроков рынка. Некоторые страховые компании предлагают расширить классический полис имущественного страхования и включают в него риск кибер-угроз.

На текущем этапе для более широкого распространения данного вида страхования отсутствует и законодательная база, и судебная практика. Также серьезным препятствием является нехватка в российских страховых компаниях специалистов, имеющих представление о структуре рисков. Поэтому для развития кибер-страхования на отечественном рынке рекомендуется:

3. Использовать фронтинг.

Так как страхование кибер-рисков является недостаточно перспективным и слишком рисковым, на помощь 55 отечественным страховым компаниям может прийти фронтинг.

В этом случае российским страховым компаниям лучше всего удерживать минимальную долю риска у себя, а оставшуюся передавать иностранному партнеру;

– Повысить квалификацию сотрудников страховых компаний для возможности выхода на рынок страхования кибер-угроз;

– Использовать передовые аналитические разработки (такие как Blockchain, андеррайтинг) для возможности оценки кибер-рисков, так как в отечественной практике нет общепринятой методики.

УДК 343

Ю. А. ГАРАЕВА[1]

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 207.3 УК РФ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СМИ

В условиях современной геополитической ситуации наблюдается поступательная и закономерная криминализация законодателем ряда деяний, которые, характеризуясь высокой общественной опасностью, представляют угрозу для наиболее значимых и ключевых общественных отношений. Так, отметим, что правоприменительная практика по новым статьям (ст.ст. 207.3, 280.3,

[1] Научный руководитель – ФЕДЫШИНА Полина Викторовна, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации.

280.4 УК РФ) проходит фазу активного формирования и характеризуется высокой степенью дифференциации, что связано с отсутствием четких разъяснений относительно ряда категорий, непосредственно коррелирующих с признаками объективной и субъективной стороны вышеупомянутых составов.

В рамках данной работы научный интерес представляют некоторые вопросы квалификации деяний лиц по ст. 207.3 УК РФ с точки зрения анализа объективных признаков анализируемого состава и отдельных особенностей, относящихся к субъекту рассматриваемого преступления.

Так, резюмируя объективную сторону состава исследуемого преступления, следует отметить, что она проявляется в осуществлении действий, которые находят свое отражение в публичном распространении под видом достоверных сообщений заведомо ложной информации, содержащей данные об использовании Вооруженных Сил Российской Федерации и исполнении государственными органами Российской Федерации своих полномочий, а равно содержащей данные об оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные силы Российской Федерации.

Отметим, что категорию «публичности» применительно к данному составу в доктрине предлагается рассматривать (в силу отсутствия частных разъяснений как законодателя, так и высшей судебной инстанции) в тех рамках, в которых она широко используется в конструкции иных составов преступлений (ст. 205.2, 280, 280.1 УК РФ), т.к. их совершение характеризуется аналогичной особенностью[1].

Так, научный анализ положений судебного истолкования данной категории, которые содержатся в Постановлении Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 (в ред. от 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности, ориентирует на то, что «публичность» должна решаться с учетом места,

[1] Кибальник А. Г. Уголовная ответственность за публичное распространение фейков об использовании Вооруженных Сил РФ. Как применять новую статью // Уголовный процесс. 2022. № 5. С. 67.

способа, обстановки и иных обстоятельств совершенного деяния (к примеру, публичными считаются призывы к группе людей в общественных местах, на митингах; распространение листовок, обращения путем массовой рассылки сообщений посредством мобильной связи и др.).

Также, следуя указаниям высшей судебной инстанции, отметим, что средства массовой информации, электронные или информационно-телекоммуникационных сетей, в том числе сети «Интернет» также используются в указанных целях, что приобретает особую актуальность в связи с современными способами распространения новостей.

Применяя разъяснения высшей судебной инстанции по аналогии, мы можем обратиться к положениям обзоров судебной практики, а именно, разъясняющих особенности применительно к ст. 207.1 и 207.2 УК РФ, так как в настоящих составах усматривается определенное сходство (в силу размещения в одной главе УК РФ, сходности в особенностях распространения информации и др.), которые ориентируют нас на то, что распространение заведомо ложной информации следует признавать публичным, если такая информация адресована группе или неограниченному кругу лиц и выражена в любой доступной для них форме (например, это может осуществляться с использованием устной формы, а также письменной, могут использоваться технические средства)[1].

Сделаем небольшое уточнение относительно того, что в доктрине выделяют несколько видов «публичности»[2] – в рамках совершения рассматриваемых нами преступных деяний с использованием средств массовой информа-

[1] Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2 : утв. Президиумом Верховного Суда Российской Федерации 30 апреля 2020 г. // Верховный Суд Российской Федерации : офиц. сайт. П. 13. URL: https://clck.ru/36oZSY (дата обращения: 27.11.2023).

[2] Дулькина Л. В. Уголовная ответственность за публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации и исполнении государственными органами Российской Федерации своих полномочий : дис. … канд. юрид. наук. Краснодар, 2023. С. 14.

ции мы можем говорить, в первую, очередь, о бесконтактной, так как положения ст. 2 Закона Российской Федерации «О средствах массовой информации»[1], которые определяют виды таких средств, дают основания полагать, что данные виды средств массовой информации в большей степени рассчитаны на создание (и распространение) новостного (информационного) контента без непосредственного контакта с воспринимающей информацию публикой, более того, характер данной «публичности» по большей части может быть рассмотрен как неконкретизированный, поскольку наблюдается их ориентированность на постоянное расширение круга воспринимающих информацию (поэтому, представляется, что наличие данных о тираже определенной газеты не будет являться подтверждением «конкретизированного» характера публичности – один экземпляр может передаваться, его прочтение осуществляться некой группой лиц).

Переходя к анализу отдельных признаков субъекта, распространяющего вышеупомянутую информацию в рамках ст. 207.3 УК РФ, отметим, что в качестве основных «проводников» информации о деятельности Вооруженных сил Российской Федерации и государственных органов Российской Федерации на данный момент выступают военные корреспонденты.

Так, подчеркнем, что одной из значимых проблем на данный момент является отсутствие в уголовно-правовом поле Российской Федерации понятия «военный корреспондент». Нормы Закона «О средствах массовой информации» подчеркивают, что журналист – это лицо, занимающееся редактированием, созданием, сбором или подготовкой сообщений и материалов для редакции зарегистрированного средства массовой информации, связанное с ней трудовыми или иными договорными отношениями либо занимающееся такой деятельностью по ее уполномочию. Представляется, что данное понятие

[1] О средствах массовой информации : Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 : текст с изм. и доп. на 13 июня 2023 г. Ст. 2. URL: https://clck.ru/33rH9h (дата обращения: 27.11.2023).

можно подвергнуть дифференциации – так, журналист может занимать штатную должность в редакционном аппарате (собственный корреспондент), либо же выполнять особое задание редакции (специальный корреспондент).

Однако, в связи с узкоспециализированным характером распространяемой информации (она должна, полагаем, способствовать формированию определенного информационного поля, характеризующегося военной направленностью и удовлетворять требованиям, предъявляемым для способствования выполнению задач, стоящих перед Вооруженными силами РФ и государственными органами в этой сфере), представляется, что данным условиям соответствует система военных средств массовой информации – соответствующих печатных и электронных средств, курируемых Министерством обороны Российской Федерации и иными военно-силовыми ведомствами, которые могут обеспечить качество распространяемых новостных сводок.

В качестве примера таких средств массовой информации можно привести газеты («Красная звезда», журналы («Армейский сборник») (курируются посредством ФГБУ «РИЦ «Красная звезда» Министерства обороны Российской Федерации»), телеканал «Звезда» (курируется Министерством обороны Российской Федерации посредством ОАО «Телерадиокомпания Вооруженных Сил Российской Федерации «Звезда»).

Но исключительно ли средства массовой информации, учредителями и издателями которых являются вышеупомянутые ведомственные структуры, используют штатных военных корреспондентов в целях освещения информации о деятельности силовых структур?

Так, в качестве примеров вневедомственных средств массовой информации, специализирующихся не исключительно на военной тематике, о чем свидетельствуют материалы, размещенные в открытом доступе в информационно-телекоммуникационной сети «Интернет), можно привести главный информационный телеканал страны – ВГТРК (специальным корреспондентом

которой является Е.Е. Поддубный). Также, можно отметить общественно-политическую газету «Комсомольская правда» (специальный корреспондент – Д.А. Стешин).

В связи с этим, корректируя понятие военного корреспондента, мы должны акцентировать внимание как на различного рода средствах массовой информации, курируемых Министерством обороны Российской Федерации и иными ведомствами, так и ими не курируемых.

Так, предлагается понятие военного корреспондента – это профессиональный журналист, занимающий штатную должность в аппарате как ведомственного, так и вневедомственного органа публичной передачи информации, так и иностранного органа средств массовой информации, целью деятельности которого является наглядная репрезентация событий, связанных с участием Российской Федерации в военных конфликтах в целях осуществления задач, стоящих перед Вооруженными Силами Российской Федерации и государственными органами Российской Федерации в соответствии с международными договорами и соглашениями, стороной в которых является Российская Федерация, а также федеральными конституционными и федеральными законами Российской Федерации. В данном случае применимо понятие «военного конфликта», так как, согласно Военной доктрине Российской Федерации, понятие военного конфликта охватывает все виды вооруженного противоборства и включает различного рода войны и вооруженные конфликты.

Представляется значимым вопрос, будут ли в качестве данных лиц в контексте совершения преступления, предусмотренного ст. 207.3 УК РФ, рассматриваться лица, имеющие гражданство иностранных государств. Так, в Российской Федерации презюмируется действие уголовного закона в отношении иностранных лиц (совершивших такое деяние вне пределов нашего государства) в том случае, если оно направлено против интересов Российской Федерации, что провозглашает ст. 12 УК РФ, а в соответствии с п. 26 Стратегии национальной безопасности Российской Федерации, обеспечение и защита нацио-

нальных интересов Российской Федерации осуществляется в рамках реализации такого стратегического приоритета, как государственная и общественная безопасность[1] (что имеет непосредственную корреляцию с родовым объектом преступлений гл. 24 УК РФ), в связи с чем данное понятие было дополнено – «так и иностранного органа средств массовой информации».

Интересен для рассмотрения иной проблемный аспект – можем ли мы рассматривать военного корреспондента как в качестве субъекта п. а) ч. 2 ст. 207.3 УК РФ, а именно, может ли данное лицо рассматриваться в качестве использующего для совершения вышеупомянутого деяния служебное положение, которым оно наделено.

Так, вполне разумным замечанием является тот факт, что военные корреспонденты не могут рассматриваться как в качестве должностных лиц (п. 1 прим. к ст. 285 УК РФ), так и, соответственно, лиц, выполняющих управленческие функции в коммерческих и иных организациях (п. 1 прим. к ст. 201 УК РФ).

Анализируя разъяснения, которые были даны высшей судебной инстанцией относительно вышеупомянутых лиц, подчеркнем, что в Постановлении Пленума Верховного Суда Российской Федерации от 15.06.2006 № 14 наблюдается непосредственная корреляция использования служебного положения с осуществлением трудовых функций[2].

Применительно к военным корреспондентам, видится вполне разумным отметить, что они ответственны за содержание репортажей, ими осуществляемых в прямом эфире, информационных заметок, публикуемых в сети «Интернет» относительно ситуации, связанной с участием Российской Федерации

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 г. № 400. Пп. 25, 26. URL: https://clck.ru/36oZd2 (дата обращения: 27.11.2023).

[2] О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами : Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14. П. 22. Доступ из справ.-правовой системы «КонсультантПлюс».

в военных конфликтах, поскольку у них имеются определенные профессиональные полномочия, связанные с формированием содержания публикуемых ими аудио-, видео- и графических фрагментов что вытекает из осуществления ими трудовых функций в соответствующем средстве массовой информации.

В связи с вышеизложенным, квалификация по п. а) ч. 2 ст. 207.3 УК РФ будет характеризоваться высокой степенью распространенности и найдет отражение в формирующейся судебной практике судов различных уровней, если в соответствующих разъяснениях высшей судебной инстанции будет дано расширительное толкование понятия «служебное положение» и будет обращено внимание на соответствующие профессиональные полномочия, присущие военным корреспондентам.

В условиях современной ситуации отмечается наличие еще одного проблемного аспекта, а именно – наличия определенной плеяды как блогеров, распространяющих контент в широком диапазоне, так и военно-политических блогеров, которые, имея образование журналиста, формируют свои собственные страницы в сети «Интернет», новостные каналы и создают информационные заметки, посты, выкладывают различные графические изображения, которые являются наглядной иллюстрацией участия Российской Федерации в военных конфликтах и выступают в качестве маркера, формирующего общественное мнение граждан нашего государства. Данные лица также могут заниматься ведением данной деятельности, не связав себя узами трудового договора с какой-либо организацией или средством массовой информации.

Так, анализируя возможность ответа на данный вопрос, отметим, что, в соответствии с требованиями Закона «О средствах массовой информации», в качестве таких средств рассматриваются лишь вышеупомянутые нами в ст. 2 данного нормативного правового акта. Немаловажен и тот факт, что к сетевым изданиям закон относит только сайты, зарегистрированные как средствах массовой информации (новостных каналов, соответственно, в этом списке нет).

Подчеркнем, что в соответствии с вышеупомянутой нормативной правовой базой, введением отдельных субъектов в поле правового регулирования

и рассмотрением их в качестве средствах массовой информации в России занимается Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В рамках официального приобретения соответствующего статуса на редакцию или издателя (в качестве таковых может рассматриваться блогер или объединение блогеров – создателей контента в сети «Интернет) налагаются определенные обязанности в виде подачи соответствующей заявки на регистрацию, тщательной подготовки устава редакции с указанием необходимых данных об учредителях и оплаты государственной пошлины.

Однако, несмотря на необходимость осуществления уравнения в делегированных законодателем правах и обязанностях всех распространителей информации – средств массовой информации, блогеров, в настоящее время наблюдается вполне линейная направленность при квалификации общественно опасных деяний, совершаемых блогерами – так, в приговоре по делу Белоцерковской судом была осуществлена квалификация деяния блогера по п. «д» ч. 2 ст. 207.3 УК РФ (по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды)[1], в приговоре по делу Курмоярова суд пришел к выводу о неизбежности квалификации по п. «г» (из корыстных побуждений), п. «д» ч. 2 ст. 207.3 УК РФ[2]. Представляется, однако, что распространение вышеупомянутой информации блогерами, которые будут регистрироваться в качестве средств массовой информации, может послужить основанием для квалификации соответствующих действий, ими совершаемых, по п. «а» ч. 2 ст. 207.3 УК РФ (наравне с военными корреспондентами).

В заключение хочется отметить, что условия, сложившиеся в рамках современной геополитической ситуации, вне всякого сомнения, определенным образом повлияли на деятельность средств массовой информации, военных

[1] Приговор Басманного районного суда г. Москвы от 6 февраля 2023 г. по делу № 01-0001/2023. URL: https://clck.ru/36oxSC (дата обращения: 27.11.2023).

[2] Приговор Калининского районного суда г. Санкт-Петербурга от 31 августа 2023 г. по делу № 1-168/2023. URL: https://clck.ru/36oxza (дата обращения: 27.11.2023).

корреспондентов, блогеров и других участников, осуществляющих в рамках единого информационного пространства Российской Федерации свою деятельность, ставшую предметом обоснованного научного интереса в рамках науки уголовного права.

Так, особое внимание следует уделить разъяснению положений анализируемой нами статьи в рамках интерпретации категории «публичности» (ее бесконтактный характер, неконкретизированность), а также вопросам квалификации действий указанных лиц (военных корреспондентов, блогеров, как выступающих в качестве средств массовой информации, так и функционирующих независимо от системы таких средств) по соответствующим пунктам статьи 207.3 УК РФ. Включение указанных рассмотренных нами вопросов в новое Постановление Пленума Верховного Суда Российской Федерации, позволит приблизиться к закономерному расширению правоприменительной практики по данной статье и ориентировать соответствующие органы на слаженную работу в данной сфере.

УДК 343

Г. Н. ГЛУЗДАК,
Д. В. МАТВЕЕВ[1]

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ (статья 274.2 УК РФ)

На сегодняшний день деятельность человека немыслима без использования компьютерных технологий, в том числе информационно-телекоммуникационных сетей, среди которых особое место занимает сеть «Интернет». Количество интернет-пользователей увеличивается из года в год: так, по данным

[1] Научный руководитель — ШАРАПОВ Роман Дмитриевич, профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, профессор.

Росстата, если в 2016 году сеть «Интернет» использовали 76,4 % населения[1] страны, то уже в 2018 году данный показатель был равен 83,8 %[2], в 2020 году достиг 87,2 %, а в 2021 году составил 90,1 %[3]. В связи с этим особую опасность приобретает информация, распространяемая с нарушением закона. Попадая в сеть «Интернет», она становится публичной, то есть адресованной неопределенному кругу лиц, а значит может воздействовать на сознание широких слоев населения[4].

Противодействие распространению противоправной информации является одним из основных направлений политики цифрового суверенитета. Для этих целей, помимо прочего, используются технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (далее также – ТСПУ). Обязанности операторов связи по установке ТСПУ, а также по пропуску интернет-трафика через ТСПУ предусмотрены п. 8 ст. 44, п. 5.1, п. 5.2 ст. 46, п. 2 ст. 56.2 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи».

Для обеспечения выполнения указанных обязанностей приняты Федеральные законы от 24 февраля 2021 года № 19-ФЗ, от 14 июля 2022 года № 259-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», в соответствии с которыми административно-деликтный закон дополнен соответственно ст. 13.42, предусматривающей административную ответственность за нарушение оператором связи порядка установки, эксплуатации и модернизации ТСПУ, и ст. 13.42.1, вводящей

[1] Информация получена Росстатом по материалам выборочных обследований населения по вопросам использования ИКТ в группе «население в возрасте 15—74 лет».

[2] Российский статистический ежегодник. 2019 / Росстат. М., 2019. С. 499. URL: https://rosstat.gov.ru/storage/mediabank/Ejegodnik_2019.pdf (дата обращения: 08.10.2023).

[3] Российский статистический ежегодник. 2022 / Росстат. М., 2022. 691 с. URL: https://rosstat.gov.ru/storage/mediabank/Ejegodnik_2022.pdf (дата обращения: 08.10.2023).

[4] Глуздак Г. Н., Булгакова Л. С. Понятие публичных призывов как признака объективной стороны противоправного деяния // Вестник Академии Следственного комитета Российской Федерации. 2023. № 2(36). С. 47.

санкцию за нарушение оператором связи требований к пропуску трафика через ТСПУ. Ответственность по ч. 1 ст. ст. 13.42, 13.42.1 КоАП РФ несут лица, впервые совершившие указанные проступки, а по ч. 2 ст.ст. 13.42, 13.42.1 КоАП РФ – лица, повторно совершившие правонарушения указанной категории.

Однако такие меры законодатель счел недостаточными, поэтому Федеральным законом от 14 июля 2022 года № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» уголовный закон был дополнен ст. 274.2, фактически предусматривающей ответственность за повторное совершение административных правонарушений, предусмотренных ч. 2 ст.ст. 13.42, 13.42.1 КоАП РФ.

Анализ данной нормы полагаем целесообразным начать с ее названия. Так, ст. 274.2 УК РФ именуется не иначе как «нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования». По нашему мнению, подобная формулировка является не вполне логичной.

Полагаем, что при конструировании бланкетной диспозиции ст. 274.2 УК РФ законодатель преследовал цель сделать ссылку на Правила централизованного управления сетью связи общего пользования[1] (далее – Правила № 127). Однако в силу п. 2 данных правил централизованное управление осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Таким образом, основываясь на буквальном толковании уголовного закона, нарушение правил централизован-

[1] Об утверждении Правил централизованного управления сетью связи общего пользования : Постановление Правительства Российской Федерации от 12 февраля 2020 г. № 127. Доступ из справ.-правовой системы «КонсультантПлюс».

ного управления ТСПУ должно предусматривать в первую очередь ответственность должностных лиц данной службы (например, в случае нарушения указанным органом установленной п. 7 ст. 65.1 Закона о связи обязанности по информированию лиц, участвующих в централизованном управлении, в случае возникновения соответствующих угроз). Вместе с тем объективной стороной ч. 1, ч. 2 ст. 274.2 УК РФ подобные деяния не охватываются, при этом обязательные требования для операторов связи содержатся в ином нормативном правовом акте – Правилах установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования[1] (далее – Правила № 126).

Видовым объектом всех преступлений, сгруппированных в главе 28 УК РФ, выступает информационная безопасность, являющаяся более узким понятием по отношению к общественной безопасности. Определение информационной безопасности приведено в Доктрине информационной безопасности Российской Федерации[2]. В соответствии с этим документом под информационной безопасностью следует понимать состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства. В качестве непосредственного объекта преступления, предусмотренного

[1] Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования : Постановление Правительства Российской Федерации от 12 февраля 2020 г. № 126 : текст с изм. и доп. на 28 мая 2022 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 г. № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

ст. 274.2 УК РФ, находим обоснованным рассматривать общественные отношения, обеспечивающие защищенность личности, общества и государства от угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Как отмечает А. Н. Попов, с появлением статьи 274.1 УК РФ предмет преступлений главы 28 УК РФ расширился от компьютерной информации до объектов информатизации; информационных систем; сайтов; сетей связи; информационных технологий; деятельности субъектов, связанной с формированием и обработкой информации, развитием и использованием информационных технологий, обеспечением информационной безопасности[1]. С включением в уголовный закон ст. 274.2 УК РФ данный перечень также дополнился техническими средствами противодействия угрозам. При этом Е. А. Русскевич обращает внимание на тот факт, что в открытом доступе отсутствуют достоверные сведения о составе ТСПУ, поскольку указанная информация составляет коммерческую тайну[2].

Объективная сторона ч. 1 ст. 274.2 УК РФ состоит в нарушении порядка установки, эксплуатации и модернизации ТСПУ, а ч. 2 ст. 274.2 УК РФ – в нарушении требований к пропуску трафика через ТСПУ. При этом законодателем не уточняются последствия, которые может повлечь нарушение указанных обязательных требований, что позволяет сделать вывод: рассматриваемый состав является формальным. К числу нарушений порядка установки, эксплуатации и модернизации ТСПУ, требований к пропуску трафика через ТСПУ, влекущих ответственность по ст. 274.2 УК РФ, на наш взгляд, может быть отнесен значительный круг действий (бездействий) оператора связи: от полного отказа от установки ТСПУ (в нарушение п. 8 ст. 44, п. 5.1 ст. 46 Закона

[1] Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб., 2018. С. 22—23.

[2] Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 663.

о связи) до несоблюдения правил эксплуатации ТСПУ, установленных производителем соответствующего оборудования (в нарушение пп. «е» п. 10 Правил № 126). Мы не ставим под сомнение обоснованность криминализации злостного игнорирования требований федерального законодательства, однако множество вопросов вызывает возможность привлечения к уголовной ответственности за отход от требований эксплуатационной документации, которая может произвольно изменяться производителями ТСПУ, даже если указанное обстоятельство не повлекло каких-либо общественно опасных последствий. Во втором случае, на наш взгляд, справедливо говорить о малозначительности деяния.

По нашему мнению, чтобы преодолеть изложенную проблему, следует изменить конструкцию состава преступления, предусмотренного ст. 274.2 УК РФ, с формального на материальный. Для определения возможных криминообразующих общественно опасных последствий нарушения правил централизованного управления ТСПУ можно обратиться к ч. 10 ст. 19.2 Федерального закона от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности», характеризующей грубые нарушения лицензионных требований: в частности, возникновение угрозы причинения вреда жизни, здоровью граждан, вреда животным, растениям, окружающей среде, объектам культурного наследия (памятникам истории и культуры) народов Российской Федерации, а также угрозы чрезвычайных ситуаций техногенного характера; нанесение ущерба правам граждан (например, праву на получение достоверной информации, право на защиту детей от информации, причиняющей вред их здоровью и развитию и т. д.), законным интересам граждан, обороне страны и безопасности государства.

Субъект преступления, предусмотренного ст. 274.2 УК РФ, специальный. Им является должностное лицо, определение которого дано в примечании рассматриваемой статьи. Под должностным лицом для целей ст. 274.2 УК РФ по-

нимается лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации.

При этом, поскольку рассматриваемое преступление предусматривает административную преюдицию, следует упомянуть, что единственное отличие между составом преступления с административной преюдицией и составом аналогичного административного правонарушения заключается в их субъекте, в остальном же (по объекту, объективной и субъективной стороне) они тождественны[1]. Из этого следует, что субъектом рассматриваемого преступления может быть исключительно должностное лицо оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет». В соответствии с подп. 12 п. 1 ст. 2 Закона о связи оператором связи считается юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии. Мы убеждены, что деятельность должностного лица организации, фактически оказывающей услуги связи при отсутствии такой лицензии, не охватывается составом по ст. 274.2 УК РФ, но при наличии оснований может и должна получить оценку, например, по ст. 171 УК РФ.

Кроме того, п. 17 Правил № 127 устанавливает, что лица, участвующие в централизованном управлении, определяют должностное лицо (лиц) из числа сотрудников, ответственное за организационно-техническое взаимодействие в рамках централизованного управления. Таким образом, полагаем, что субъектом рассматриваемого преступления надлежит считать указанное лицо, а при его отсутствии – руководителя организации, оказывающей услуги связи, либо индивидуального предпринимателя, оказывающего услуги связи.

При всем при этом для квалификации действий (бездействий) названных должностных лиц по ст. 274.2 УК РФ на момент выполнения объективной стороны рассматриваемого состава они должны считаться лично подвергнутыми

[1] Акинина Н. Ю., Берндт А. А. Институт административной преюдиции в Уголовном кодексе Российской Федерации // Вестник Югорского государственного университета. 2017. № 1-2. С. 84.

административному наказанию по ч. 2 ст. 13.42 либо ч. 2 ст. 13.42.1 КоАП РФ, то есть претерпевать меры административно-правового воздействия самостоятельно как должностные лица либо индивидуальные предприниматели. На практике такая конструкция субъекта преступления фактически делает ст. 274.2 УК РФ неприменимой: во-первых, органы административной юрисдикции зачастую предпочитают привлекать операторов связи к ответственности не как должностных лиц, а как юридических лиц (главным образом из-за больших размеров административных штрафов); во-вторых, учредителю или руководителю организации, оказывающей услуги связи, ничего не стоит назначить нового сотрудника ответственным за организационно-техническое взаимодействие в рамках централизованного управления ТСПУ в случае привлечения предыдущего к административной ответственности по ст.ст. 13.42, 13.42.1 КоАП РФ.

Вопрос о том, может ли субъективная сторона данного состава преступления наряду с умыслом характеризоваться неосторожностью, на наш взгляд, является неоднозначным. С одной стороны, как отмечает Е. А. Русскевич, поскольку состав ст. 274.2 УК РФ является формальным, то субъективная сторона рассматриваемого преступления выражается виной в виде прямого умысла[1]. Такую точку зрения подтверждают и рассуждения о том, что должностное лицо, дважды привлеченное к административной ответственности за совершение аналогичных деяний, должно осознавать общественную опасность своих действий (бездействия).

Вместе с тем уголовный закон не исключает возможности совершения преступлений с формальным составом по неосторожности, а именно в силу преступной небрежности[2]. Полагаем, что преступления, предусмотренные ст. 274.2 УК РФ, могут характеризоваться и неосторожной формой вины: например, преступная небрежность усматривается в ситуациях, когда долж-

[1] Русскевич Е. А. Указ. соч.

[2] Муромцев А. М. К вопросу об уголовно-правовой оценке неосторожной формы вины // Наука. Общество. Государство. 2020. Т. 8, № 4 (32). С. 110.

ностное лицо оператора связи не обеспечило надлежащий контроль за деятельностью подчиненных работников по установке ТСПУ, хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия. Кроме того, в поддержку данной точки зрения можно привести позицию, в соответствии с которой если в диспозиции статьи Особенной части УК РФ форма вины не конкретизирована, то соответствующее преступление может быть совершено умышленно или по неосторожности при условии, если об этом свидетельствуют содержание деяния, способы его совершения и иные признаки объективной стороны его состава[1].

Учитывая приведенные недостатки, касающиеся практически всех элементов состава данного преступления и даже самой формулировки ст. 274.2 УК РФ, встает вопрос об обоснованности криминализации рассматриваемых деяний. Более подходящим и функционально верным нам представляется другой механизм привлечения должностных лиц операторов связи, злостно игнорирующих требования законодательства о связи в части централизованного управления ТСПУ, к юридической ответственности. Так, одним из лицензионных требований, обязательных для соблюдения при осуществлении деятельности по оказанию услуг связи по передаче данных, является обеспечение реализации требований, связанных с устойчивостью, безопасностью и целостностью функционирования на территории Российской Федерации сети связи общего пользования, в том числе информационно-телекоммуникационной сети «Интернет»[2]. В силу ст. ст. 37, 39 Закона о связи лицензия на оказание услуг связи может быть приостановлена и впоследствии аннулирована. В случае,

[1] О применении судами законодательства об ответственности за нарушения в области охраны окружающей среды и природопользования : Постановление Пленума Верховного Суда Российской Федерации от 18 октября 2012 года № 21. П. 4. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О лицензировании деятельности в области оказания услуг связи и признании утратившими силу некоторых актов Правительства Российской Федерации : Постановление Правительства Российской Федерации от 30 декабря 2020 г. № 2385. П. 11. Доступ из справ.-правовой системы «КонсультантПлюс».

если организация либо индивидуальный предприниматель продолжат оказывать услуги связи, указанная деятельность при наличии оснований может оцениваться как незаконное предпринимательство по ст. 171 УК РФ.

В заключение отметим, что на момент проведения исследования нам не удалось найти информации о практике привлечения операторов связи к административной ответственности по ст. ст. 13.42, 13.42.1 КоАП РФ. Обобщая вышеизложенное и учитывая обозначенные проблемы, которые могут возникать в связи с применением ст. 274.2 УК РФ, находим дополнение уголовного закона данной статьей преждевременным.

УДК 343

К. Н. ГОРДИЕНКО[1]

КВАЛИФИКАЦИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ (на примере п. «б» ч. 2 ст. 228.1 УК РФ)

Наркотизм как социальное явление приобрело массовый характер, все еще являясь многофакторной национальной угрозой. Преступления в сфере незаконного оборота наркотиков всегда влекут вполне определенные негативные последствия: их распространение причиняет вред здоровью и жизни лицам, их употребляющим. Так, все усложняющиеся способы сбыта качественно увеличивают уровень конспирации соучастников преступления, что вызывает затруднения при оценке данный деяний, их правильной квалификации. Так, например, согласно статистическим данным, представленным главным информационно–аналитическим центром в период за январь-июль 2023 года преступлений, которые связаны с незаконным производством, сбытом или пересылкой наркотических средств, совершенных при

[1] Научный руководитель – ФЕДЫШИНА Полина Викторовна, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации.

этом с применением информационных технологий составляет 47 685 тыс.[1], что обуславливает необходимость уделять данному способу при совершении преступных действий особое внимание.

Также стоит отметить повышенную общественную опасность таких деяний, выраженную в их распространенности, возможности сбыта данных средств и веществ неопределенному кругу лиц, а также легкой доступности их приобретения и продажи в любой момент времени.

Из Указа Президента Российской Федерации от 23.11.2020 № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» следует, что появление новых форм противоправной деятельности организованных групп и преступных сообществ (преступных организаций), усиление ими конспирации каналов поставки и сбыта наркотиков с использованием инновационных коммуникационных и других новых технологий представляет угрозу национальной безопасности в сфере оборота наркотиков, а также в области противодействия их незаконному обороту. Наряду с этим, «фактом, существенно осложняющим борьбу с преступлениями, носящими международный характер, является то обстоятельство, что, несмотря на то что российским специальным службам о существовании интернет-сети DarkNet давно известно как о лидере по распространению наркотических средств и психотропных веществ, указанная интернет-сеть до сих пор остается «черной дырой», которая не позволяет предотвращать либо поставить под контроль совершаемые посредством этой сети преступления»[2].

По части второй ст. 228.1 УК РФ устанавливается ответственность с соответствующим квалифицирующим признаком только в случае сбыта нарко-

[1] Краткая характеристика состояния преступности в Российской Федерации за январь—июль 2023 года // Статистика и аналитика. URL: xn--b1aew.xn--p1ai (дата обращения: 18.09.2023).

[2] Конин В. В. Новые особенности элементов криминалистической характеристики контрабанды наркотических средств (на основе анализа материалов уголовного дела) / В. В. Конин // Современное право. 2018. № 5. С. 86.

тических средств психотропных веществ и их аналогов, но не растений, содержащих наркотические средства и психотропные вещества либо их части, что не всегда замечает законодатель. Кроме того, практике известны случаи ошибочного вменения квалифицирующего признака при пересылке.[1] В п. 17 Постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» указано, что «под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. При этом следует иметь в виду, что сеть «Интернет» является одним из их видов»[2].

Обозначим, что предметом рассмотрения не является признак использования электронных сетей или средств массовой информации.

М.А. Любавина со ссылкой на Федеральный закон «О наркотических средствах и психотропных веществах» пишет, что «под сбытом новых потенциально опасных психоактивных веществ понимается отчуждение веществ другим лицам любыми способами. Поэтому объективная сторона сбыта заключается в совершении действий по отчуждению указанных средств и веществ приобретателю, а сбыт с использованием информационно-

[1] Кассационное определение Верховного Суда Российской Федерации от 28 мая 2019 г. по делу № 127-УД19-8. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37: текст с изм. и доп. на 21 февр. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

телекоммуникационных сетей (включая сеть «Интернет») – является способом бесконтактной реализации (отчуждения)[1].

Данная позиция, однако, не вполне соотносится с мнением законодателя. В продолжение этого, сбыт предлагается рассматривать не как конкретные действия (совокупность действий), а как незаконную деятельность лица, направленную на их возмездную либо безвозмездную реализацию (продажа, дарение, обмен, уплата долга, дача взаймы и т. д.) другому лицу[2]. Следовательно, согласно разъяснениям Верховного Суда Российской Федерации, под данный признак подпадают и действия на стадии неоконченного сбыта. Это свидетельствует о непоследовательности в понимании сбыта и дальнейшей оценке дополнительных признаков состава, не учитывая позицию Верховного Суда Российской Федерации. Проблема учета данного признака, думается, коренится в самом понятии сбыта. Ранее сбыт рассматривался как любая передача и проблем с разграничением стадий особо не было, но сейчас, ввиду видоизменения конструкции понятия, под сбытом предложено понимать деятельность, направленную на реализацию, а признак «с использованием сети «Интернет» стал учитываться даже и при совершении действий до начала отчуждения, то есть по сути на приготовительной стадии: переговоров между соучастниками, с потенциальными покупателями об условиях приобретения, ассортименте, свойствах и др., о чем прямо говорится в Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

---

[1] Любавина М. А. Уголовно-правовое противодействие наркотизму: закон, теория, практика : монография. М., 2021. С. 701.

[2] О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами : Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14: текст с изм. и доп. на 16 мая 2017 г. Доступ из справ.-правовой системы «КонсультантПлюс».

В связи с этим следует согласиться с позицией М.А. Любавиной и отдать предпочтение определению сбыта, изложенному в Федеральном законе «О наркотических средствах и психотропных веществах». Ведь с точки зрения права Пленум Верховного Суда Российской Федерации лишь дает разъяснения и толкует правовые нормы, поэтому нельзя апеллировать к понятию сбыта, данному в постановлении Пленума, тем более, при наличии Федерального Закона, в котором дано определение сбыта именно через их отчуждение другим лицам любыми способами (хотя и применительно к новым потенциально опасным психоактивным веществам), более того, закрепленное в Федеральном законе после постановления.

Как справедливо отмечает автор, использование средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») — способ совершения преступления, характеризующий объективную сторону преступления, а в данном случае сбыта наркотических средств, психотропных веществ или их аналогов[1]. Следовательно, сбыт наркотических средств, психотропных веществ или их аналогов следует признавать совершенным с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), когда применение указанных сетей связано исключительно с выполнением объективной стороны преступления — с процессом передачи запрещенных веществ потребителю, т. е. в данном случае — с получением информации о месте нахождения тайника-закладки[2].

Итак, в связи с этим возникает проблема правомерного вменения п. б ч. 2 ст. 228.1 УК РФ. По нашему мнению, возможно смоделировать следующие случаи использования информационно-телекоммуникационной сети (включая сеть «Интернет») при незаконном сбыте:

---

[1] Любавина М. А. Указ. соч. С. 695.

[2] Хромов Е. В. Проблемы квалификации сбыта наркотических средств, психотропных веществ или их аналогов с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») // Криминалист. 2021. № 3 (36). С. 34—35.

1. использование при приобретении предмета преступления в целях дальнейшего сбыта;

2. использование для установления контакта между сбытчиком и получателем предмета преступления в целях сбыта при личной встрече, непосредственном контакте;

3. использование для установления контакта между сбытчиком и получателем предмета преступления в целях сбыта при бесконтактном способе;

4. использование соучастниками преступления в целях поддержания контакта между собой;

5. использование для оплаты наркотиков.

В Постановлении Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием информационно – телекоммуникационных сетей, включая сеть «Интернет» указано, что по признаку, предусмотренному п. «б» ч. 2 ст. 228.1 УК РФ, при незаконном сбыте наркотических средств квалифицируется и совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (например, при незаконном сбыте наркотических средств обеспечивалась связь между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

Согласно приговору Ш. осужден за незаконный сбыт наркотических средств, совершенный группой лиц по предварительному сговору с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» в крупном размере. Однако в кассационной жалобе осужденный не согласился с приговором[1].

[1] Кассационное определение Четвертого кассационного суда общей юрисдикции от сентября 2022 г. по делу № 77-3331. Доступ из справ.-правовой системы «КонсультантПлюс».

Ш. считал, что ему ошибочно вменили квалифицирующий признак «с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», т.к. применение такой сети для достижения договоренности о приобретении наркотиков, предназначенных для сбыта, не подтверждает то, что при непосредственной их передаче и получении оплаты за них использовалась данная сеть.

Вопреки доводам жалобы, суд пришел к выводу о наличии в действиях осужденного данного признака, поскольку согласно п. 20 «преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», независимо от стадии совершения преступления, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети»[1], а, как следует из обстоятельств дела, умыслом Ш. и его соучастником охватывался незаконный сбыт посредством сети «Интернет», выразившийся в обмене между ними и приобретателями информации о нахождении наркотиков.

Так, по логике законодателя, необходимо квалифицировать сбыт с учетом данного признака в любом случае: на любой стадии, даже при приготовительных действиях сбытчиков, при наличии простого факта использования средств связи соучастниками, для поддержания общения и конспирации. С данной позицией сложно согласиться полностью. Думается, только лишь факт общения соучастниками через интернет не характеризует способ сбыта и, соответственно, не повышает степень общественной опасности преступления.

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37: текст с изм. и доп. на 21 февр. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Таким образом, получается, что данная ситуация охватывает сразу два случая, смоделированных нами – первая и третья ситуации, изложенные выше: использование при приобретении предмета преступления в целях дальнейшего сбыта, а также при общении между соучастниками.

Считаем, правомерным учитывать данный признак в случае использования интернета при приобретении наркотика для дальнейшего сбыта.

Следующей типичной ситуацией является сбыт через специально созданные интернет-магазины. Здесь может возникнуть вопрос касаемо того возможно ли сочетание двух совершенно различных способов: сбыт «из рук в руки», то есть передача непосредственно при встрече одновременно с дистанционным способом. Можно смоделировать следующую ситуацию:

А. решил приобрести наркотическое средство, выбрал наркотик через интернет-магазин и оформил заказ, но при этом требует личной встречи, чтоб проверить наркотик при сбытчике и оплатить его при получении. Необходимо ли в этом случае учитывать квалифицирующий признак?

Правоприменительная практика утвердительно отвечает на данный вопрос. Так, Судом установлено, что для взаимодействия между собой, получения сведений о местах нахождения тайников с наркотиками и передачи наркотических средств от одного соучастника другому члены организованной группы использовали «Интернет», потому в действиях осужденного вопреки доводам его жалобы, имеется указанный квалифицирующий признак независимо от того, каким способом наркотики впоследствии передавались приобретателям. Помимо этого, установлено, что интернет-магазин, куда устроился К., предполагал выполнение в автоматическом и круглосуточном режиме обработку запросов потребителей наркотических средств, проверку поступивших от последних платежей и передачу информации о местонахождении наркотических средств, то есть объективно передача наркотических средств без использования сети «Интернет» исключалась[1]. Иная позиция изложена

[1] Кассационное определение Седьмого кассационного суда общей юрисдикции от 2 августа 2023 г. по делу № 77-3015. Доступ из справ.-правовой системы «КонсультантПлюс».

в апелляционном определении, согласно которому получается, что если место встречи оговорено через интернет, выбран наркотик, при этом была непосредственная встреча, на которой передали деньги и сам наркотик покупателю, то квалифицирующего признака не будет[1].

Такого мнения придерживаются и Н.П. Ведищев и Д.Ю. Гладышев: «Если информация о возможности приобретения наркотических средств, психотропных веществ или их аналогов была размещена на сайте, передана посредством электронного сообщения, а также место встречи для их передачи было оговорено тем же способом, а их передача осуществлялась при непосредственном контакте сбытчика и приобретателя, то такой квалифицирующий признак, как сбыт с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), отсутствует[2]. Таким образом, обязательным условием для вменения рассматриваемого признака является отсутствие непосредственного контакта сбытчика и приобретателя[3].

Кроме того, в данной ситуации интересен следующий пример. Так, автор жалобы поместил приобретенные им наркотические средства в тайники, и сообщил об их местонахождении второму осужденному, который, в свою очередь, передал эту информацию неустановленному лицу. Вместе с тем данные о том, что информация о конкретных местах нахождения наркотических средств была доведена до потребителей наркотиков, отсутствуют, поэтому Верховный суд согласился с жалобой обвиняемого и переквалифицировал

---

[1] Апелляционное определение Свердловского областного суда от 8 апреля 2015 г. по делу № 22-2675/2015. Доступ из справ.-правовой системы «КонсультантПлюс». (По смыслу закона при дистанционном сбыте наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») исключается непосредственный контакт приобретателя и сбытчика. Однако в судебном заседании установлено, что И. денежные средства за приобретенное наркотическое средство передал Б. не посредством информационно-телекоммуникационной или электронной сети, а через третье лицо, а Б. приготовился сбыть наркотическое средство Ч. при непосредственном контакте.)

[2] Ведищев Н. П., Гладышев Д. Ю. Незаконный оборот наркотических средств, психотропных веществ или их аналогов (вопросы квалификации, расследования, ОРМ, экспертизы) : монография. М., 2016. С. 114—115.

[3] Щетинина Н. В. Особенности квалификации преступлений, предусмотренных статьями 228 и 228.1 Уголовного кодекса Российской Федерации. Екатеринбург, 2022. С. 43 ; Быкова Е. Г., Казаков А. А. Особенности вменения квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ // Наркоконтроль. 2022. № 1. С. 17.

оконченный сбыт на его покушение, правомерно указав на отсутствие сведений о предоставлении потребителям информации интернет-магазином через сайт в автоматическом режиме без участия оператора[1].

Исходя из этого, можно сделать вывод, что использование при незаконном сбыте подобного рода компьютерных программ, осуществляющих без участия оператора передачу потребителям информации о местах расположения тайников с наркотическими средствами, может указывать на то, что виновное лицо, заранее подготовив для интернет- рассылки указанную информацию, по сути своей выполняет все необходимые действия по передаче приобретателю наркотических средств.

Таким образом, правоприменительная практика свидетельствует о непоследовательности, разных позициях. По итогам исследования данного вопроса, представляется, возможным прийти к следующим выводам:

1. Необходимо вменять квалифицирующий признак «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)» (п. «б» ч. 2 ст. 228.1 УК РФ) в следующих случаях: когда наркосбытчик использовал данные средства для установления и поддержания контакта именно с наркополучателем в целях последующего сбыта (например, передача информации о номере счета, на который покупатель будет перечислять деньги, сообщать о месте тайника, фотографии места, координатах, так как это уже характеризует, непосредственно, способ отчуждения).

2. Представляется верным квалифицировать сбыт с учетом данного признака лишь в том случае, когда информационно-телекоммуникационные сети (включая сеть «Интернет») являются способом совершения преступления, характеризующим объективную сторону незаконного сбыта наркотических средств и психотропных веществ.

[1] Кассационное определение Седьмого кассационного суда общей юрисдикции от 19 июля 2022 г. дело № 44-УД22-18-К7. Доступ из справ.-правовой системы «Консультант-Плюс».

3. Следует исключить случаи неправомерного вменения признака в ситуации, когда данные сети использовались для поддержания контакта между соучастниками. Их использование не усиливает общественной опасности, являясь обычным средством общения между соучастниками, как и при совершении иных видов преступлений.

4. Таким образом, если информация о возможности приобретения наркотических средств размещена на сайте, передана посредством электронного сообщения, а также место встречи для их передачи и способы и размер оплаты были оговорены посредством проводного, сотового телефона или радиостанции, электронной почты, а их передача и (или) оплата осуществлялись при непосредственном контакте сбытчика и приобретателя, то такой квалифицирующий признак, как сбыт наркотических средств, психотропных веществ или их аналогов с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), отсутствует. Это обусловлено тем, что рассматриваемый квалифицирующий признак следует вменять тогда, когда информационно-телекоммуникационные сети используют для непосредственной реализации (отчуждения) наркотиков <20>. Тогда как поиск потребителей, достижение с ними договоренности о месте встречи, способе и размере оплаты не являются способом совершения преступления, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ, и не повышают общественную опасность ввиду того, что если затем наркотические средства будут передавать при непосредственном контакте, то произойдет это без использования приемов конспирации, которая обеспечивается применением обсуждаемого способа сбыта: общественная опасность сбыта наркотических средств посредством электронных или информационно-телекоммуникационных сетей заключается в том, что соблюдение конспирации, когда приобретатель не знает в лицо сбытчика и не может на него указать и опознать его, существенно снижает риск привлечения сбытчика к уголовной ответственности. Это позволяет ему продолжать пре-

ступную деятельность. В то же время сбыт наркотических средств при непосредственном контакте позволяет задержать сбытчика сразу после сбыта и привлечь его к уголовной ответственности при условии надлежащего фиксирования и документирования его действий.

УДК 343

Ю. Е. ГРИБАНОВА[1]

ЭЛЕКТРОННЫЙ ДОКУМЕНТ КАК ПРЕДМЕТ ПОДЛОГА

С развитием информационных технологий и доступностью различных ресурсов становится проще внести недостоверные сведения в официальные документы. Защита граждан от подделки информации является важным вопросом, и существуют различные меры, которые могут быть предприняты для противодействия этому явлению. Одной из такой мер является совершенствование нормативно-правовой базы.

Анализируя УК РФ, можно заметить, что он не содержит в себе ни одного упоминания об официальном документе в электронной форме. Вместе с тем в научной литературе электронный документ уже давно воспринимается наравне с бумажным.

Е. В. Иванова в своей работе отметила, что, если исходить из прямого толкования ст. 327 УК РФ, можно заключить, что она позволяет привлекать к уголовной ответственности тех, кто подделывает официальные документы в электронном виде[2].

Подобного мнения придерживаются и другие авторы, например, В.И. Баландин отмечает: «бурное развитие электронного документооборота и мас-

[1] Научный руководитель – ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

[2] Иванова Е. В. Официальный документ в электронной форме как предмет преступления, предусмотренного ст. 327 УК РФ // Уголовное право. 2012. № 3. С. 30.

совое внедрение электронно-вычислительной техники позволяют с уверенностью говорить о признании в качестве официального не только бумажного, но и электронного документа»[1].

Судебная практика на сегодняшний день также признает электронный документ в качестве предмета преступлений, предусматривающих ответственность за подлог документов. Этому уделяет внимание Постановление Пленума Верховного Суда Российской Федерации от 17.12.2020 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324–327.1 Уголовного кодекса Российской Федерации», в п. 1 которого указывается, что под официальными документами понимаются в том числе электронные документы.

Можно сделать вывод, что вопреки тому, что наука и практика к официальным документам относит и электронные документы, на сегодняшний день законодатель не решается идти на введение их в УК РФ. В связи с этим появляются определенные трудности в деятельности правоохранительных органов и судов. По своей сути правоприменители оказываются в такой ситуации, когда необходимо самостоятельно давать оценку закону. Поскольку уголовно-правовые нормы, которые устанавливают уголовную ответственность за подделку документов, не определяют содержание термина «официальный документ», они оставляют его неопределенным в части характеристики предмета преступления. Это позволяет правоприменителю широко толковать предмет подлога, что, можно предположить, приводит к нарушению прав граждан.

Конституционный Суд Российской Федерации отмечает, что законодатель целенаправленно не включает понятие официального документа в УК РФ, поскольку он имеет субъективную оценочную природу. Правоприменитель самостоятельно в каждом конкретном случае должен оценивать

[1] Баландин В. И. О понимании официального документа по статьям 292 и 327 УК РФ для целей квалификации преступлений // Юридический вестник Самарского университета. 2020. Т. 6, № 2. С. 66.

свойства документа и признавать его либо официальным, либо нет и в зависимости от этого привлекать или не привлекать к уголовной ответственности[1].

Кроме того, Конституционный Суд Российской Федерации указывает на то, что само по себе то обстоятельство, что в УК РФ не содержится определение понятия «официальный документ» не свидетельствует об неопределенности уголовно-правового запрета и основание для произвольного применения данной статьи[2].

Не оспаривая мнение о том, что УК РФ не должен содержать определение «официального документа», видим необходимость в расширении перечня предмета преступлений, предусматривающих уголовно-правовую ответственность за подделку документов. Первым делом это касается введения в Кодекс понятия «электронный документ». Представляется, что изменения в УК РФ будут способствовать тому, что за совершение одних и тех же действий в отношении официальных документов, но на разных носителях информации (в данном случае речь идет об материальном и электронном носителях), виновные лица будут нести уголовную ответственность одинаково. Кроме того, это оздоровит обстановку на рынке дистанционных услуг и снизит риски при использовании электронного документооборота.

Особое внимание заслуживает вопрос о том, что представляет из себя официальный электронный документ.

Штаб О.Н. в своей работе приходит к выводу, что официальность электронного документа зависит от наличия определенных реквизитов, которые идентифицируют содержащуюся в нем информацию, прежде всего – наличия электронной подписи[3].

Законодательство в области информационного права определяет критерии, по которым можно определить официальность электронного документа.

---

[1] Определение Конституционного Суда Российской Федерации от 19 мая 2009 г. № 534-О-О. Доступ из справ-правовой системы «КонсультантПлюс».

[2] Определение Конституционного Суда Российской Федерации от 16 декабря 2010 г. № 1671-О-О. Доступ из справ-правовой системы «КонсультантПлюс».

[3] Штаб О. Н. Понятие официального документа в уголовном праве // Вестник МВД России. 2011. № 4. С. 13—20, С. 19.

Так, по ч. 4 ст. 11 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» «в целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами».

Статья 6 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» гласит, что информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью».

В соответствии ч. 5 ст. 9 Федерального закона от 6 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете» «первичный учетный документ составляется на бумажном носителе и (или) в виде электронного документа, подписанного электронной подписью».

Исходя из этого можно предположить, что одним из ключевых элементом признания электронного документа официальным является цифровая электронная подпись. Вместе с тем судебная практика не всегда соглашается с таким мнением.

Кассационным определением Седьмого кассационного суда общей юрисдикции от 14.04.2022 № 77-1702/2022 осталась без удовлетворения жалоба осужденной, утверждавшей о своей невиновности, ссылаясь на то, что документы, которые она изготовляла, не были подписаны электронной подписью, поэтому они не являются официальными.

Вопреки доводом кассационной жалобы, суд указал, что отсутствие в документах цифровой электронной подписи не исключает преступность действий так как электронный документ, который был вынесен подсудимой, по-

влек определенные правовые последствия, которые выразились в виде прекращения мер принудительного исполнения к должнику. Поэтому несмотря на отсутствие электронной подписи документ был признан официальным[1].

Привлекая виновное лицо к уголовной ответственности за подлог официальных электронных документов, на наш взгляд, прежде всего правоприменителю следует обращать внимание не на их форму, а на содержание. Официальный документ независимо от того представлен он в электронном или бумажном виде должен содержать информацию, которая имеет юридическую значимость. Это может включать установление прав или обязанностей, а также юридически значимых фактов. Электронная цифровая подпись должна выступать в качестве одного из способа проверки подлинности электронного документа и рассматриваться наравне с хэш-суммой, сертификатами для проверки подлинности идентификации отправителя, проверкой метаданных и т. д.

Некоторые авторы обращают внимание еще на одну проблему в сфере использования электронного документооборота, которая выражается в использовании поддельных QR-кодов[2]. Во время пандемии COVID-19 наблюдалось увеличение случаев продажи QR-кодов, связанных с требованием контроля и отслеживания в рамках мер по борьбе с распространением вируса. Совсем недавно Минцифры России презентовало проект правил предъявления «цифрового паспорта»[3]. Электронная версия документа представляет собой QR-код и

---

[1] Кассационное определение Седьмого кассационного суда общей юрисдикции от 14 апреля 2022 г. №77–1702/2022. Доступ из справ-правовой системы «КонсультантПлюс».

[2] Русскевич Е. А., Чернова К. Б. Цифровые аналоги официальных документов как предмет преступления: постановка проблемы // Вестник Московского университета МВД России. 2022. № 3. С. 231—235.

[3] Проект постановления Правительства Российской Федерации «О применении мобильного приложения федеральной государственной информационной системы “Единый портал государственных и муниципальных услуг (функций)” в целях представления гражданами Российской Федерации сведений, содержащихся в документах, удостоверяющих личность гражданина Российской Федерации, либо в иных документах, выданных гражданам Российской Федерации государственными органами Российской Федерации, и о внесении изменений в постановление Правительства Российской Федерации от 15 июня 2022 г. № 1067 “О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической систем”». Доступ из справ-правовой системы «КонсультантПлюс».

фотографию, в отдельные случаях при предъявлении потребуется получить одноразовый числовой пароль. Предъявить QR-код вместо бумажного паспорта можно будет в десятки категориях случаев, в том числе при покупке алкоголя и сигарет, установлении личности в финансовых организациях, заселении в гостиницу, посадки в поезд дальнего следования и т. д.

В этой связи возникает логичный вопрос: можно ли отнести QR-коды к документам в целом? Отвечая на этот вопрос, отметим, что QR-коды представляют собой двухмерные штрих-коды, которые содержат информацию и могут быть прочитаны с помощью мобильных устройств или сканеров. Сами по себе они не являются документами и не отвечают требованиям официальности. QR-коды могут быть использованы в официальных документах для различных целей: проверка подлинности, получение доступа к информации и т.д., однако сами по себе они не являются предметом преступлений о подлоге.

Ошибочным будет являться предположение о том, что использование поддельных QR-кодов не влечет никакую ответственность. Как правило, QR-коды позволяют переходить на конкретный источник информации, например, к числу которой может относиться сведения о вакцинировании. Соответственно, использование через QR-код сертификата о вакцинации, содержащего недостоверные реквизиты и сведения должно быть квалифицировано по соответствующей статьи УК РФ. Вместе с тем не будет являться подлогом документов использование поддельного QR-кода, не отсылающего к официальным документам, устанавливающим права и обязанности или юридические факты, поскольку как указывалось выше сам по себе QR-код не является документом. В данном случае лицо можно привлечь к административной ответственности, например, за невыполнения требований по санитарно-эпидемиологическому контролю (ст. 6.3 КоАП РФ).

Действия виновного лица, выражающиеся в использовании QR-кодов или цифровых сертификатов без разрешения их владельца могут быть квалифицированы как нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных

данных (ст. 13.11 КоАП РФ). Нарушение неприкосновенности частной жизни может повлечь уголовную ответственность в соответствии со статьей 137 УК РФ. Эта статья гарантирует защиту личной и семейной тайны, включая сведения о вакцинации, и нарушение ее может быть выражено в случае незаконного сбора или распространения информации.

Ответственности подлежит виновное лицо и в тех случаях, когда он осуществил копирование чужого QR-кода посредством незаконного получения доступа к чужому техническом устройству. Такие деяния необходимо квалифицировать по соответствующей части статьи 272 УК РФ.

Исходя из вышесказанного, мы приходим к тому, что на сегодняшний день УК РФ продолжает нуждаться в развитии и совершенствовании. Законодателю следует ввести в УК РФ понятие «электронный документ». Возможен и такой вариант, что данный термин, не теряя свое содержание будет называться в УК РФ иначе. Кроме того, на наш взгляд, в уголовном законе следует уделить внимание вопросу использования цифровой электронной подписи, QR-кодов, а также других, подлежащих использованию цифровых элементов электронных официальных документов.

УДК 343

Я. Р. ДАРШТ[1]

ПРОБЛЕМЫ КВАЛИФИКАЦИИ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ: ДОКСИНГ

В настоящее время наряду с программами-вымогателями, вирусами или фишингом нарастающие обороты набирает такая киберугроза, как доксинг. Термин «доксинг» возник в 90-е годы прошлого столетия и происходит от английского выражения «dropping dox» («сбрасывать документы»)[2]. Такое значение

[1] Научный руководитель — ВАСИЛЬЕВ Федор Юрьевич, доцент кафедры уголовного процесса Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент.

[2] Что такое доксинг? // SecurityLab : сайт. URL: https://www.securitylab.ru/ (дата обращения: 14.10.2023).

связано с местью хакеров, которые «сбрасывают» компрометирующую или закрытую информацию о жертве в сети «Интернет». Человека, который совершает доксинг, называют доксером[1].

В качестве примера доксинга можно привести ситуацию в 2022 году с Илоном Маском, который заблокировал аккаунты журналистов в Twitter и обвинил одного в отслеживании и опубликовании перемещений его самолета[2]. То есть мы видим вторжение в частную жизнь и возможную угрозу как самому лицу, так и его семье.

«Доксинг» — это свободное опубликование персональных данных в сети «Интернет», например, логины, пароли, адрес места жительства, личный кабинет налогоплательщика, госуслуг, различные фотографии, чаще всего интимного характера и т.д. Доксинг использует конфиденциальные данные в качестве оружия, сопровождающегося обвинениями, направленными на общественное унижение и оскорбление и на угрозу личной жизни, карьере и безопасности[3]. Побуждающим фактором могут выступать: личная обида, месть или прибыль. Конечно же, информация уже опубликована в социальных сетях. Но несмотря на то, что она в открытом доступе, ее использование без согласия в корыстных целях недопустимо. Жертвой может стать каждый пользователь, поэтому важно уберечь себя от подобного случая.

Такое явление относится к нацеливанию на людей путем злонамеренной публикации их личной информации, которая может включать:

1. Домашние адреса;
2. Данные о месте работы;
3. Номера личных телефонов;
4. Номера социального страхования;
5. Информацию о банковском счете и кредитных картах;

[1] Доксинг в 2022 году: неожиданно масштабная угроза кибербезопасности // SafeHome : сайт. URL: https://www.safehome.org/family-safety/doxxing (дата обращения: 08.10.2023).

[2] РБК Life : сайт. URL: https://www.rbc.ru/life/news/ (дата обращения: 14.10.2023).

[3] Федоров Р. В. Теоретико-правовые аспекты права на анонимность в сети «Интернет» / Юридический вестник ДГУ. 2022. Т. 44, №4. С. 34—42.

6. Детали личной переписки;

7. Личные фотографии и т.д.[1]

По данным организации «Лаборатория Касперского», более 43 млн американцев лично сталкивались с доксингом. Для России это тоже распространенное явление. Согласно опросу, который проводила «Лабораторий Касперского» в 2021 году, почти 20 % пользователей приложений для онлайн-знакомств становились жертвами доксинга. В 2020 году, опрос компании показал, что 64 % пользователей в России пытались удалить свои личные данные с сайтов или из социальных сетей. При этом пятая часть опрошенных заявляли, что находили в Сети информацию о себе или своих близких, которую не хотели бы видеть в открытом доступе[2].

Опасен доксинг как частным пользователям, так и организациям. Благодаря утечкам и развивающейся техники злоумышленники с легкостью находят информацию о сотрудниках и используют ее против них в целях финансовой выгоды.

Доксинг носит негативный характер, но его все равно не относят к незаконному деянию. В силу того, что правовая сфера не может полностью контролировать Интернет-пространство. Поскольку факты незаконного вторжения анонимны, цифровая конфиденциальность в полной мере не осуществима и чаще всего жертвы не сообщают об атаках властям. Это происходит по разным причинам:

1. Страх рассказать об информации, содержащей личный, интимный характер;

2. Разочарование во власти и в правовой защите;

3. Невозможно назвать своих злоумышленников, так как доксеры действуют анонимно.

[1] Что такое доксинг – определение и описание // Kaspersky : сайт. URL: https://www.kaspersky.ru/resource-center (дата обращения: 08.10.2023).

[2] Как личные данные попадают в Сеть и можно ли защитить себя от доксинга URL: https://trends.rbc.ru/ (дата обращения: 09.10.2023).

Стоит учесть и положительный феномен доксинга. Он также активно применяется при разоблачении лиц, совершающих административные и уголовные правонарушения. Журналисты тоже используют данную процедуру для поиска необходимых персональных данных об объекте исследования. Правда, в этом случае, это уже будет незаконный способ. Но в большинстве случаев доксинг представляет собой общественно опасное деяние, которое может повлечь отрицательные последствия и нанести вред человеку.

Проблема правовой защиты жертв доксеров заключается в ее отсутствии в действующем законодательстве. Можно только провести параллель к зафиксированным преступлениям в уголовном законодательстве РФ. Согласно главе 2 статьи 17 Конституции Российской Федерации «осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц».

То есть хакеры не вправе реализовывать свое право на свободу информации, нарушая чужое право на личную жизнь. Статья 21 говорит о том, что достоинство личности охраняется государством. Ничто не может быть основанием для его умаления. Далее статья 23 «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.». А в доксинге как раз и проявляются вторжение в личную жизнь, унижение человеческого достоинства – все то, что выходит за пределы допустимого. Статья 24 тому подтверждение: «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

Таким образом, доксинг — явное проявление нарушения законности. Да, мы можем принять факт, что сведения доксеры берут из социальных сетей, которые в открытом доступе. Казалось бы, это могли видеть и без их распространения, но информация используется в корыстных целях и без согласия пользователя.

Общие черты доксинга можно рассмотреть с вымогательством, закрепленного в статье 163 УК РФ. Только вымогательство имеет открытый характер, это действие напрямую в отличие от доксинга, который проходит анонимно, но цели их одинаковы.

В доксинг могут входить: мошенничество (ст. 159 УК РФ), кража (ст. 158 УК РФ), оскорбление (ст. 5.61 КоАП). Совершаются такие преступления через тайное хищение, в отдельных случаях, как и при мошенничестве путем обмана, но в целях последующего распространения по сети «Интернет». Касаемо административного правонарушения «Оскорбление» в доксинге при опубликовании чужих данных тоже прослеживается унижение чести и достоинства другого лица в неприличной форме и противоречащей нормам морали и нравственности.

Согласно ГК РФ ч. 1 ст. 152.1. «Охрана изображения гражданина» обнародование и дальнейшее использование фотографий человека возможно только с его согласия.

По Федеральному закону от 27. 07. 2006 №149 «Об информации, информационных технологиях и о защите информации» п. 2 ст. 17 «Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации».

Объект доксинга может включать в себя: человек, достоинство, честь, личная жизнь, личное имущество, личные сведения. В объективную сторону входит: использование конфиденциальных данных, позорящих потерпевшего, либо сведений, которые могут причинить существенный вред конституционным правам и свободам человека и гражданина, путем их распространения в сети «Интернет» без его согласия.

Субъектом доксинга является вменяемое физическое лицо, достигшее возраста уголовной ответственности. Субъективная сторона характеризуется

умышленной формой вины. Доксинг можно отнести к главе 19 УК РФ «Преступления против конституционных прав и свобод человека и гражданина» и квалифицировать как преступление небольшой тяжести, если оно не повлекло особо опасных последствий и материального ущерба в особо крупных размерах или не повлекло смерть человека.

Обобщая вышесказанное, подведем итог, что каждый гражданин может доксировать, собирать информацию из открытых источников, но при этом не используя ее в противоправных целях[1]. Нарушая это, осуществляется доксинг, то есть использование и опубликование персональных данных, позорящих потерпевшего, либо сведений, которые могут причинить существенный вред правам, здоровью, чести и достоинству потерпевшего путем их распространения в сети «Интернет» без его согласия.

УДК 343

А. Р. ДАУДОВА[2]

МЕСТО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННОМ УГОЛОВНОМ ПРАВЕ

В век современных технологий выражение «искусственный интеллект» закрепилось не только в науке, но и в правовом поле. В связи с этим есть ряд проблем, связанных с правовым регулированием искусственного интеллекта. В частности, они выражаются не только в отсутствии четкого толкования понятия «искусственный интеллект» но и в том, что отсутствуют определения непосредственно связанных с ним явлений, таких как: «носитель искусственного интеллекта», «интеллектуальный агент», «робот» и т. д.

[1] Романовская Е. А. Публично-правовые основы противодействия доксингу // Наука. Общество. Государство: электронный научный журнал. 2023. Т. 11, № 2. С. 72.

[2] Научный руководитель — АБДУЛАЗИЗОВА Патимат Гасановна, преподаватель кафедры государственно-правовых дисциплин Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук.

Так, изучив предлагаемые научной литературой понятия «искусственного интеллекта», мы определяем «искусственный интеллект» как «полностью или частично автономная самоорганизующаяся компьютерно-программная виртуальная или киберфизическая система, которая наделена определенным перечнем возможностей и программ и которая способна выполнять функции и решать задачи, в том числе специально не оговоренные в системе изначально, а также обучаться и адаптировать свое поведение под конкретные условия, в том числе и принимать решения исходя из этих условий и поставленных целей».

Актуальность исследуемой проблемы заключается тем, что искусственный интеллект оказывает влияние на многие сферы жизни, в том числе и на правовую деятельность человека, так как научные технологии постепенно проникают в правовую сферу жизни людей. Искусственный интеллект связан как с публичным, так и частным правом. Рассмотрим основные направления использования искусственного интеллекта в праве. В конституционном праве влияние искусственного интеллекта довольно неочевидно. Однако проникновение его в отдельные институты становится все более заметным.

Например, паспорт национальной программы «Цифровая экономика Российской Федерации» включает постепенную автоматизацию процесса нормотворчества и формирование концепции машиночитаемого права. Внедрение использования искусственного интеллекта в законотворческой деятельности уже происходит в некоторых странах. В административном праве процесс цифровизации идет достаточно давно. В РФ создана нормативная основа для организации деятельности органов публичной власти с использованием новых технологий для обмена и обработки информации (электронное правительство).

Появляются новые возможности для реализации полномочий государственных органов по вопросам безопасности, противодействию террористическим угрозам. В ближайшее время будут использоваться инструменты на основе искусственного интеллекта в налоговой сфере. Это позволит упростить

многие действия, например, обработку налоговых уведомлений, прогнозирование остатков по счетам и работу по уплате налогов. ФНС РФ уже начала внедрение данных механизмов.

Одним из направлений использования искусственного интеллекта в гражданском праве является совершение гражданско-правовых сделок. К тому же, его системы активно выступают объектами гражданских прав. Трудовое право также трансформируется под влиянием интеллектуальной автоматизации.

Активное применение роботов на рабочих местах, приведет к изменению некоторых норм, например, института рабочего времени и отдыха. Возможно внедрение искусственного интеллекта в судопроизводство. В частности, будет развиваться система работы с электронными доказательствами, с электронными делами и т.д. Более подробно хотелось бы рассмотреть всестороннее проникновение искусственного интеллекта в уголовное право. Отличительной особенностью искусственного интеллекта является то, что он предрасположен к самообучению. Но вместе с тем имеется такая проблема, как постепенно изменяющийся уровень самостоятельности искусственного интеллекта — от необходимости постоянного контроля со стороны человека до полной автономности, которая станет доступна в ближайшем или отдаленном будущем. С развитием технологий развивается и преступность: появляются новые способы совершения преступления, так если еще в 80-х гг. прошлого столетия никто и подумать не мог о таком составе преступления, как «мошенничество в сети «Интернет», то на сегодняшний день эти преступления на слуху у каждого.

В связи с этим считаем целесообразным определить место искусственного интеллекта в уголовном кодексе. Данная проблема является актуальной хотя бы потому, что в последнее время внедрение самообучаемых систем в повседневную жизнь человека порождает деяния, причиняющие вред охраняемым общественным отношениям. В частности, имеется в виду использование систем, оснащенных искусственным интеллектом, с помощью которых совершаются преступления и, собственно, причиняется вред общественным отношениям.

Актуальным является вопрос определения субъекта преступления, совершаемого с использованием систем искусственного интеллекта.

Можно выделить перечень возможных субъектов.

Во-первых, к ответственности может быть привлечен сам производитель искусственного интеллекта. Так, например, если смерть человеку была причинена вследствие нарушения правил дорожного движения управляемым беспилотным автомобилем, то ответственность должна быть возложена на разработчика программного обеспечения.

Во-вторых, к ответственности может быть привлечен продавец продукта, оснащенного искусственным интеллектом. При этом субъект должен заведомо знать о дефектах либо об опасности для жизни и здоровья при использовании данной продукции.

В-третьих, существует возможность привлечения к ответственности пользователя продукта, оснащенного искусственным интеллектом. В некоторых случаях автоматизированные процессы напрямую зависят от действий (бездействия), контроля со стороны пользователей. Поэтому ненадлежащая эксплуатация систем искусственного интеллекта может стать причиной преступного деяния.

И наконец, можно поставить вопрос о привлечении самого искусственного интеллекта к ответственности. Однако современные реалии таковы, что активность указанного субъекта связана с человеческим фактором и подчиняется его воле. Таким образом, в деянии искусственного интеллекта отсутствует субъективный признак состава преступления. В связи с вышеизложенным, считаем необходимым, предусмотреть уголовную ответственность за ненадлежащее создание программного обеспечения для систем с использованием искусственного интеллекта, а также за нарушение технологии их эксплуатации, в случае создания угрозы для жизни или здоровья людей либо причинения имущественного вреда.

Необходимо отметить, что целесообразным будет признать новое отягчающее обстоятельство — совершение преступления с использованием систем искусственного интеллекта. С другой стороны, использование искусственного

интеллекта открыло новые возможности для решения задач во многих сферах жизнедеятельности, в том числе и в расследовании преступлений.

Сегодня следователи применяют искусственный интеллект для поиска убийц и особо опасных преступников. Руководитель НИИ криминалистики Следственного комитета Российской Федерации Алексей Бессонов в своем интервью рассказал, что на текущий момент существует программа на основе технологии искусственного интеллекта, позволяющая строить наиболее вероятный портрет серийного преступника по совокупности признаков совершенных им насильственных преступлений[1].

Полученная информация позволяет следователю более эффективно организовывать расследование. Данная технология активно используется с 2021 г. Таким образом, в настоящее время количество преступлений с участием искусственного интеллекта довольно незначительно, однако его интенсивное совершенствование и использование может оказывать более существенное влияние на жизнедеятельность человека. Деятельность искусственного интеллекта может представлять угрозу охраняемым уголовным законом. Поэтому необходимо как можно раньше пересмотреть уголовно-правовые нормы, регулирующие данный вопрос.

УДК 343

О. В. ЗАЙЦЕВА[2]

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИЧНЫЕ ПРИЗЫВЫ К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

В последние годы наиболее актуальными становятся случаи распространения в сети «Интернет» материалов экстремистского характера, призывов к насильственным действиям по мотивам политической, расовой, религиозной ненависти или вражды.

[1] Интервью руководителя НИИ криминалистики СК России А. А. Бессонова информационному агентству ТАСС // Следственный комитет Российской Федерации : офиц. сайт. URL: https://sledcom.ru/press/interview/item/1621439/?print=1 (дата обращения: 13.10.2023).

[2] Научный руководитель – ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

Реалии развития уголовного законодательства и реализации превентивной деятельность в сфере преступлений экстремистской направленности сложны и противоречивы. С одной стороны, наблюдается закономерный рост преступности в данной сфере на фоне политической нестабильности, экономического кризиса и социальной напряженности. С другой стороны, очевидна цифровая трансформация преступности экстремистской направленности в условиях цифровизации общественной жизни: экстремизм, обывательски ассоциирующийся с несанкционированными протестами и иной идеологически мотивированной и запугивающей активностью, в современных условиях все чаще начинает выражаться в форме запрещенной к обороту информации экстремистского содержания.

Ответственность за публичные призывы к осуществлению экстремистской деятельности предусмотрена ст. 280 УК РФ. Совершение данного деяния с использованием сети «Интернет» выступает в качестве квалифицированного состава, представляющего собой повышенную степень общественной опасности.

Подобная законодательная конструкция обусловлена информатизацией и цифровизацией российского общества, его многонациональностью и многоконфессиональностью.

Объектом преступления, предусмотренного ч. 2 ст. 280 УК РФ, выступают общественные отношения, направленные на защиту основ конституционного строя и безопасности государства. Объективная сторона данного преступления выражается в осуществлении публичных призывов к осуществлению экстремистской деятельности с использованием средств массовой информации или информационно-телекоммуникационных сетей: размещение информации определенного содержания в сетевых изданиях, зарегистрированных в качестве электронных средств массовой информации в соответствии с Федеральным законом от 27 декабря 1991 года № 212401 «О средствах массовой информации[1], а также на интернет-сайтах, страницах в социальных сетях,

[1] О средствах массовой информации : Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 : текст с изм. и доп. на 13 июня 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

видеохостингах, блогерских страницах и форумах. Таким образом, в рамках уголовно-правового толкования, с учетом сложившейся судебной практики, термин «с использованием сети «Интернет» подлежит расширительному толкованию и «Интернет» понимается как любой электронный информационный источник. А.Ю. Алаторцев полагает, что подобная квалификация является избыточной и может оказывать влияние на вид и размер наказания, законодатель необоснованно приравнивает «Интернет» к средствам массовой информации, что расширяет сферу действия статьи 280 Уголовного кодекса Российской Федерации, поскольку не требует установления ни признака публичности, ни признака использования СМИ[1]. Представляется, что сложившаяся правоприменительная, в том числе судебная практика, обоснованно квалифицирует публичные призывы к осуществлению экстремисткой деятельности в социальных сетях, как совершенные с использованием сети «Интернет».

Представляется, что призывы к осуществлению экстремистской деятельности необходимо квалифицировать как совершенные с использованием сети «Интернет» и в том случае, когда они совершаются на закрытых форумах и страницах, даже при ограничении пользователем доступности к данному ресурсу, если число пользователей превышает двух лиц, которые владельцу ресурса неизвестны, также необходимо учитывать направленность умысла, действия владельца ресурса или страницы в социальных сетях, направленные на повышение числа просмотров, привлечение неограниченного круга лиц к размещаемой информации, выражение лицом своего желания побудить неограниченный круг лиц к совершению преступлений экстремистской направленности.

При квалификации публичных призывов к осуществлению экстремистской деятельности с использованием сети «Интернет» необходимо разграничивать составы преступлений, предусмотренных ч. 2 ст. 280 и ч. 2 ст. 280.1, п. «в» ч. 2 ст. 280.4 УК РФ.

[1] Алаторцев А. Ю. Новые разъяснения Пленума Верховного Суда об уголовной ответственности за экстремизм в интернете в контексте принципа правовой определенности // Уголовное право. 2017. № 2. С. 4—11.

Указанные преступления имеют одинаковый способ совершения – с использованием информационно-телекоммуникационных сетей, а также сети «Интернет», однако законодатель разграничивает данные составы по объективной стороне преступления, при этом положения статьи 280 Уголовного кодекса Российской Федерации выступают в качестве общей нормы по отношению к остальным. Представляется, что подобная законодательная конструкция может приводить к проблемам квалификации у правоприменителя.

Введение новых составов преступлений, предусмотренных ст. 280.3, 280.4 УК РФ, обусловлено сложившейся политической обстановкой в мировом пространстве. Анализируя систему норм, предусматривающих ответственность за публичные призывы к осуществлению экстремистской деятельности, наблюдается отсутствие единообразия законодательного регулирования.

Так, в ст. 280.3 УК РФ отсутствует квалифицирующий признак «с использованием средств массовой информации, либо электронных или с использованием информационно-телекоммуникационной сетей, в том числе «Интернет». Представляется, что в целях единообразия законодательного регулирования необходимо введение данного квалифицирующего признака, так как публичный призыв к осуществлению действий, указанных в ст. 280.3 УК РФ в настоящее время чаще совершается именно с использованием информационно-телекоммуникационных технологий.

Таким образом, законодательное регулирование уголовной ответственности за публичные призывы к осуществлению экстремистской деятельности с использованием сети «Интернет» требует совершенствования и приведения в единую систему. При квалификации данных преступлений правоприменителю следует обращать внимание на общественную опасность совершаемых призывов, с учетом наличия административной ответственности за подобные деяния, а также учитывать форму и содержание призывов к осуществлению экстремистской деятельности, действия самого лица, факт личного создания или заимствования размещаемой информации.

УДК 343

В. А. ЗАПЕВАЛОВА,
М. Ю. ПУХОВА[1]

ШАНТАЖ В СЕТИ «ИНТЕРНЕТ»: ПРОБЛЕМЫ РЕАЛИЗАЦИИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Социальные сети в настоящее время являются незаменимым инструментом общения благодаря их распространению, простоте и эффективности. Пользователи по всему миру используют социальные сети как инструмент социального взаимодействия, распространения новостей, игр, политической пропаганды и рекламы для повышения узнаваемости бренда и т. п. В то же время многие пользователи социальных сетей непреднамеренно раскрывают свою личную информацию, которая используется злонамеренными пользователями и третьими лицами[2].

Иными словами, при всей привлекательности человеческого общения онлайн в сети «Интернет» содержится множество «подводных» камней и поджидает опасность похуже, чем в Бермудском треугольнике. И речь не о мифических подводных чудищах, а вполне реальных людях, которые ради наживы способны дойти до остракизма и разрушения чужих жизней.

В этой статье пойдет речь о таком явлении, как шантаж преимущественно в социальных сетях, доступных в нашей стране, и будут рассмотрены проблемы выявления преступления в сети «Интернет» и их правильной квалификации.

Исследованием современных проблем противодействия киберпреступлениям против личности активно занимаются представители зарубежной и отечественной криминологической науки[3].

---

[1] Научный руководитель – КРАСНОВА Кристина Александровна, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

[2] Drury B., Drury S., Rahman M.A., Ullah I. (2022). A social network of crime: A review of the use of social networks for crime and the detection of crime. Online Social Networks and Media. 30. 100211. DOI: 10.1016/j.osnem.2022.100211.

[3] Антонян Е. А., Клещина Е. Н. Киберпреступность на современном этапе: тенденции и направления противодействия // Вестник экономической безопасности. 2022. № 5. URL: https://cyberleninka.ru/article/n/kiberprestupnost-na-sovremennom-etape-tendentsii-i-napravleniya-protivodeystviya (дата обращения: 01.11.2023) ; Никульченкова Е. В. Проблемы противодействия киберпреступности в России // Психопедагогика в правоохранительных органах. 2023. № 3 (94). С. 345—352.

Общим для перечисленных исследований является глобализация проблемы киберпреступности. Применительно к нашему исследованию представляют интерес научные публикации с особым акцентом на шантаж в социальных сетях.

Ключевым термином, который мы проанализируем является «шантаж» и формы его проявления в цифровой среде.

Под шантажом понимается одна из форм угрозы, ориентированная на создание обстановки, вынуждающей потерпевшего совершить выгодное виновному деяние[1].

С чего начинается шантаж? Во-первых, с поиска подходящей жертвы и платформы проведения всего действия[2]. И если ранее жертвами шантажа становились представительницы прекрасного пола[3], то на данный момент преступные взгляды обращаются в большинстве своем на мужчин.

Для примера возьмем популярную в нашей стране социальную сеть «ВКонтакте». В соответствующих тематических группах злоумышленники преимущественно ищут женатых мужчин с детьми с тем, чтобы такой «объект» шантажа впоследствии оказался «скован» собственной семьей и своим благополучным социальным статусом.

Далее идет создание подходящей страницы персоны, которая могла бы в теории его заинтересовать. В самом простом случае «страница» создается с нуля, то есть, проходит обычную регистрацию, в более продуманном же злоумышленники выкупают одну из «заброшенных страниц», бывшую когда-то активной. С помощью взаимодействия с алгоритмами социальной сети, фотографии бывших владельцев изменяются на те, которые хотел бы видеть преступник, сохранив дату и время публикации. Таким образом страница становится «живой», то есть ранее обладавшей соответствующей активностью.

---

[1] Ганченко О. И. Понятие шантажа в уголовном праве // Общество и право. 2011. № 5 (37). URL: https://cyberleninka.ru/article/n/ponyatie-shantazha-v-ugolovnom-prave (дата обращения: 01.11.2023).

[2] Я – девушка в интернете! #2 // YouTube. URL: https://www.youtube.com/watch?v=T0GirXiRGa0 (дата обращения: 30.10.2023).

[3] Срам себе режиссер: как шантажисты доводят девушек до суицида // Известия. 2019. 20 мая.

Необходимо отметить, что иногда за конкретным «злоумышленником» закрепляется целая группировка лиц. Ведь если сам злоумышленник – мужчина, ему нужно откуда-то брать фотографии, видеоматериалы и голосовые сообщения. Обычно их предоставляют девушки, состоящие «в доле», то есть имеющие свой процент с каждой жертвы.

Итак, ничего не подозревающая будущая жертва как обычно заходит в группу, посвященную, допустим, рыбалке. Стоит помнить, что каждый из нас оставляет так или иначе в социальных сетях «информационный след», который обычно представляет из себя упоминания, комментарии, участие в беседах. Именно по этому «следу» и идут преступники. Неожиданно на устройство среднестатистическому гражданину приходит оповещение о новом сообщении. Пишет ему очаровательная молодая девушка, якобы поступившая в то же высшее учебное заведение, что и он сам, но еще не определившаяся с тем, нравится ли ей учеба или нет.

Просьба от нее кажется вроде бы простой и не слишком замысловатой: рассказать о своем опыте студенчества, дальнейшем карьерном росте, основанном на соответствующем дипломе. Злоумышленники при общении с жертвой обычно пользуются, во-первых, эффектом внезапности, играющим на человеческом любопытстве, во-вторых, привлекательностью внешних данных «собеседницы». Слово за слово, завязывается ни к чему не обязывающая переписка, наполненная ностальгическими воспоминаниями жертвы и поддерживающими фразами злоумышленника. Так заканчивается первая фаза преступления, с которой жертва еще может уйти без последствий.

Вторая фаза более сложна для преступника, но вместе с тем результативность подобного «общения» тоже повышается. Играя на человеческом самолюбии, общение уходит в более личную сферу жизни. Обычно от «девушки» следуют сообщения, отмечающие мудрость и компетентность жертвы по первоначальному вопросу, что, конечно же, очень ей приятно. Комплименты незаметно для самого мужчины перетекают во взаимное русло, ведь не может же

собеседник не отметить красоту написавшей ему особы, не зря же злоумышленник перед этим скрупулезно выбирал и обрабатывал внешность «оболочки». Постепенно комплименты прекращаются, а «девушка» проявляет активность в дальнейшем общении, присылая жертве заранее заготовленные голосовые сообщения с обычными житейскими рассказами о своей жизни, заботах и проблемах. Таким образом укрепляется доверие, критическое мышление жертвы заметно снижается, выражаясь в ответных голосовых сообщениях или даже фотографиях. Тогда преступник и понимает: время третьей фазы, финальной и самой жестокой.

Выглядит она следующим образом: «девушка» тонко намекает на свою симпатию к собеседнику, прибегая к самым льстивым и стеснительным выражениям. Она выражает свое восхищение и робеет перед тем, кому пишет, девичьи чувства не дают ей покоя, но она готова положить на алтарь любви всю свою жизнь и репутацию, только бы получить хоть толику внимания от объекта своего воздыхания. Конечно же, наш читатель обратит внимание на то, что преступники в большинстве своем выбирают именно женатых мужчин, как и было сказано в начале статьи, неужели узы самого брака не удерживают от самой мысли о параллельных отношениях с другой девушкой, пусть и по сети «Интернет»? Подобным вопросом задаемся не только мы, исследователи данной проблемы, но и злоумышленники. Именно поэтому они и прибегают к самым изощренным психологическим манипуляциям, таким, что и самые достойные члены нашего общества, к сожалению, вступают на шаткую дорожку компрометирующего общения.

Если жертва все же оказалась «схвачена», критическое мышление у нее полностью заблокировано. Сообщения от собеседницы переходят в разряд интимных, страстных, в ход снова идут голосовые сообщения, через некоторое количество времени – фотографии. На экране своего устройства пользователь видит утонченный силуэт молодого обнаженного тела и просьбу прислать тоже «что-то интересное». И присылает, в ответ получая тишину или пару ничего не значащих фраз…

В это самое время преступник активно фотографирует всю переписку, включая подтверждающие доказательства ее подлинности. Неожиданно собеседнику приходит сообщение с раскрытием всех карт игры и прямой угрозой: если он не выплатит определенную сумму денег на конкретный виртуальный кошелек, скрины переписки разлетятся между всех его знакомых, друзей, а, главное, первой их получит жена и работодатель. Далее возможны два варианта развития событий.

В первом случае обычно растерянные и обманутые жертвы сразу же переводят средства, но иногда в них просыпается протест. В ответ они сами фиксируют переписку и конкретное сообщение с шантажом и идут в полицию писать заявление. Только на кого писать заявление? Сама страница – фейк, созданная личность – тоже, можно найти обладательницу снимков, но она может быть такой же невинной жертвой обмана. К тому же, внешность может быть сильно отредактированной в фотошопе, тогда найти по ней реальную девушку не представится возможным.

Второй вариант «противодействия» – заблокировать или скрыть свою страницу, но на этот случай у злоумышленника уже есть все необходимые данные для связи с ближайшим кругом общения жертвы. В случае блокировки злоумышленник сначала присылает переписку одному выбранному из списка, чаще всего ближайшему другу, который, конечно же, сообщит об этом жертве. Та же, поняв, что злоумышленник не собирается останавливаться, все же возвращается к первому варианту развития событий и пересылает деньги, надеясь забыть о произошедшем, как о страшном сне.

Прямого упоминания понятия «шантаж» в УК РФ нет, однако разумно соотнести его с определением «вымогательство» (ст. 163 УК РФ). Законодательство определяет его как «требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого иму-

щества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких».

Общение злоумышленника с жертвой может продолжаться в течение нескольких дней, а то и месяцев, отсюда возникает вопрос с определением времени совершения преступления. Анализ нормы ч. 1 ст. 163 УК РФ, сконструированного по типу формального, позволяет сделать вывод о том, что преступление считается оконченным, когда шантажист сформулировал требования и сообщил их, независимо от дальнейших действий пострадавшего: пойдет ли он на уступки или немедленно обратится в полицию.

Санкция в уголовном законе характеризуется относительной определенностью. Тогда при соответствии действий преступника ст. 163 УК РФ и отсутствии отягчающих обстоятельств, максимальное наказание будет заключаться в лишении свободы на срок до 4 лет с наложением штрафа в размере до 80 тыс. рублей. Однако, как упоминалось ранее, шантаж в сети «Интернет» часто совершается группой лиц по предварительному сговору (п. «а» ч. 2 ст. 163 УК РФ) либо организованной группой (п. «а» ч. 3 ст. 163 УК РФ), следовательно, и санкции становятся строже.

При этом, необходимо отметить, что число преступлений, связанных с шантажом в сети «Интернет», за последний год увеличилось на 10 % и составило 79 %, при этом раскрыть такую категорию дел очень сложно (раскрываемость составляет лишь 4 %)[1].

Препятствием для своевременного выявления подобных преступлений выступает анонимность преступников, то есть невозможность установить истинную личность и количество злоумышленников, скрывающихся за аккаунтом в сети «Интернет».

[1] Число IT-вымогательств выросло на 60 % – прокуратура // РАПСИ : Российское агентство правовой и судебной информации : сайт. URL: https://rapsinews.ru/digital_law_news/20230928/309257465.html (дата обращения: 01.11.2023).

Чтобы не стать жертвой шантажа, необходимо помнить, что хотя Интернет предлагает бесконечное множество возможностей для общения и обмена информацией, важно предпринимать возможные меры предосторожности: тщательно проверять личность собеседника, не делиться конкретикой личной жизни, прерывать переписку при возникновении подозрений и так далее.

Таким образом, в связи с быстрым развитием цифровых технологий и все большим уровнем использования сети «Интернет», безопасность в онлайн-пространстве становится все более важной проблемой. Преступники активно используют социальные сети для совершения различных преступлений, в том числе кражи личных данных, нарушения конфиденциальности и шантажа. Анонимность злоумышленников является основным препятствием на пути к раскрытию преступления.

Однако, законы, которые сейчас действуют, не всегда отвечают актуальным вызовам и проблемам в онлайн-мире. Необходим постоянный мониторинг и обновление законодательства, чтобы оно соответствовало последним технологическим тенденциям.

Одним из таких обновлений может стать добавление в ст. 163 УК РФ квалифицирующего признака, который характеризовал бы существенные аспекты такого преступления, как шантаж в сети «Интернет». Как говорилось ранее, злоумышленник предпринимает попытки добиться расположения своей жертвы, чтобы получить желаемую информацию и средство шантажа, что является одной из форм психологического воздействия, однако недостаточно охватывается этим термином. Наиболее уместным в данном случае будет выделение такого квалифицирующего признака, как осуществление манипулятивных действия, с целью получения доверия.

Расширение компетенций правоохранительных органов и судов в области борьбы с шантажом в сети «Интернет» может стать неплохим преобразованием и решить ряд насущных проблем. Например, предоставить более широкий доступ к личным данным и информации о пользователях, которые осуществляют шантаж.

Еще одним решением может стать разработка и совершенствование технических решений для предотвращения и обнаружения шантажа в интернете. Это может включать разработку алгоритмов и программного обеспечения для распознавания и блокировки шантажных сообщений или угроз.

Таким образом, социальные сети являются неотъемлемой частью нашей современной жизни, но без должной защиты мы оказываемся под угрозой киберпреступлений. Поэтому явное понимание важности безопасности в онлайн пространстве и принятие соответствующих мер защиты являются необходимыми для сохранения конфиденциальной информации.

УДК 343

Е. А. ЗУЕВА[1]

НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ДОВЕДЕНИЕ ДО САМОУБИЙСТВА, СОВЕРШЕННОЕ В ПУБЛИЧНОМ ВЫСТУПЛЕНИИ, ПУБЛИЧНО ДЕМОНСТРИРУЮЩЕМСЯ ПРОИЗВЕДЕНИИ, СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

Россия в 2022 году заняла девятое место в мире по количеству самоубийств[2]. По данным Федеральной службы государственной статистики Российской Федерации в 2019 году в результате акта суицида погибло 16 983 человек, в 2020 году – 16 546, в 2021 – 15 615[3]. Одним из факторов, подталкивающих людей к лишению себя жизни, становятся новые технологии, уверенно закрепившиеся в жизни каждого. Уже трудно представить наш мир без средств массовой информации и «Интернета», но они несут с собой и негативные последствия. Одинокие, психологически неустойчивые, несовершеннолетние

[1] Научный руководитель — КРАЕВ Денис Юрьевич, профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

[2] Самоубийства в России в 2023 году // Сайт об отличиях и различиях : сайт. URL: https://aarr.ru/samoubijstva-v-rossii-v-2022-godu/ (дата обращения: 26.10.2023).

[3] Федеральная служба государственной статистики Российской Федерации : офиц. сайт. URL: https://rosstat.gov.ru/folder/12781 (дата обращения: 24.10.2023).

лица подвергаются воздействию «групп смерти», «кибербуллингу», и для некоторых это влияние становится фатальным.

В 2019 году было осуждено по предъявленному прокурором обвинению по статье 110 УК РФ 19 лиц, в 2020 году – 6, в 2021 году – 13, в 2022 году – 13[1]. Принимая во внимание приведенные официальные данные, можно сделать вывод о том, что несмотря на чрезвычайную распространенность самоубийств, только незначительная их часть совершается из-за преступного воздействия на потерпевшего – примерно из тысячи самоубийств лишь одно совершается вследствие доведения.

На практике правовая норма, закрепленная в ст. 110 УК РФ, не получила широкого распространения, что обусловлено трудностью раскрытия и расследования преступлений данного вида, а также отсутствием единообразия в квалификации рассматриваемого деяния, по этим причинам состав доведения до самоубийства остается недостаточно изученным.

В статье мы уделим внимание проблемным аспектам квалифицированного состава доведения до самоубийства, предусмотренного п. «д» ч. 2 ст. 110 УК РФ.

Данный пункт появился в уголовном законе в 2017 году. Введение указанного признака было обусловлено повышенной степенью общественной опасности доведения до самоубийства, совершенного в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), ввиду публичного и глобального характера (распространения неограниченному кругу лиц), а также относительной анонимности субъекта (использования псевдонимов, «фейковых» аккаунтов).

Остановимся на совершении доведении до самоубийства с помощью средств массовой информации.

[1] Судебная статистика РФ / Агентство правовой информации : сайт. URL: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения: 24.10.2023).

Под средствами массовой информации, в соответствии со ст. 2 Закона Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации», понимаются «периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием (названием)»[1].

Данный закон допускает регистрацию сайта в информационно-телекоммуникационной сети «Интернет» в качестве средств массовой информации.

В таком случае встает вполне логичный вопрос: как следует квалифицировать доведение до самоубийства, совершенное с помощью интернет-сайта, имеющего статус средств массовой информации?

В приведенной ситуации невозможно применить правило квалификации при конкуренции специальных норм, предусматривающих квалифицированные составы, так как оба квалифицированных признака прописаны в одном и том же пункте одной статьи. Однако сделать выбор чему отдать предпочтение придется, ведь п. «д» ч. 2 ст. 110 УК РФ сконструирован таким образом, что между «средствами массовой информации» и «информационно-телекоммуникационной сетью (включая сеть «Интернет»)» стоит разделительный союз «или», не позволяющий вменить вышеуказанные признаки единовременно. Правильным видится использовать правило квалификации при конкуренции части и целого, которое предписывает использовать норму целого с наибольшей полнотой, охватывающей содеянное. В нашем случае в качестве такой нормы выступает норма, закрепляющая ответственность за доведение до самоубийства, совершенное в средствах массовой информации.

Данной квалификации есть вполне житейское объяснение, информационно-телекоммуникационная сеть «Интернет» включает в себя множество

[1] О средствах массовой информации : Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 : текст с изм. и доп. на 13 июня 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

различных источников информации и лишь некоторые из них зарегистрированы в качестве средств массовой информации.

Из вышеизложенного следует еще один проблемный момент, как квалифицировать деяние, если доведение до самоубийства, совершено через сайт в «Интернете», обладающий всеми признаками средств массовой информации, но в качестве такового не зарегистрированный?

На данный вопрос поможет дать ответ абз. 5 п. 6 Постановления Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. № 16, в соответствии с которым «лица, допустившие нарушения законодательства при распространении массовой информации через сайты в сети «Интернет», не зарегистрированные в качестве средств массовой информации, несут уголовную, административную, гражданско-правовую и иную ответственность в соответствии с законодательством Российской Федерации без учета особенностей, предусмотренных законодательством о средствах массовой информации»[1]. Следовательно, деяние будет квалифицироваться как доведение до самоубийства, совершенное в информационно-телекоммуникационной сети «Интернет».

Согласно п. 4 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники[2].

Наиболее распространенной и общедоступной является информационно-телекоммуникационная сеть «Интернет», помимо нее существуют и другие сети, различных уровней (от глобальных до локальных).

---

[1] О практике применения судами Закона Российской Федерации «О средствах массовой информации» : Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. № 16 : текст с изм. и доп. на 9 февр. 2012 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об информации, информационных технологиях и о защите информации : Федерального закона от 27 июля 2006 г. № 149-ФЗ: текст с изм. и доп. на 2 нояб. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

Шесть лет назад активизировали свою деятельность так называемые «группы смерти» – сообщества, пропагандирующие и призывающие к совершению актов суицида. Наибольшую известность получили «Синий кит», «Тихий дом», «Фея огня», «Беги или умри». Для соответствующей уголовно-правовой оценки их деятельности в уголовный закон были введены статьи 110.1 и 110.2 УК РФ.

Как верно отмечает Председатель Следственного комитета Российской Федерации А. И. Бастрыкин, объектом противоправных действий руководителей «групп смерти» являются общественные отношения, охраняющие не только жизнь и здоровья человека, но и общественную нравственность, так как влияние этих сообществ распространяется не только на конкретную жертву, но и на неопределенное количество людей.

В силу того, что ранее названные объекты охраняются не только главой 16, но и главой 25 УК РФ, ученый рекомендует квалифицировать деяние руководителей «групп смерти» по совокупности преступлений, в которую будет входить ст. 239 УК РФ, закрепляющая ответственность за создание некоммерческой организации, посягающей на личность и права граждан[1].

По мнению А.И. Бастрыкина, даже если организация не имеет государственной регистрации, это не мешает применению ст. 239 УК РФ, ввиду того, что ст. 18 Федерального закона от 19 мая 1995 г. № 82-ФЗ «Об общественных объединениях» позволяет общественным объединениям осуществлять свою деятельность без государственной регистрации в качестве юридического лица[2].

Стоит отметить, что члены «групп смерти», действуя через сеть «Интернет», оказывают влияние на жертв в основном такими предусмотренными

[1] Бастрыкин А. И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. Т. 11, № 1. С. 9.

[2] Об общественных объединениях : Федеральный закон от 19 мая 1995 г. № 82-ФЗ : текст с изм. и доп. на 24 июля 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

в ч. 1 и ч. 2 ст. 110.1 УК РФ способами, как уговоры, предложения, советы, указания, а значит их действия должны квалифицироваться по п. «д» ч. 3 ст. 110.1 УК РФ. Однако, деяние, начатое как склонение к совершению самоубийства или содействие совершению самоубийства, может перерасти в доведение до самоубийства.

Например, если лицу начинают высказываться угрозы (обещая причинить вред близким или распространить порочащие личность сведения), систематически унижают его человеческое достоинство (оскорбляя, подвергая травле, притворяя в жизнь обещание о распространении клеветы). Подобные действия должны найти отражение в квалификации по п. «д» ч. 2 ст. 110 УК РФ.

Еще одним способом доведения до самоубийства в сети «Интернет» является «кибербуллинг», который выступает формой электронного или онлайн-буллинга, когда лицо или группа лиц целенаправленно оскорбляют и унижают других, тем самым причиняя им психологический вред[1]. Анализ открытых источников показывает, что киберзапугивание может выражаться в высмеивании, унижении, оскорблении, издевательстве, психологическом давлении, распространении информации о частной жизни, компрометирующих материалов, фото-, видеомонтажей и др.

Приведем пример доведения до самоубийства посредством «кибербуллинга». Так, в 2015 году несовершеннолетняя вступила в переписку с неизвестным мужчиной в социальной сети «ВКонтакте». В ходе общения по просьбе незнакомца девочка прислала фотографии интимного характера. Данная пара также созванивалась по видеозвонку в «Skype», где девочка демонстрировала обнаженные части своего тела. Однако, осознав неправильность своих действий, несовершеннолетняя предприняла попытку прервать общение, заблокировав аккаунт неизвестного мужчины и удалив свою страницу.

[1] Бобровникова Н. С. Кибербуллинг: виды и особенности проявления // Международный научно-исследовательский журнал. 2022. № 11 (125). С. 1—4.

Через несколько лет, в мае 2017 г. тот же мужчина снова отправил сообщение несовершеннолетней в социальной сети «ВКонтакте» с предложением продолжить интимное общение, в противном случае пообещав обнародовать компрометирующие ее материалы, сделанные раннее. Несовершеннолетняя, воспринимая угрозы реально, предприняла попытку акта суицида путем медикаментозного отравления, но самоубийство ей не удалось довести до конца по независящим от нее обстоятельствам, ввиду своевременной помощи врачей. По обращению матери потерпевшей УМВД г. Тюмени было возбуждено уголовное дело по ст. 110 УК РФ[1]. С учетом изложенного деяние мужчины необходимо квалифицировать по пп. «а», «д» ч. 2 ст. 110 УК РФ, как доведение лица до покушения на самоубийство путем угроз, совершенное в отношении несовершеннолетнего в информационно-телекоммуникационной сети «Интернет».

В заключении следует отметить, что в доктрине уголовного права существует множество вопросов квалификации доведения до самоубийства, часть из которых была рассмотрена в настоящей работе. Выявленные проблемы нуждаются в дальнейшем изучении и анализе с целью поиска научно-обоснованных путей их решения. На наш взгляд, одним из вариантов преодоления этих проблем может выступать издание специального Постановления Пленума Верховного Суда Российской Федерации, посвященного разъяснению спорных вопросов, связанных с доведением до самоубийства и смежными с ним составами преступлений.

[1] Шарапов Р. Д., Смахтин Е. В. Новые основания уголовной ответственности за вовлечение в самоубийство и иное опасное для жизни поведение // Всероссийский криминологический журнал. 2018. № 3. С. 350.

УДК 343

Д. М. ЗУЕНКО[1]

НЕКОТОРЫЕ АСПЕКТЫ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В НЕЗАКОННЫЙ ОБОРОТ НАРКОТИЧЕСКИХ И ПСИХОТРОПНЫХ ВЕЩЕСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Одной из самых серьезных проблем, связанных с незаконным оборотом наркотических и психотропных веществ, является вовлечение в совершение связанных с ним преступлений несовершеннолетних. Изучению этой проблемы уделено достаточно внимания отечественных исследователей, однако, малоизученным остается вопрос использования для этих целей современных информационно-телекоммуникационных технологий.

В целях профилактики преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ или их аналогов, Указом Президента Российской Федерации от 23 ноября 2020 г. № 733 утверждена Национальная антинаркотическая стратегия Российской Федерации до 2030 г. В ней указан перечень угроз национальной безопасности в сфере оборота наркотиков, в числе которых отмечается масштабное использование сети «Интернет» для пропаганды незаконного потребления наркотиков[2].

По данным анонимного опроса, проведенного Кузиной Л.С., 144 сотрудников подразделений по контролю по обороту наркотиков из 23 регионов и 242 сотрудников подразделений по делам несовершеннолетних МВД РФ в 30 регионах, 91 % сотрудников по контролю за оборотом наркотиков и 89 %

[1] Научный руководитель — КРЮЧКОВ Роман Олегович, доцент кафедры уголовно-правовых дисциплин Крымского юридического института (филиала) Университета прокуратуры Российской Федерации.

[2] Стратегия государственной антинаркотической политики России до 2030 года : утв. Указом Президентом Российской Федерации от 23 ноября 2020 г. № 733. Доступ из справ.-правовой системы «КонсультантПлюс».

сотрудников подразделений по делам несовершеннолетних МВД России заявили, что им неизвестно реальное количество преступлений, связанных с незаконном наркотических и психотропных веществ, совершаемых с участием несовершеннолетних. Из этого автор исследования делает вывод, что количество незарегистрированных преступлений в данной сфере превышает число выявленных[1].

Увеличение количества несовершеннолетних, вовлекаемых через сети «Интернет» в преступную деятельность, связанную с незаконным оборотом наркотических и психотропных веществ, обусловлена рядом причин.

Во-первых, вовлечению несовершеннолетних в распространение наркотических и психотропных веществ способствует легкий доступ к информации, обеспечиваемый современными информационно-телекоммуникационными технологиями. Этот доступ позволяет получить необходимую информацию о наркотиках, их видах, эффектах и способах употребления на различных интернет-ресурсах, форумах и социальных сетях.

Во-вторых, на некоторых скрытых площадках интернета (например, darknet) продажа наркотических и психотропных веществ происходит с использованием криптовалют, чем обеспечивается анонимность и конфиденциальность. Так, Darknet, которым ежедневно пользуется около 400 тыс. россиян и охватывающий более 1 тыс. российских городов, имеет VPN-шифрование для всех пользователей по всему миру, что делает практически невозможным вычисление IP-адресов и персональных данных[2].

---

[1] Кузина Л. С. «Сетевой наркомаркетинг» как один из факторов вовлечения несовершеннолетних в сети «Интернет» // Вестник Воронежского института МВД России. 2020. № 4. С. 285—290.

[2] Фарахиева Г. Р. Влияние интернет-пространства на процессы вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов // Вестник Саратовской Государственной Юридической Академии. 2021. № 5 (142). С. 182—191.

В-третьих, поступающие к несовершеннолетним через мессенджеры «привлекательные» предложения о «выгодной работе» или «легком заработке» способствуют все большему вовлечению в незаконный оборот наркотических и психотропных средств, нуждающихся в деньгах и быстром заработке несовершеннолетних.

Для вовлечения несовершеннолетних в совершение исследуемую группу преступлений используются всевозможные способы. Однако начинается «диалог», как правило, в игровой форме, которая более всего привлекает потенциальную жертву. Молодые люди воспринимают такое поведение как приключение, своего рода «квест». Например, несовершеннолетние платят определенную сумму денег или предоставляют паспортные данные, чтобы принять участие в «игре» или «квесте». Затем они приходят в одно место, берут «закладку» с наркотиком, идут в другое указанное место (например, телефонную будку) и оставляют ее там. В день несовершеннолетний может сделать 10–15 таких «закладок». За каждую такую «закладку» подросток получает деньги. В так называемой игре есть еще один участник («мастер-клад»), который контролирует весь процесс преступной деятельности «закладчика», а также предоставляет наркотики для продажи. Когда несовершеннолетний предлагает выйти из так называемой игры, используются методы психологического воздействия. Организаторы напоминают несовершеннолетнему его паспортные данные, место жительства, сведения о родственниках, и в случае необходимости, могут с ними связаться[1].

Следует отметить, что вовлечение несовершеннолетних в деятельность, связанную с незаконным оборотом наркотических и психотропных веществ, осуществляется не только через закрытые сети типа Darknet. Любые социальные сети, мессенджеры и открытые онлайн-площадки («ВКонтакте», Одноклассники и другие, мессенджеры и др.) создавая благоприятные условия анонимности, играют значительную роль в этом процессе.

[1] Кузина Л. С. Незаконный оборот наркотиков в сети «Интернет» // Вестник Воронежского института МВД России. 2020. № 2. С. 323—328.

Например, в мессенджере Telegram происходит распространение психотропных и наркотических веществ и вовлечение несовершеннолетних в оборот посредством рассылки пользователям информации о предложении выгодной работы «курьером», а также с предложением по выгодным ценам приобрести известный товар, с гарантированной конфиденциальностью и безопасностью сделки. В связи с этой и иной противоправной деятельностью по данным Роскомнадзора было заблокировано 4 179 страниц пользователей и каналов мессенджера Telegram, а также 10 498 специализированных сайтов[1].

Вовлеченных несовершеннолетних условно можно подразделить на две категории. К первой относятся лица, которых вовлекли с целью расширения клиентской базы. У таких лиц возникает устойчивое желание употреблять наркотические средства. Ребенок из-за приобретенной зависимости и отсутствием в силу своего возраста денег вынужден участвовать в незаконном обороте запрещенных веществ для получения новой дозы наркотических веществ. Наиболее распространяемыми веществами в сети «Интернет» среди несовершеннолетних являются снюс, экстази, амфетамин, кокаин, мефедрон, соли, ЛСД и другие.

Ко второй категории относятся несовершеннолетние, которые принимают участие лишь в организации преступного наркооборота. Наркотические вещества они не употребляют. У них присутствует лишь материальная заинтересованность.

Особые опасения вызывает то, что несовершеннолетние, участвуя в такой преступной деятельности, активно вовлекают в нее своих сверстников.

В заключении следует отметить, что более широкое использование новейших информационно-телекоммуникационных технологий для вовлечения несовершеннолетних в преступления в сфере незаконного оборота наркоти-

[1] Роскомнадзор удалил 85 тысяч материалов с пропагандой наркотиков / РИА Новости : сайт. URL: https://ria.ru/20211101/roskomnadzor-1757181150.html (дата обращения: 07.11.2023).

ческих и психотропных веществ, обусловливает необходимость поиска новых способов их предупреждения. Очевидной становится необходимость выработки эффективной стратегии противодействия распространению наркотиков с использованием современных технологий.

Представляется, необходимым поиск четкого алгоритма действий при выявлении интернет-магазинов и площадок, предлагающих незаконные услуги в сфере незаконного оборота наркотиков. Боле того, речь идет не только об их закрытии (поскольку на их месте появляются новые), а о выявлении их конечных бенефициаров и привлечении их уголовной ответственности, в том числе и за вовлечение несовершеннолетних в совершение преступлений. При этом за вовлечение в незаконный оборот наркотических и психотропных веществ ответственность должна быть значительно ужесточена.

УДК 343

И. А. ИВАШИНА[1]

О НЕКОТОРЫХ КРИМИНАЛИСТИЧЕСКИХ АСПЕКТАХ РАССЛЕДОВАНИЯ НЕЗАКОННОГО ОБОРОТА ОРУЖИЯ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Незаконный оборот оружия признан одной из основных и острых социальных проблем в Российской Федерации, поскольку несет в себе угрозу национальной безопасности государства, обществу и безопасности личности.

Статистика показывает, что за 2021 год количество зарегистрированных преступлений в сфере незаконного оборота оружия составило 23 507, из них 8 502 уголовных дел были направлены в суд с обвинительным заключением (обвинительным актом, обвинительным постановлением)[2].

[1] Научный руководитель — ШЕВЕЛЕВА Ксения Владимировна, старший преподаватель кафедры «Правовое обеспечение национальной безопасности» Института кибербезопасности и цифровых технологий Российского технологического университета – МИРЭА.

[2] Сводный отчет по России «единый отчет о преступности» за январь–декабрь 2021 г.

По итогам 2022 года наблюдается сокращение количества подобных преступлений на 5,5 % (до 22 206). Однако следует обратить внимание на увеличение фактов хищения, вымогательства оружия, боеприпасов, взрывчатых веществ и взрывных устройств с 779 до 844[1].

Нам видится, что в данном случае, снижение вызвано повсеместным использованием различных технологий для совершения преступлений, что существенно затрудняет их выявление.

Так, количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий в 2021 году составило 517 722, в то время как в 2022 году было зарегистрировано 522 065 преступлений, из которых 381 112 (за 2021 год – 351 463) преступлений совершены с применением сети «Интернет», 212 963 (за 2021 год – 217 552) – средств мобильной связи[2].

Сеть «Интернет» в качестве средства совершения преступления привлекательна для преступника ввиду неограниченных возможностей сокрытия личности, трансграничного характера использования, удобства и др.

В свою очередь, вышеназванное усложняет процесс расследования преступлений, совершенных посредством сети в сфере незаконного оборота оружия, боеприпасов, взрывчатых веществ и взрывных устройств, выявление лиц, участвующих в преступных сделках.

С точки зрения криминалистики, при разработке частной криминалистической методики расследования отдельного вида преступления, следует пользоваться базисной информацией о преступлении, которая, традиционно, заключена в криминалистической характеристике преступления.

Р.С. Белкин выделяет в качестве элементов криминалистической характеристики преступления способ совершения преступления, орудие соверше-

[1] Сводный отчет по России «единый отчет о преступности» за январь–декабрь 2021 г.

[2] Сведения о состоянии преступности в Российской Федерации // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/37377025/ (дата обращения: 17.04.2023).

ния преступления, информация о личности преступника и потерпевшего, типичная следовая картина преступления, данные об обстановке совершенного преступления[1].

Рассмотрим некоторые отдельные элементы криминалистической характеристики незаконного оборота оружия, совершенного посредством сети «Интернет».

Личность преступника играет довольно значимую роль в совершении определенного рода преступлений. Благодаря знаниям о личности предполагаемого преступника, можно выявить его особые способы в совершении преступлений, в частности, связанных с незаконным оборотом оружия, боеприпасов, взрывчатых веществ и взрывных устройств с использованием сети «Интернет».

Согласно отчету Судебного Департамента при Верховном Суде Российской Федерации о демографических признаках осужденных по всем составам преступлений УК РФ за 12 месяцев 2021 года уровень образования осужденных в категории преступлений в сфере незаконного оборота оружия следующий: лица, имеющие высшее образование – 15 %, среднее и средне специальное образование – 60 %[2].

Наличие у преступника в сфере незаконного оборота оружия образования играет важную роль, так как лицо, обладая профессиональными навыками в сфере технического устройства и конструирования оружия, способно самостоятельно изготовить предметы вооружения и использовать их в качестве орудия преступления[3], а также иметь цель их сбыта.

---

[1] Белкин Р. С. Курс криминалистики. Общая теория криминалистики. В 3 т. Т. 1. М., 1997. 408 с.

[2]. Отчет о демографических признаках осужденных по всем составам преступлений Уголовного кодекса Российской Федерации за 12 месяцев 2021 г. Форма № 11.1 // Судебный Департамент при Верховном Суде Российской Федерации : офиц. сайт. http://cdep.ru/?ref=w3use.com (дата обращения: 12.10.2023).

[3] Егорова Т. И., Курбатова Г. В. Криминологическая характеристика и предупреждение незаконного оборота оружия в России // Известия ТулГУ. Экономические и юридические науки. 2022. № 3. С. 77—84.

Наличие у преступника знаний, умений и навыков в сфере IT-технологий позволяет ему свободно использовать технические устройства и Интернет-пространство для поиска клиентов, публикации товаров, покупки оружия, боеприпасов, взрывчатых веществ или взрывных устройств с целью их перепродажи, не боясь быть пойманным сотрудниками правоохранительных органов, так как доступ к неподконтрольным властям Интернет-ресурсам чаще всего затруднен или невозможен.

Помимо обладания определенными знаниями у преступников должны быть специальные средства, благодаря которым совершаются преступные деяния. Для этого используются различного вида телефоны, планшеты, ноутбуки и иные технические средства. Они обеспечивают анонимность и затрудняют поиск лиц, совершивших преступные деяния, правоохранительными органами, так как часто данные средства либо зарегистрированы на подставное лицо, либо преступник имеет более двух предметов, с помощью которых осуществляет незаконный оборот оружия, боеприпасов, взрывных устройств и взрывчатых веществ.

Специфика предметов посягательства требует достаточно высокий уровень организации деятельности в сфере незаконного «бизнеса оружия». Это приводит к тому, что отдельные преступники объединяются в организованные преступные группы. Это позволяет им повысить уровень организации их преступной деятельности в сфере незаконного оборота оружия, так как подобные группировки обладают иерархической структурой, в которой действует вертикальная подчиненность, требующая строгого распределения обязанностей. Подобная организация позволяет заниматься преступным бизнесом длительное время, оказывая при этом противодействие правоохранительным органам.

В результате, при расследовании преступлений, связанных с незаконным оборотом оружия с использованием сети «Интернет», следственным органам необходимо учитывать, что за лицом «продавца товара» может скрываться целая преступная группа, имеющая доступ к оружию, боеприпасам, взрывным устройствам и взрывчатым веществам.

Развитие сети «Интернет» в сфере преступной деятельности открыло преступникам возможность участвовать в незаконной онлайн-торговле оружием, используя модель «преступление как услуга» в качестве ключевого канала распространения. Эта модель оказывает сильное влияние на незаконный оборот оружия, поскольку снижает планку доступа к информации о производстве оружия и к незаконному оружию неопытным субъектам[1]. Это важно учитывать при составлении портрета подозреваемого, так как этот канал распространения обеспечивает более легкий доступ к незаконному оружию, боеприпасам, взрывчатых веществ и взрывных устройств лицам без криминального прошлого, а также лицам, занимающихся несколькими видами преступной деятельности[2].

Благодаря Интернет-ресурсам появилось множество торговых площадок для незаконной торговли. Самой распространенной из них среди большинства преступных предпринимателей является сервис DarkNet, однако, оборот товара через него, как по объему, так и по стоимости довольно ограничен из-за существующих конкретных требований к инфраструктуре и услугам, являющимися основой для этого вида торговли. В связи с чем, преступники используют менее технологичные средства для реализации своей деятельности, не применяя различные рынки «темной» части сети «Интернет». Например, предложения о продаже оружия, макетов его изготовления, отдельных частей, боеприпасов, взрывчатых веществ и взрывных устройств можно встретить в профилях социальных сетей и мессенджерах. Используются также различные интернет-форумы, а доставка товара покупателю производится с помощью почтовых услуг.

Расследование незаконного оборота оружия посредством сети «Интернет» имеет особые специфичные черты, одной из них является получение

[1] Серия университетских модулей «Модуль 4. Незаконный рынок огнестрельного оружия» 2019 // Управление Организации Объединенных Наций по наркотикам и преступности : сайт. URL: https:// https://www.unodc.org/documents/e4j/Firearms/Module_04_-_The_Illicit_Market_in_Firearms_final_rus.pdf (дата обращения: 18.09.2023).

[2] Там же.

первичной информации о факте преступления. Такая информация может быть получена как от конфиденциальных источников информирования органов ОВД, так и посредством их сотрудничества с иными правоохранительными службами, получающих такую информацию в ходе исполнения своих прямых обязанностей. Применяется также мониторинг тематических сайтов и форумов, различных торговых интернет-площадок, однако, данный метод неэффективен, так как является длительным и труднозатратным.

Важным шагом в расследовании преступления, связанного в сфере незаконного оборота оружия, является обнаружение устройств, с которых совершались противоправные действия – телефоны, планшеты, ноутбуки и т. д.

Однако сложность на этом этапе расследования состоит в том, что для преступника в сети «Интернет» важна анонимность, которая позволяет отделить его преступные действия и деятельность от его настоящей личности. Для этого лицо, совершающее незаконный сбыт оружия использует такие ресурсы, как Tor, Dedicated-серверы, VPN-серверы, позволяющее ему скрываться от правоохранительных органов.

Определения IP-адреса устройства (которое является уникальным и позволяет отследить месторасположение абонента) является первоочередной задачей для следственной группы.

После того, как установлен IP-адрес технического устройства, необходимо его изъять и произвести осмотр. Для этих целей целесообразно привлечь специалистов в сфере информационно-телекоммуникационных сетей и сети «Интернет» для изучения устройств, электронных носителей информации, сайтов и иных ресурсов, использующихся для совершения незаконных сделок с продажей, покупкой, передачей, хранением оружия.

Проверка устройств происходит с помощью компьютерно-технических экспертиз (программно-компьютерная, информационно-компьютерная, компьютерно-сетевая), также возможно привлечение переводчиков, в том случае, если покупка была совершена с иностранного сайта.

Получив доступ к информации устройства, с помощью которого были совершены противоправные действия, связанные с незаконной продажей, покупкой, сбытом оружия или изъяв его, правоохранительные органы получают доказательственную базу.

Переписки в мессенджерах или социальных сетях, где обсуждается стоимость оружия, его вид, количество, наличие боеприпасов, составляют следовую картину преступления.

Телефоны, планшеты, ноутбуки и иные технические средства, посредством которых происходит сбыт незаконного товара, содержат в себе информацию о сайтах, форумах, интернет-магазинах или сообществах, где происходит нелегальная продажа оружия и боеприпасов, а также цифровые следы. Такими следами являются денежные транзакции. Не только заключение незаконной сделки происходит посредством цифровых технологий, но и оплата товара. Чаще всего в незаконном обороте в силу своей доступности популярностью пользуются QIWI-кошельки[1].

Сложность в выявлении незаконного денежного потока сотрудниками следственных органов состоит в том, что они могут работать лишь с той информацией, которую им предоставляют электронные платежные системы, а выявление скрытых переводов возможно только с помощью компьютерных экспертиз.

В результате исследования содержимого изъятого устройства, следователи могут установить личности всех участников преступления (продавца, покупателя, «закладчика», курьеров и т. д.), Интернет-площадки, где совершалось преступление и электронные счета, на которые пересылались денежные средства, то есть определить всю картину преступления в сфере незаконного оборота оружия, боеприпасов, взрывчатых устройств и взрывных веществ, совершенного посредством сети «Интернет».

[1] Богданов А. В., Ильинский И. И., Хазов Е. Н. Особенности раскрытия преступлений и выявление лиц, осуществляющих сбыт огнестрельного оружия, боеприпасов, взрывчатых веществ и взрывных устройств через сеть «Интернет» // Криминологический журнал. 2020. № 3. С. 39—45.

Основная проблема в расследовании преступлений, связанных с незаконным оборотом оружия, боеприпасов, взрывчатых веществ и взрывных устройств посредством сети «Интернет» является недостаточная квалификация действующих сотрудников правоохранительных органов, которым не хватает базисного юридического образования.

Таким образом, развитие способов совершения преступлений с использованием сети «Интернет» требует использования современных технический средств и применений специальных знаний в сфере IT-технологий следственными группами, которые занимаются раскрытием такого рода деяний. На данный момент способов использования сети «Интернет», как возможность незаконно организовать оборот оружия, больше, чем способов предотвращения и раскрытия этого преступления.

УДК 343

И. Д. КАРАБИН[1]

К ВОПРОСУ О ВОЗМОЖНОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЗА РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ

На данный момент времени средства массовой информации в погоне за показателями периодически публикуют недостоверную информацию, вводя в заблуждения большую часть общества России.

Иногда высказывания средств массовой информации фактически имеют уголовную ответственность. В свою очередь стоит отметить, что конкретное средство массовой информации является юридическим лицом, что усложняет процесс привлечения данных компаний к уголовной ответственности несмотря на то, что преступления совершаются от лица средства массовой информации.

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

В классическом понимании любое преступление, которое рассматривается непосредственно на стадии судебного расследования имеет свой состав, необходимый набор юридических фактов и элементов, без которого работники правоохранительных органов не смогли бы четко дифференцировать общественно опасные деяния между собой, а также правильно их квалифицировать.

Так, составом преступления признается «совокупность признаков, характеризующих общественно опасное деяние как преступление»[1].

Непосредственными признаками, характеризующим каждый состав преступления являются: объект, объективная сторона, субъективная сторона, а также сам субъект совершения общественно опасного деяния. Стоит уделить особое внимание такому признаку, как субъект, так как в привычной доктрине состава преступления, субъектом преступления признается «физическое лицо, достигшее возраста уголовной ответственности, совершившее во вменяемом состоянии общественно опасное деяние, предусмотренное Особенной частью УК РФ. Обязательный элемент состава преступления»[2].

Данная дефиниция имеет свое логическое обоснование, но сравнивая уголовно-правовую систему других государств, а также смежных отраслей права, неизбежно прослеживается неопределенность в истинности данного определения.

В различных научных источниках, а также в других отраслях российского права можно обнаружить понятие «коллективная ответственность», которое приравнивает юридические лица к субъектам правоотношений, наделяя их правосубъектностью (гражданские, административные правоотношения).

Существует коллизия, связанная с правосубъектностью юридических лиц, которая заключается в том, что в классическом понимании правоспособностью и дееспособностью (точнее деликтоспособностью) обладает только

[1] Уголовное право. Общая часть : учебное пособие в таблицах / Д. А. Безбородов, А. В. Зарубин, Р. М. Кравченко [и др.] ; под ред. А. Н. Попова. 2-е изд., перераб. и доп. СПб., 2019. С. 12.

[2] Там же. С. 17.

персонифицированный субъект, а в юридическом лице данный субъект размыт, его не существует.

Для детального определения субъекта ответственности, стоит обратиться к «теории директоров», предложенной Ю.К. Толстым для гражданских правоотношений, где «именно директор уполномочен действовать от имени организации в сфере гражданского оборота, поэтому он и является основным носителем юридической личности государственного юридического лица»[1].

Но, если в гражданских и административных правоотношениях юридическое лицо способно эффективно функционировать как субъект, то в уголовной отрасли российского права существует обоснованная коллизия, связанная с коллективной уголовной ответственностью, так как «этот вид ответственности является наиболее суровым по сравнению с другими ее видами»[2].

Ответственность заключается не в имущественных убытках, как, например, в гражданской или административной отрасли права, а в изоляции конкретного субъекта от общества (лишение свободы). В свою очередь это усложняет процесс привлечения коллективного субъекта к уголовной ответственности, и «теория директора» способствует устранению коллизионной ситуации, четко определяя субъекта ответственности.

Рассматривая вопрос ответственности юридических лиц, стоит обратить внимание, что по сей день существует дискуссия по поводу субъекта, который несет ответственность корпорации за совершенное правонарушения. Так, по мнению А. С. Никифорова «деяние признается совершенным корпорацией, если оно совершено (непосредственно или при посредстве других лиц) лицом или лицами, которые контролируют осуществление корпорацией ее прав и действуют в осуществление этих прав»[3].

---

[1] Гражданское право. Учебник. В 3 т. Т. 1. / Е. Ю. Валявина, И. В. Елисеев [и др.] ; отв. ред. А. П. Сергеев, Ю. К. Толстой. 4-е изд., перераб. и доп. М., 2005. С. 118.

[2] Честнов И. Л. Теория государства и права. Учебное пособие. В 2 ч. Ч. 2. Теория права. СПб., 2017. С. 114.

[3] Никифоров А. С. Юридическое лицо как субъект преступления и уголовной ответственности. М., 2002. С. 50.

Следует полагать, что директор или же другое лицо, ответственное за компанию, субъект в данном случае выступает как alter ego корпорации, поэтому фактически деятельность юридических лиц зависит от воли и намерении конкретных персонифицированных субъектов, делегируя первому возможность в принятии решении от лица компании.

Сторонники классического понимания уголовной ответственного права отрицают теории об юридической ответственности. Такие ученые, как М. И. Бажанов, Л. Д. Ермакова, Н. Ф. Кузнецова, Т. В. Кондрашова, Л. К. Савюк и др. парируют «краеугольным принципам» уголовного права, где

закреплены базовые принципы в уголовной системе России: «принципам личной и виновной ответственности».

Уголовно-правовые системы других стран включают в себя юридическую ответственность. Так, например, «в США теоретическим основанием ответственности организаций (корпораций) была признана доктрина «respondeat superior» (пусть ответит старший), имевшаяся в гражданском деликтном праве, согласно которой индивидуум нес гражданскую ответственность за действия своих агентов (представителей)»[1].

Данная теория применяется в уголовной системе при условии «actus reus», незаконного действия субъекта юридического лица (директора). Также стоит отметить, что в правовой системе США уголовная и административная отрасль объедены в одну, следовательно, ряд преступлений оцениваются в нашей правовой системе как административные правонарушения, и влекут за собой имущественные наказания, а не лишение лица свободы.

Во Франции так же существует коллективная ответственность за совершенные преступления. К юридическим лицам применяются следующие виды

[1] Волженкин Б. В. Уголовная ответственность юридических лиц. СПб., 1998. С. 19. (Серия «Современные стандарты в уголовном праве и уголовном процессе»).

наказания: «штраф; ликвидация юридического лица; запрещение, окончательное или на срок не более пяти лет, осуществлять прямо или косвенно один или несколько видов профессиональной или общественной деятельности; помещение на срок до пяти лет под судебный надзор; закрытие, окончательное или на срок не более пяти лет, всех заведений или одного или нескольких заведений предприятия, использовавшихся для совершения инкриминируемых действий; и др.»[1].

Следовательно, данные виды наказаний относятся к имущественным взысканиям и приостановлениям деятельности, поэтому они включены в уголовную систему Франции, ведь наказания не связаны с лишением свободы конкретного субъекта.

На данном этапе развития уголовной отрасли в России отсутствуют наказания, применяемые юридическим лицам, за совершенные преступления. Но, согласно ч. 2 ст. 45 УК РФ, к конкретному субъекту преступления, в качестве дополнительного или основного вида наказаний может быть назначен штраф, лишение права занимать определенные должности или заниматься определенной деятельностью. Несмотря на то, что корреляция видов наказаний во Франции в России заметна, но в отличие от Франции, Уголовный кодекс России не включает в себя институт привлечения к уголовной ответственности юридических лиц.

Из этого следует, что за совершение преступлений по составам ст. 207 УК РФ (например, заведомо ложное сообщение о готовящихся взрыве) предусмотрена уголовная ответственность в виде штрафа персонифицированному субъекту.

Данная концепция не совсем эффективная, ведь в таком случае средства массовой информации как юридические лица могут избегать ответственности, наказывая лишь отдельных редактор.

[1] Там же. С. 18.

Но перед опубликованием какой-либо информации директор компании всегда проверяет материалы для публикаций, следовательно, редактор действует от лица компании, и ответственность в виде штрафа или приостановление деятельности за преступления в области заведомо ложных сообщений об актах терроризма должна нести компания (в лице директора).

В заключение считаю необходимым предложить путь решения коллизии, связанной с привлечением средств массовой информации к уголовной ответственности. Как было сказано выше, само по себе юридическое лицо носит абстрактный характер субъекта, но все же, согласно «теории директора» персонифицированным лицом, которое представляет компанию является директор.

В других странах данная концепция имеет свое воплощение в уголовной отрасли. Во Франции наказаниями являются штрафы; приостановления деятельности; ликвидация юридического лица, где ответственным субъектом компании выступает директор, наделенный всей полнотой власти по отношению к средствам массовой информации.

С учетом данных обстоятельств, стоит внести уголовную ответственность средства массовой информации в лице директора по заведомо ложным сообщениям об актах терроризма через наложения штрафов, приостановления деятельности или же ликвидации юридического лица.

Для этого следует дополнить ч. 2 ст. 45 УК РФ, где необходимо внести штрафы; приостановление деятельности в отношении юридического лица или же его ликвидацию, то же самое стоит дополнить в ст. 207 УК РФ. Данные внесения в уголовное законодательство необходимо, так как при привлечении к ответственности редакторов по ст. 207 УК РФ нет гарантии, что данная компания не будет снова публиковать информацию, подрывающую целостность государства.

УДК 343

А. В. КИРЕЕВА[1]

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Несмотря на процесс гуманизации современного общества, нацеленность государства на содействие развитию и реализации личности каждого ребенка, продолжает сохраняться угроза их жизни, здоровья и нормального развития, которая исходит от взрослых людей. Залогом развития правового и социального государства является, в том числе, признание и понимание проблемы защиты ребенка от асоциального поведения взрослого.

Важнейшим механизмом разрешения обозначенной проблемы является УК РФ, в котором содержится норма, устанавливающая ответственность за вовлечение несовершеннолетнего в совершение преступления – ст. 150 УК РФ.

Согласно данным статистики за 2022 год было зарегистрировано 1 237 преступлений, предусматривающих ответственность за вовлечение несовершеннолетнего в совершение преступления или антиобщественных действий[2]. За указанный период число лиц, привлеченных к уголовной ответственности по ст. 150 УК РФ, составило 243, в то время как в 2021 г. – 271, в 2020 г. – 266, в 2019 г. – 333, в 2018 г. – 365[3].

Несмотря на то, что статистические данные показывают ежегодный спад количества совершаемых в отношении несовершеннолетних преступлений, показатели все же вызывают опасение.

В век информационных технологий сильное воздействие на становление личности оказывает сеть «Интернет». В России насчитывается порядка 130 млн пользователей сети «Интернет», что составляет практически 90 % населения страны[4].

---

[1] Научный руководитель — МОРОЗОВА Юлия Владимировна, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

[2] URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 18.02.2023).

[3] URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 18.02.2023).

[4] URL: https://habr.com/ru/news/690628/ (дата обращения: 07.10.2023).

Причем контент, содержащийся в данной платформе, оказывает влияние на формирование взгляда на жизнь современного человека, являясь инструментом для развития и самореализации. Однако, кроме позитивных моментов, можно выделить и негативные.

Сегодня у каждого в распоряжении имеется как минимум одно устройство, имеющее доступ к сети «Интернет», в том числе и у несовершеннолетних, что означает почти круглосуточное нахождение ребенка в зоне риска. По данным опроса Института статистических исследований и экономики знаний НИУ ВШЭ, проведенного в 2022 году, среди респондентов в возрасте от 14 до 17 лет в сеть «Интернет» выходят 99 %, причем еще в дошкольном возрасте собственный телефон с доступом в «Интернет» есть у каждого третьего (30 % среди детей 3–6 лет)[1].

Социальные сети являются для детей неким развлечением, платформой для общения или же нахождения новых «виртуальных» друзей. Соответственно, в их сознании это отражается как что-то позитивное и создает видимость определенной дружелюбной атмосферы[2].

Однако, указанное ощущение является ложным по причине того, что в данной среде действуют различные субъекты, в том числе, имеющие возможность оказывать на подростков и негативное воздействие. Неокрепшая психика ребенка, недостаточно развитая общая культура и невысокий интеллектуальный уровень, ряд психофизиологических особенностей под влиянием агрессивного и социально-опасного контента, исходящего от других пользователей, позволяют несовершеннолетнему стать «объектом» для вовлечения в общественно опасные деяния.

Существует определенный механизм вовлечения несовершеннолетнего в противоправную деятельность. Так, начинается все с безобидного привлечения внимания с помощью различного рода публикаций, материал в которых

[1] URL: https://academia.interfax.ru/ru/news/articles/10586/ (дата обращения: 07.10.2023).

[2] Жоков Д. В. Ответственность за вовлечение несовершеннолетних в совершение преступлений с использованием информационно-телекоммуникационных технологий и сети «Интернет» // Вызовы глобализации и развитие цифрового общества в условиях новой реальности : сб. материалов IV Международной научно-практической конференции, г. Москва, 19 декабря 2022 г. / Институт развития образования и консалтинга. М., 2022. С. 56–65.

преподносится в достаточно легкой форме, например, шутки. Далее, ребенок вступает в диалог с тем, кто, по его мнению, понимает и разделает его интересы, однако на этом этапе уже начинается вовлечение путем предоставления определенной информации в более грубой форме. «Вовлекатель» приглашает несовершеннолетнего в сообщество «единомышленников», в котором происходит активная подготовка к действиям, а в дальнейшем предоставляется доступ, к так называемым, «закрытым каналам связи». К сожалению, последним этапом является совершение ребенком преступления под влиянием лиц, имеющих судимость или преступный опыт. Стоит отметить, что личная жизнь несовершеннолетнего тщательно изучается с целью оказания большего воздействия на него.

Так, согласно Приговору Серовского районного суда, совершеннолетний подсудимый С. при использовании социальной сети «Друг вокруг», предназначенной для общения и поиска новых друзей, зная о несовершеннолетнем возрасте Х., предложил последнему совершить хищение металлолома из сгоревшего ангара, пообещав денежные средства от продажи похищенного имущества поделить. Лицо, не достигшее совершеннолетия, согласилось на предложение. Решением суда С. был признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 30, п. «а» ч. 2 ст. 158, ч. 1 ст. 150 УК РФ[1].

Данный пример судебной практики показывает, что вышеизложенный механизм воздействия на ребенка через сеть «Интернет» используется преступниками для облегчения процесса вовлечения.

Увеличения риска заинтересованности ребенка опасным контентом в условиях интенсивности совершенствования IT-технологий, отметила Е. Е. Леоненко, а также «... желание попробовать что-то новое позволяют несовершеннолетним легко поддаться на предложения поучаствовать в опасных мероприятиях[2]».

[1] Приговор Серовского районного суда Свердловской области от 13 ноября 2015 г. по делу № 1-584/2015. Доступ через информ.-правовой портал «Гарант».

[2] Замглавы СК РФ Елена Леоненко: цифровую гигиену нужно прививать с детства : [интервью, данное 1 июля 2022 года]. // РИА Новости : сайт. URL: https://sledcom.ru/press/interview/item/1693826/?tab=images (дата обращения: 03.10.2023).

Отмечается, что на практике встречаются случаи, когда взрослому с легкостью удается через сеть «Интернет» завербовать ребенка в террористические и экстремистские организации, а также сбыт наркотиков.

Кроме того, законодатель в п. 44 Указа Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» акцентирует внимание, что международные террористические и экстремистские организации стремятся усилить пропагандистскую работу и работу по вербовке российских граждан, в том числе вовлечь в противоправную деятельность российскую молодежь[1]. Для распространения информации используются возможности интернет-компаний.

В части 4 ст. 150 УК РФ содержится квалифицирующий признак: вовлечение несовершеннолетнего, в том числе, в совершение преступления по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы. Информация, содержащаяся в сети «Интернет», может быть направлена на провокацию ненависти и насилия к людям определенной социальной группы, а также на пропаганду подобных взглядов, что представляет угрозу для развития ребенка. Через платформу несовершеннолетний имеет возможность вступить в виртуальную, а затем и реальную группу, пропагандирующую данные убеждения.

По Приговору Новороссийского гарнизонного военного суда Т. признан виновным по ч. 1 ст. 282.1, ч. 4 ст. 150 УК РФ. Установлено, что Т. и лицо, уголовное дело в отношении которого выделено в отдельное производство, договорились о создании экстремистского сообщества, для чего с использованием мобильного телефона создали виртуальные группы в социальной сети «ВКонтакте» и мессенджере «Телеграм», в которые, в общей сложности, добавили пять несовершеннолетних, разделявших идеи экстремистского сообщества. Спустя время фигуранты данного уголовного дела организовали

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

встречи с участниками сообщества в реальной действительности, в ходе которых договорились о целях их деятельности – совершение преступлений экстремистской направленности. Так, они осуществляли пропаганду нацистской идеологии, а также совершали нападения на лиц, злоупотребляющих алкогольной или спиртосодержащей продукцией, наркотическими средствами, представителей определенных субкультур с применением перцовых баллончиков, сожжение символа воинской славы России – Знамени Победы[1].

Сеть «Интернет» используется для вовлечения подростков в преступные группы, цель которых совершение различных преступлений.

По одному из Приговоров Железнодорожного районного суда г. Самары[2] К., на основании исследованных Судом первой инстанции доказательств, оправдана по обвинению в совершении преступления, предусмотренного ч. 4 ст. 150 УК РФ в связи с непричастностью к совершению преступления. Так, из материалов уголовного дела следует, что подсудимая вместе со своей троюродной несовершеннолетней сестрой Л. откликнулись на объявление о работе в мобильном приложении «Авито», после чего в мессенджере «WhatsApp» от неизвестного лица на протяжении двух недель поступили предложения и уговоры о работе курьером наркотических средств с обещанием высокой заработной платы, от которого они, первоначально, отказались. Затем именно несовершеннолетняя Л. уговорила К. принять предложение. Таким образом, вовлечение несовершеннолетней Л. в совершение ряда преступлений преступной группой путем обещаний осуществлено не К., а неустановленным лицом через мессенджер «WhatsApp».

Данные примеры свидетельствуют об активном использовании возможностей сети «Интернет» для привлечения подростков в совершении противоправных деяний.

---

[1] Апелляционное определение Судебной коллегии по уголовным делам Южного окружного военного суда от 20 мая 2022 г. по делу № 22-231/2022. Доступ через информ.-правовой портал «Гарант».

[2] Апелляционное определение Судебной коллегии по уголовным делам Самарского областного суда от 22 мая 2023 г. по делу № 22-2855/2023. Доступ через информ.-правовой портал «Гарант».

Стоит констатировать тот факт, что лицам, совершившим преступление, предусмотренное ст. 150 УК РФ, удается избежать уголовной ответственности по определенной причине. Так, согласно п. 42 Постановления Пленума Верховного Суда Российской Федерации от 01.02.2011 № 1 «О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних», если совершеннолетнее лицо не знало о несовершеннолетии вовлекаемого, то он не может привлекаться к ответственности по ст. 150 УК РФ[1]. Перенося данный факт на возможность использования сети «Интернет» как одного из способов вовлечения в совершении преступления, нельзя не обратить внимание на возможность возникновения следующей ситуации: несовершеннолетний срывает свой возраст, чтобы при общении с «вовлекателем» выглядеть старше. В свою очередь, совершеннолетнее лицо, вовлекающее ребенка в какое-либо преступление, часто указывает на неосведомленность о несовершеннолетии лица. В таком случае деяние лица, осуществляющего вовлечение, остается безнаказанным, что является проблемой в достижении цели уголовного права: охрана прав и свобод человека и гражданина.

Обращаясь к зарубежному опыту, можно остановиться на Уголовном кодексе Республики Казахстан, в котором по ряду преступлений, в том числе в отношении вовлечения несовершеннолетнего в совершении преступления, законодатель предусмотрел квалифицирующий признак: совершение преступления посредством использования сети «Интернет». Данный факт очередной раз подтверждает необходимость установления повышенной защиты ребенка от оказания противоправного влияния, порой, совсем незнакомых лиц.

Опрос, проведенный среди прокурорских работников, показал, что 73 % респондентов считаю, что существует необходимость в дополнении ст. 150

[1] О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : Постановление Пленума Верховного Суда Российской Федерации от 1 февраля 2011 г. № 1 : текст с изм. и доп. на 28 окт. 2021 г. Доступ из справ.- правовой системы «КонсультантПлюс».

УК РФ таким квалифицирующим признаком как «вовлечение несовершеннолетних в совершение преступления или антиобщественных действий с использованием сети «Интернет».

Подводя итог, отметим, что, на наш взгляд, целесообразно внести изменения в ч. 3 ст. 150 УК РФ, дополнив ее квалифицирующим признаком «либо с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)». Не останавливаясь на исследованных выше вопросах, обозначим, что дополнительной целью является также законодательное обособлении анализируемого преступления для формирования объективных статистических данных, позволяющих выявить их первопричины и сформировать комплекс превентивных мер[1].

УДК 343

Э. А. КИРШИНА,
А. Р. ЧУПАШОВА[2]

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

Преступление в сфере информационных технологий или киберпреступление — это предусмотренное уголовным законодательством общественно опасное противоправное деяние, совершенное посредством удаленного доступа к объекту посягательства с использованием глобальных компьютерных сетей в качестве основного средства достижения цели[3].

---

[1] Бошаева Л. Л. Интернет-технологии как способ вовлечения несовершеннолетнего лица в преступную деятельность // Право и государство: теория и практика. 2022. № 4 (208). С. 155.

[2] Научный руководитель — МОРОЗОВА Юлия Владимировна, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

[3] Гузеева, О. С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети «Интернет» (криминологические и уголовно-правовые проблемы) : автореф. дис. ... канд. юрид. наук. М., 2008. 25 с.

Продолжительное время в Российской Федерации наблюдается высокий рост преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, данный вывод основан на статистических данных, которые показывают, что за последние 6 лет число вышеперечисленных преступлений выросло более чем в 50 раз: в 2022 году в России было зафиксировано около 510 тыс. преступлений с использованием информационных технологий, а в 2014 году – всего 10 тысяч.

Стоит обратить внимание, что тенденция по преступности в ИТ-сфере идет в разрез с общей тенденцией преступности по России, которая идет на спад уже не первый год.

20 марта 2023 года президент Российской Федерации Владимир Путин на расширенном заседании коллегии МВД сообщил, что преступления в ИТ-сфере составили четверть от всех уголовных правонарушений в России в 2022 году, превысив полмиллиона. Для сравнения: в 2015 году такие преступления составляли всего 2 % от общего числа.

Опасность данных преступлений заключается не только в количественном, но и в качественном показателях: способы совершения преступлений меняются крайне быстро и подстраиваются под уровень развития общества, обстановку в стране и в мире. Так в период пандемии начали приходить SMS-сообщения со следующей информацией: «Согласно геолокации вами был нарушен режим самоизоляции и карантина согласно ст. 20.6.1 КоАП РФ и необходимо срочно заплатить штраф, а в случае неоплаты в течение 24 часов против вас будет возбуждено уголовное дело на основании ст. 236 УК РФ»[1]. По этой причине затруднительным становится расследование таких преступлений, а также снижается статистика раскрываемости, так, согласно данным Генеральной прокуратуры, в России раскрывается менее 25 % киберпреступлений.

[1] Баранов А. А., Соломатина Е. А., Шукаева Д. Т Предупреждение преступлений и правонарушений органами внутренних дел в период распространения новой коронавирусной угрозы // Вестник экономической безопасности. 2020. № 5. С. 107.

Преступления в сфере ИТТ разнообразны, прежде всего к ним относится, мошенничество, совершаемое посредством информационно-телекоммуникационной сети «Интернет», так и с помощью средств мобильной связи (ст. 159 УК РФ) — фишинг, вишинг. Преимущественно это хищения денежных средств с банковских счетов граждан. Также к таким преступлениям относятся, например, хищения, совершенные с использованием расчетных (пластиковых) карт (п. «г» ч. 3 ст. 158 УК РФ) — кардинг; создание, использование и распространение вредоносных программ (ст. 273 УК РФ), распространение противоправной информации (клеветы) посредством информационно-телекоммуникационной сети «Интернет» (ч. 2 ст. 128.1 УК РФ), незаконный оборот наркотиков, оружия, доведение до самоубийства (ст. 110 УК РФ) — «Синий кит», «Тихий дом», «Млечный путь».

Таким образом, преступления, совершенные с использованием ИТ-технологий не ограничиваются какой-либо главой уголовного кодекса, что создает серьезную угрозу для национальной безопасности.

Этот факт подтверждается такой проблемой, как сложность и проблемность раскрытия преступлений. Трудности возникли, потому что подобным уголовным правонарушениям присущи следующие черты:

1) анонимность и конфиденциальность нарушителей закона: преступники скрывают свою личность, используя различные псевдонимы и технические средства для маскировки своего местоположения и следов своей активности. Все это существенно затрудняет процесс выявления и наказания таких преступников, что делает борьбу с ними сложной и долгой.

2) получение информации, запрошенной правоохранительными органами у банковских организаций, операторов мобильной связи, является долгим процессом и не приносит большой пользы, так как все счета, телефонные номера регистрируются на третьих лиц;

3) способность преступников подстраиваться под окружающую обстановку и использовать новые, ранее не известные способы совершения преступлений. В связи с этим не успевают разрабатываться методики для раскрытия данных преступлений;

4) объективный фактор: нестабильная эпидемиологическая ситуация в государстве, в связи с чем большинство организаций и учреждений перешли на дистанционную работу, количество пользователей интернета увеличилось, как и количество кибератак со стороны злоумышленников.

5) большая часть населения в силу своей неграмотности в сфере компьютерных технологий, чрезмерной доверчивости и неосведомленности о новых способах совершений преступлений является уязвимой и слабозащищенной.

Криминологический анализ данного вида преступности в России позволяет констатировать, что в последнее время ей характерно свойство нелинейного роста. Например, в условиях применения мер ограничения во время пандемии новой коронавирусной инфекции в 2020 г. число преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, существенно выросло (363 034 к 205 116 АППГ).

В январе–мае 2020 г. число преступлений в сфере информационных технологий увеличилось на 85,1 % и составило 180 498. Отмечен рост преступлений, совершенных с использованием: расчетных (пластиковых) карт (63 696, +466 % к 2019 г.); сети «Интернет» (102 175, +74,1 % к 2019 г.); средств мобильной связи (76 558, +99,7 % к 2019 г.); программных средств (3 831, +53,2 % к 2019 г.). Наибольший прирост показали кражи (60 765, +158,2 % к 2019 г.) и мошенничества, совершенные с использованием электронных средств платежа (10 826, +138,8 % к 2019 г.)[1].

Статистика МВД показывает, что в 2023 году тенденция на рост преступности в сфере компьютерных технологий сохраняется: за январь-сентябрь зарегистрировано 489 044 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. в том числе совершенных с использованием или применением: сети «Интернет» — 377 608 преступлений (+36,7%), средств

[1] Колчевский И.Б., Бицадзе Г.Э. Преступления в сфере информационных технологий: понятие, структура // Научный портал МВД России. 2021. № 2 (54). С. 40—47.

мобильной связи — 220 258 уголовных правонарушений (+46,7%). Мошенничества ст. 159 УК РФ — 254 395 (+42,8%). Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества ст. 228.1 УК РФ — 60 534 (+30,7%). Наибольший прирост показал неправомерный доступ к компьютерной информации ст. 272 УК РФ 19 325 (+224,0%). При этом, раскрыто всего 24,2 % преступлений.

Лидирующими регионами, в которых наблюдаются наибольшие темпы прироста являются: Ненецкий АО, прирост в данном регионе составил 151,1 %, Калининградская область — 70,4 % и Ямало-Ненецкий АО — 69 %. Регионы с зафиксированным отрицательный приростом: Чеченская Республика — 30,4 %, Псковская область — 29,5 % и Республика Калмыкия — 25,6 %.

Наибольший удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации приходится на Ямало-Ненецкий АО, где совершается 50,9 % данных преступлений, второе место занимает Республика Марий-Эл – 46, 2 %, на третьем месте по интернет-преступности находится г. Москва, на который приходится 45,3%. Меньше всего преступлений в данной сфере совершается в Чеченской Республике, Дагестане и Тыве, где удельный вес составляет 7,2 %, 7,9 % и 13,4 % соответственно[1].

Однако, по нашему мнению, в силу специфики преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, географическая привязанность теряет свою значимость. Данное утверждение связано с тем, что территориальное местонахождение преступника не обуславливает место совершения пре-

[1] Состояние преступности в Российской Федерации за январь–сентябрь 2023 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/42989123/ (дата обращения: 21.11.2023).

ступления, поскольку интернет-преступник, используя всемирную сеть, способен совершить преступления в отношении лица, находящегося в любой точке страны и мира.

Например, в феврале 2023 года в городе Санкт-Петербург в результате реализации оперативной информации сотрудники полиции задержали пятерых местный жителей, которые на протяжении последних четырех лет занимались обманом покупателей интернет-магазинов, от действий которых пострадали около 150 человек из 30 регионов России.

Члены организованной группы создали более 70 онлайн-маркетов, специализирующихся на продажах якобы качественной текстильной продукции и цифровой техники, ими руководили анонимные кураторы, которые находились за пределами России.

Рекламируя свои сайты в социальных сетях, аферисты завлекали пользователей низкими ценами и высокими скидками в случае приобретения сразу нескольких изделий. Доставка приобретенных товаров осуществлялась только после ее полной оплаты. Однако, вскрыв полученную посылку, заказчик обнаруживал товар, который не соответствовал заявленным характеристикам, либо вовсе был неисправен. Кроме этого, злоумышленники клали в упаковки пакеты с песком или землей, а после их отправки переставали выходить на связь. Общая сумма ущерба составила порядка семи миллионов рублей, а по всем фактам возбуждены уголовные дела по ч. 4 ст. 159 УК РФ[1].

Стоит обратить внимание, что немалая часть преступлений в информационно-телекоммуникационном пространстве остается нераскрытой правоохранительными органами. Латентная преступность – это объективное социально-правовое явление, имеющее свои качественные и количественные характеристики, представляющее собой совокупность противоправных посягательств,

[1] В Санкт-Петербурге полицией пресечена деятельность организованной группы интернет-мошенников // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/news/item/35903714?ysclid=lp8ma4jbuy159319068 (дата обращения: 21.11.2023).

совершенных с использованием ИТТ, не выявленных и (или) не учтенных правоохранительными органами на той или иной территории в определенный период времени[1].

Безусловно, статистические показатели латентной преступности в данной сфере выявить крайне сложно, поэтому в данной ситуации уместно обратиться к мнению экспертов, которые считают, что латентность указанных противоправных посягательств составляет 80–85 %, а факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер[2].

Криминологами представлена интересная классификация данных преступлений по механизму образования, согласно которой:

– к естественно-латентным следует отнести совокупность преступлений, совершаемых с использованием ИТТ, не ставших известными (не выявленных) правоохранительным органам, соответственно, не учтенных в уголовной статистике, в отношении которых не приняты предусмотренные законом меры реагирования;

– к искусственно-латентным следует отнести совокупность преступлений, совершаемых с использованием ИТТ, ставших известными правоохранительным органам, но в силу различных причин умышленно сокрытых от регистрации;

– к третьей разновидности латентной преступности, совершаемой с использованием ИТТ, следует отнести совокупность противоправных посягательств, информация о которых стала известна правоохранительным органам, но которые оказались за рамками статистического учета в силу их добросовестно ошибочной или заведомо незаконной правовой оценки[3].

Чем же обусловлен столь высокий уровень латентных преступлений?

---

[1] Иванова Е. О. Латентная преступность: понятие и критерии классификации // Современное право. 2015. № 5. С. 119—123.

[2] Бойко О. А., Унукович А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Юридический вестник Самарского университета. 2020. Вып. 6, № 3. С. 53—59.

[3] Джафарли В. Ф. Краткий криминологический анализ причин и условий киберпреступности и методы ее предупреждения // Ученые труды Российской Академии адвокатуры и нотариата. 2017. № 2. С. 54—58.

Данное явление объясняется различными условиями, которые способствуют латентности, например, такими являются:

– доступ самых широких слоев населения к компьютерной технике и Интернету;

– трансграничность географии совершения преступлений, совершаемых с использованием ИТТ;

– отсутствие у значительного числа пользователи минимальных знаний о «компьютерной гигиене» и правилах безопасной работы в информационном пространстве;

– безконтактность и относительная доступность объекта преступного посягательства;

– относительная комфортность деятельности преступников, связанной с подготовкой и реализацией преступных замыслов.1

Несомненно, высокий уровень латентности представляет серьезную угрозу, поскольку большинство преступников остается безнаказанными. Поэтому нами предлагается рассмотреть возможные пути решения сложившейся проблемы. Вряд ли правоохранительным органам удастся опередить злоумышленников в ИТ-сфере, поэтому противодействие киберпреступности будет носить, скорее, догоняющий характер. В этой связи будет целесообразно ввести в штат правоохранительных органов постоянно действующий отдел специалистов в сфере компьютерных технологий. На наш взгляд, это должно помочь работникам органов предварительного расследования понять, какими способами преступники совершают уголовные правонарушения и как этому противодействовать. Предполагается, что это ускорит возможность разрабатывать методики по раскрытию подобных преступлений.

Также стоит уделить внимание «киберпрофилактике» населения. Постоянное освещение темы киберпреступности среди граждан сотрудниками правоохранительных органов, информирование о появлении новых способов совершения преступлений защитит неосведомленных и даже предотвратит некоторое количество нарушений уголовного закона в данной сфере.

[1] Бойко О. А., Унукович А. С. Указ. соч.

УДК 343

А. Ю. КОЗЕНКОВА[1]

НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ЛЕГАЛИЗАЦИЮ (ОТМЫВАНИЕ) ДЕНЕЖНЫХ СРЕДСТВ ИЛИ ИНОГО ИМУЩЕСТВА, ПРИОБРЕТЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, СОВЕРШАЕМУЮ ПУТЕМ ПРИОБРЕТЕНИЯ КРИПТОВАЛЮТЫ

В настоящее время такой «объект» гражданских правоотношений, как криптовалюта, справедливо является камнем преткновения в научном сообществе.

Между тем, сама криптовалюта лишь в несколько лет назад стала признаваться в Российской Федерации. С 01.01.2021 года вступил в силу Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах и цифровой валюте» четко установила, что цифровая валюта может использоваться в качестве средства платежа, не являющегося денежной единицей Российской Федерации или иностранного государства[2].

Используя ее свойства, такие как отсутствие единой оценки на как финансового инструмента, анонимность, многие субъекты криминальной отрасли нашли возможность использования такого ресурса в качестве средства платежа, способа легализации средств, полученных незаконным путем. Данный факт вызывает все большую обеспокоенность у правоохранительных органов в силу латентности данных противоправных деяний. Кроме того, даже у выявленных преступлений процент раскрываемости крайне мал.

Анализ процессуальных документов, приговоров судов и уголовных дел в целом свидетельствует о том, что как объект платежных операций криптовалюта наиболее часто используется при незаконном сбыте наркотических

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ : текст с изм. и доп. на 14 июля 2022 г. Доступ из справ.-правовой системы «КонсультантПлюс».

средств, а также при легализации (отмывании) доходов. При проведении оценки рисков оборота криптовалюты было справедливо отмечено, что в 2015 году количество зафиксированных фактов использования виртуальной валюты в целях легализации не превышало 5% от общего объема криптовалюты, а на 2018 год этот показатель составил уже 40%, что свидетельствует о повышении темпа роста использования такого «средства платежа» в обороте.

Целью данной работы является выяснение следующих аспектов: разграничение цифрового рубля и криптовалюты в рамках ст. 174 УК РФ; выяснение может ли криптовалюта признавать предметом 174. (Ответ нет, все равно конечный результат деньги после обнала).

Какие действия с криптовалютой свидетельствуют о признаках преступления, предусмотренного ст. 174 УК РФ? Просто обналичивание будет являться окончанием? определение момента окончания объективной стороны ст. 174 УК РФ при использовании в качестве предмета криптовалюту.

Согласно ст. п. 1 Постановления Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» предметом преступлений, предусмотренных ст. 174, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления».

Статья 27 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» содержит прямой запрет выпуска на территории Российской Федерации денежных суррогатов. В подзаконных нормативных актах и документах федеральных органов государственной власти неоднократно подчеркивалось, что возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания, служит предпосылкой высокого риска потенциального вовлечения криптовалют в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

Анализируя судебную практику по данному обстоятельству, стоит отметить, что приговоры судов различных инстанций достаточно противоречивы. Например, встречаются случаи использования криптовалюты при осуществлении противоправной деятельности, предусмотренной ст. 288 УК РФ[1].

Так, оплата за преступную деятельность, связанную со сбытом наркотических средств, А. начислялась администраторами интернет-магазина в виде криптовалюты через платежную систему Bitcoin. На биржах криптовалюту А. конвертировал в рубли и через платежную систему «КИВИ» переводил в АО «КИВИ Банк» на электронный кошелек, привязанный к его абонентскому номеру телефона. Затем деньги переводились на банковский счет А., откуда в последующем переводились на его банковскую карту. Полученные денежные переводы А. обналичивал в банкоматах и тратил на личные нужды: оплачивал услуги мобильной связи, приобретал различные продукты питания, иные вещи для личного потребления, на лечение матери. Полученные деньги были для А. источником существования.

Вопреки доводам апелляционного представления решение суда об оправдании А. по п. «а» ч. 4 ст. 174.1 УК РФ является законным и обоснованным.

Исходя из положений Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», под легализацией (отмыванием) доходов, полученных преступным путем, понимается придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Преступление, предусмотренное ст. 174.1 УК РФ, относится к сфере экономической деятельности и его необходимым элементом является цель вовлечения денежных средств и иного имущества, полученного в результате совершения преступления, в легальный экономический оборот. Для наличия данного состава преступления необходимы не просто финансовые операции

[1] Приговор Советского районного суда г. Улан-Удэ Республики Бурятия от 5 июля 2017 г. по делу № 1-367/2017 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 21.11.2023).

и сделки с имуществом, полученным преступным путем, а действия, направленные на установление, изменение или прекращение гражданских прав и обязанностей, придание им видимости законности.

Тех же доводов придерживался и суд первой инстанции по уголовному делу в отношении В. Приговором суда первой инстанции суда В. был осужден по ч. 2 ст. 228.3 и ч. 5 ст. 228.1 УК РФ. Этим же приговором он был оправдан по обвинению в легализации денежных средств, приобретенных в результате незаконного производства наркотического средства, в целях придания правомерного вида владению, пользованию и распоряжению указанными денежными средствами.

В приговоре указывалось, что за свою преступную деятельность обвиняемый получал вознаграждение в виде биткоинов на виртуальный кошелек. Используя банковские технологии, позволяющие избежать процедуры банковского контроля и исключить возможность идентификации его и лиц, совершающих операции, он конвертировал криптовалюту в рубли. С целью придания правомерного вида владению, пользованию и распоряжению данными денежными средствами В. совершил финансовые операции по переводу денежных средств в размере 8,2 млн руб. с виртуального счета на банковские карты и счета, открытые на имя дочери его сожительницы, после чего распорядился денежными средствами по своему усмотрению.

Однако суд пришел к выводу, что совершение финансовых операций с денежными средствами, преобразованными из биткоинов, в виде перевода денежных средств с виртуального счета на банковские карты без введения полученных денежных средств в экономический оборот не свидетельствует о легализации доходов, полученных преступным путем.

Также стоит отметить, что в судебной практике значительная часть случаев неверной квалификации преступлений по ст.ст. 174, 174.1 УК РФ относится к неверному определению наличия цели совершения исследуемых преступлений. В частности, в Постановлении подчеркивается, что о направленности умысла на легализацию денежных средств или иного имущества, приобретенных преступным путем, не свидетельствует распоряжение ими в целях

личного потребления (приобретение продуктов питания, товаров первой необходимости, получение бытовых услуг и т. п.).

Так, оплата за преступную деятельность, связанную со сбытом наркотических средств, А. начислялась администраторами интернет-магазина в виде криптовалюты через платежную систему Bitcoin. На биржах криптовалюту А. конвертировал в рубли и через платежную систему «КИВИ» переводил в АО «КИВИ Банк» на электронный кошелек, привязанный к его абонентскому номеру телефона. Затем деньги переводились на банковский счет А., откуда в последующем переводились на его банковскую карту. Полученные денежные переводы А. обналичивал в банкоматах и тратил на личные нужды: оплачивал услуги мобильной связи, приобретал различные продукты питания, иные вещи для личного потребления, на лечение матери. Полученные деньги были для А. источником существования.

Таким образом квалифицировать подобное деяние как легализацию денежных средств не является корректным, т.к. конкретного умысла на легализацию денежных средств у А не было.

Еще одним вопросом, вызывающим споры в рамках данной тематике является вопрос определения фактического предмета легализации денежных средств. Ряд представителей научного сообщества считает, что криптовалюта сама по себе предметом легализации денежных средств не является, а является лишь инструментом для итогового получения денежных средств.

Данный тезис подтверждается непосредственно постановлением Пленума: Обратить внимание судов на то, что предметом преступлений, предусмотренных статьями 174 и 174.1 УК РФ, являются не только денежные средства или иное имущество, незаконное приобретение которых является признаком конкретного состава преступления (например, хищения, получения взятки), но и денежные средства или иное имущество, полученные в качестве материального вознаграждения за совершенное преступление (например, за убийство по найму) либо в качестве платы за сбыт предметов, ограниченных в гражданском обороте.

При этом под денежными средствами понимаются наличные де- нежные средства в валюте Российской Федерации или в иностранной валюте, а также безналичные денежные средства, в том числе электронные денежные средства, под иным имуществом — движимое и недвижимое имущество, имущественные права, документарные и бездокументарные ценные бумаги, а также имущество, полученное в результате переработки имущества, приобретенного преступным путем или в результате совершения преступления (например, объект недвижимости, построенный из стройматериалов, приобретенных преступным путем).

Исходя из положений статьи 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 года и с учетом Рекомендации 15 ФАТФ предметом преступлений, предусмотренных ст. ст. 174 и 174.1 УК РФ, могут выступать в том числе и де- нежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления.

Под денежными средствами в Постановлении понимаются наличные денежные средства в валюте Российской Федерации или в иностранной валюте, а также безналичные денежные средства, в том числе электронные денежные средства.

В данный момент актуальным становится также и вопрос разграничения цифрового рубля как узаконенным денежным обращением в Российской Федерации и криптовалюты в рамках ст. 174, ст. 174.1 УК РФ.

От криптовалюты цифровой рубль отличается тем, что у него есть эмитент — Банк России. Он же отвечает за безопасность и сохранность денег пользователей. А в случае с криптовалютой все риски всегда лежат на пользователях. Таким образом цифровой рубль рассматривается в рамках вышесказанных статей в качестве электронного денежного средства, в то время как криптовалюта выступает не как конечное денежное средство.

Подводя итог всему вышесказанному, необходимо отметить, что в связи с тем, что вопросы с криптовалютами в целом вызывают ряд проблем у законодателя с точки зрения кодификации норм и правил, регулирующих ее оборот, ситуацию осложняет и то, что данный инструмент все чаше внедряется в преступные механизмы. Стоит понимать, что при рассмотрении криптовалюты в рамках ст.ст. 174, 174.1 УК РФ первостепенной важности является фактор мотива и заинтересованности лица в достижении конечной цели — придания законного статуса денежным средствам, а не сам факт обмена криптовалюты на денежные средства.

УДК 343

П. А. КОМАРОВА[1]

О НЕКОТОРЫХ ВОПРОСАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ОБОРОТОМ КРИПТОВАЛЮТ

На сегодняшний день процесс информатизации, который затрагивает практически все сферы жизнедеятельности человека и в том числе оказывает существенное влияние и на использование нами финансовых средств.

Свидетельством того, что кредитно-финансовая сфера вышла на кардинально новый уровень, служит широкое распространение на мировом рынке криптовалюты (виртуальной валюты), в основе работы которой лежит технология распределенного реестра (технология Blockchain).

Сейчас рынок криптовалюты является одним из крупнейших нерегулируемых рынков в мире. Криптовалюта во многом изменила не только ведение бизнеса и личных расчетов людей, но и нелегальную финансовую деятельность.

По данным Европола, примерно четверть пользователей биткоинов и половина транзакций биткоинов связаны именно с незаконной деятельностью[2].

---

[1] Научный руководитель —ТЕРТЫЧНАЯ Илона Викторовна, доцент кафедры криминалистики Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент.

[2] Долгиева М. М. Проблемы привлечения к уголовной ответственности субъектов преступлений, совершаемых в сфере оборота криптовалюты // Российское правосудие. 2019. № 2. С. 85.

Именно цифровой и анонимный характер работы криптовалюты способствовали появлению в сети рынков, предоставляющих незаконные товары и услуги.

В современных условиях развития рынка перед правоохранительными органами остро стоит ряд проблем, связанных с процессом расследования и раскрытия преступлений в сфере оборота криптовалют, то есть таких, где она выступает в качестве предмета преступления. В так называемый сектор криптопреступности преимущественно входит хищение криптовалюты с кошельков пользователей, легализация (отмывание) денежных средств, полученных преступным путем, а также кибермошенничество (фишинг).

Одной из основных проблем в данной сфере является отсутствие полноценного правового регулирования и определения статуса криптовалюты в Российской Федерации. Несмотря на то, что в настоящее время значительно возросло количество владельцев криптокошельков, такая валюта еще не применяется в России как самостоятельный платежный инструмент. Но поскольку она все чаще начинает выступать предметом уголовного посягательства, активно назревают дискуссии по поводу ее нормативной регламентации.

В Российской Федерации криптовалюта не находится под запретом и не ограничивается право на владение ею, однако на законодательном уровне она не является средством платежа.

Согласно ст. 75 Конституции Российской Федерации, денежной единицей в Российской Федерации является рубль денежная эмиссия осуществляется исключительно Центральным банком Российской Федерации. В Федеральном законе «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ (ред. 14.07.2022) закреплены понятия цифровых финансовых активов и цифровой валюты.

В соответствии с данным нормативным правовым актом, цифровыми финансовыми активами признаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным

бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы», в свою очередь, под цифровой валютой понимается «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам».

Несмотря на то, что с момента принятия данного закона прошло более двух лет, противоречия в сфере отнесения криптовалюты к предмету регулирования данного акта до сих пор остаются. На текущий момент цифровые финансовые активы и цифровая валюта выпускаются только через операторов, официально принятыми Центральным Банком Российской Федерации в реестр.

Таким образом, криптовалюта не может являться ни тем, ни другим, поскольку ее выпуск осуществляется на закрытых Blockchain-платформах. Таким образом, отсутствие законодательно установленной системы прослеживаемости транзакций с использованием криптовалюты не дает правоохранительным органам эффективно реагировать на преступления, совершаемые в сфере ее оборота.

Нет и однозначной точки зрения относительно того, может ли криптовалюта выступать предметом хищения. Многие исследователи в данной области приходят к выводу, что обладая собственной стоимостью и принадлежностью на праве собственности конкретному лицу, криптовалюта может являться предметом гражданского оборота и должна быть отнесена к видам иного имущества в рамках ст. 128 ГК РФ, и в том числе являться предметом хищения[1].

На сегодняшний день, исходя из положений Постановления Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», денежные средства, преобразованные из виртуальных активов (криптовалюты) могут выступать в качестве предмета преступлений, предусмотренных ст.ст. 174 и 174.1 УК РФ.

Немаловажным препятствием для правоохранительных органов при расследовании преступлений, связанным с оборотом криптовалют, остается анонимность субъектов таких криминальных деяний. «Так, вся база Blockchain находится в публичном доступе, посмотреть данные того или иного блока и отследить изменение информации может любой желающий. Однако сведения о том, кто и кому перевел криптоактивы, могут быть доступны лишь непосредственным участникам обмена»[2].

Сложность или невозможность установления владельцев криптокошельков связана с тем фактом, что для их регистрации не запрашиваются персональные данные, и даже если криптовалютная биржа собирает их со своих пользователей, то не разглашает такую информацию органам предварительного расследования. Анонимность транзакций побуждает злоумышленников к

[1] Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журнал Высшей школы экономики. 2021. № 3. С. 115.

[2] Коржова И. В., Хан Н. А. Расследование совершаемых в сфере оборота цифровых финансовых активов уголовных преступлений // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2019. № 4. С. 51.

использованию криптовалюты в преступных целях, в том числе для покупки наркотических средств, финансирования терроризма, а также уклонения от уплаты налогов, что влечет рост преступности в данной сфере. Таким образом, даже зная адрес криптокошелька, без его взлома получить данные о его владельце становится невозможным.

Вместе с тем, для квалификации преступления необходимо установление обстоятельств, связанных с событием преступления, то есть места и времени его совершения. Данный процесс в том числе имеет сложности, связанные со спецификой проведения операций с криптовалютой. Так, нередки случаи, когда местонахождение преступника может не совпадать с месторасположением аппаратных и программных средств совершения преступления.

Сейчас установление места преступления в том числе может быть осложнено повсеместным применением злоумышленниками VPN-технологий, способных маскировать IP-адрес используемого для совершения преступления устройства. В том числе стоит отметить, что оборот криптовалюты часто может иметь трансграничный характер, платежи и переводы с криптокошельков могут происходить среди пользователей различных государств. В ходе расследования следует учитывать и тот факт, что время совершения подобного рода преступлений также имеет свои особенности, так как фиксация того или иного события может происходить в различных часовых поясах[1].

Помимо данных сложностей многие эксперты указывают на отсутствие на территории страны органа, уполномоченного оценивать стоимость криптовалют на конкретные дату и время, а это необходимо, так как для квалификации преступления и последующего предъявления лицу обвинения требуется установить причиненный преступлением имущественный ущерб.

Отсутствие методических рекомендаций, обобщенной судебной практики по делам указанной категории, а также необходимых знаний и опыта сотрудни-

[1] Надысева Э. Х. Проблемы расследования преступлений в сфере оборота криптовалют // Вестник экономической безопасности Московского университета МВД РФ имени В.Я. Кикотя. 2019. № 3. С. 226.

ков правоохранительных органов осложняет задачи, связанные с расследованием преступлений в сфере оборота криптовалюты. Необходимо иметь понимание не только о порядке осуществления транзакций с ней, но и в целом о данной платежной системе. Успешное раскрытие подобного рода преступлений возможно лишь при наличии квалифицированных специалистов в области компьютерных и телекоммуникационных технологий, а также криптографии, которых необходимо привлекать для участия в следственных действиях, преимущественно для работы с компьютерной информацией и ее носителями.

Таким образом, в современных реалиях перед органами предварительного расследования стоят довольно сложные задачи, поскольку распространенный оборот криптовалюты создает дополнительные угрозы безопасности личности, общества и государства, что обусловливает необходимость разработки новой методики расследования преступлений, совершаемых в этой сфере, а также совершенствования законодательства в области регулирования криптовалютного рынка.

УДК 343

В. И. КОМИНА[1]

ОТДЕЛЬНЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ ПРОТИВ ЖИЗНИ И ЗДОРОВЬЯ ЧЕЛОВЕКА, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ

Стремительное развитие информационных технологий открыло новые возможности и перспективы для человечества в целом, но также привнесло в жизнь новые угрозы и вызовы. Информационные технологии все чаще стали использоваться в качестве средства совершения преступлений, поскольку позволяют преступникам осуществлять свои преступные действия с любой точки мира. Особо остро стоит вопрос в активном использовании информационных технологий при совершении преступлений против жизни и здоровья человека,

[1] Научный руководитель — ШЕВЕЛЕВА Ксения Владимировна, старший преподаватель кафедры «Правовое обеспечение национальной безопасности» Института кибербезопасности и цифровых технологий Российского технологического университета – МИРЭА.

что предопределило появление новых видов преступлений в данной сфере. К тому же, сотрудники правоохранительных органов отмечают отсутствие четкой системы классификации преступлений, связанных с преследованием в сети «Интернет»[1].

В этой связи, исследование новых видов преступлений, совершаемых посредством информационных технологий, представляется актуальным. Преступления против жизни и здоровья человека, совершаемых с использованием IT-технологий включают в себя такие новые виды преступлений, как:

1. Кибербуллинг и киберпреследование (или киберсталкинг).

Классическая форма травли определяется как акт агрессии или поведение, которое целенаправленно и продолжительное время осуществляется группой или отдельным лицом против жертвы, которая не может этому противостоять в силу определенных обстоятельств (например, из-за психологических особенностей). В последние годы травля приобрела новую форму, которая называется кибербуллинг или онлайн-травля.

Кибербуллинг означает форму психологического насилия, при которой один человек или группа людей намеренно оскорбляют, унижают или запугивают другого человека с помощью сети «Интернет».

В Российской Федерации определение данного понятия дается в письме Минобрнауки России от 14.05.2018 № 08-1184, согласно которому под кибербуллингом понимается преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов[2].

Необходимо отметить некоторые признаки феномена кибербуллинга:

— моральное и психологическое насилие;

---

[1] Тимошкина В. А. Киберсталкинг: современное состояние и меры противодействия на досудебных стадиях уголовного процесса // Вестник Уральского юридического института МВД России. 2023. № 1 (37). С. 26—30.

[2] Методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет» : Письмо Минобрнауки от 14 мая 2018 г. № 08-1184. Доступ из справ.-правовой системы «КонсультантПлюс».

— принуждение жертвы к совершению каких-либо действий;

— запугивание жертвы путем шантажа[1].

Одной из главных проблем расследования данного вида преступления является анонимность и виртуальность субъекта преступления. Зачастую преступника бывает сложно вычислить, поскольку он может использовать поддельные имена, данные, а также пользоваться VPN-сервисом, который меняет IP-адрес, в связи с чем представляется невозможным определить его местоположение.

Хотя кибербуллинг не связан напрямую с физическим насилием, он может иметь более серьезные последствия. Особую опасность представляет участие в экстремистской деятельности и в деятельности других деструктивных группировок («групп смерти» и т.п.) или подстрекательстве к самоубийству молодежи.

Интернет-технологии, обладая широкой доступностью, могут способствовать появлению негативной обстановки для некоторых форм отклоняющегося поведения. В последнее время в качестве новой и растущей проблемы возник новый вид преступления известный как «киберпреследование» (или кибersталкинг).

Данный термин подразумевает под собой систематическое преследование и шантажирование человека в виртуальном пространстве. Чаще всего киберпреследование осуществляется путем размещения компрометирующей информации, угроз и дискредитирующих материалов о жертве на публичных ресурсах, что приводит к ее социальной изоляции и психологическому давлению.

Помимо традиционного преследования, киберпреступники могут использовать более широкий спектр методов, от отслеживания жертв через социальные сети до выдачи себя за определенных лиц (друзей, родителей, правоохранительных органов и т. д.). Жертвами киберпреследования чаще всего стано-

[1] Богомолова А. Г., Кот Е. А. Криминалистические аспекты кибербуллинга как формы деструктивного поведения в сети «Интернет» // Вестник Балтийского федерального университета им. И. Канта. 2023. № 2. С. 25—32. (Серия: «Гуманитарные и общественные науки»).

вятся подростки и молодые люди, которые находятся в более уязвимом положении, так как имеют менее сформированную самооценку и слабо развитые механизмы защиты от таких ситуаций.

На данный момент, в Российской Федерации отсутствуют эффективные инструменты для борьбы с киберсталкингом, что требует усовершенствования уголовного законодательства и введения соответствующих норм в Уголовный кодекс Российской Федерации.

Автор приходит к выводу о том, что уголовная ответственность субъекта за такой вид преступления как киберсталкинг должна наступать лишь в том случае, если у преследуемого есть все основания опасаться совершения насильственных действий по отношению к нему.

Стоит отметить, что приведенные новые виды преступлений (кибербуллинг и киберпреследование) могут иметь серьезные последствия для жертвы, включая психологическую травму, депрессию, суицидальные мысли и даже самоубийство.

Поскольку явление кибербуллинга и киберпреследования является относительно новым явлением в России, сложно понять его суть, определить его виды, причины и установить ответственность. В этой связи серьезной проблемой представляется отсутствие в российском уголовном законодательстве специальной нормы, предусматривающей ответственность за виды преступлений, которые были рассмотрены выше.

С учетом изложенного, отметим, что действующее уголовное законодательство требует советующих изменений, а именно дополнение квалифицирующего признака в виде ч. 3 ст. 119 УК РФ (Угроза убийством или причинением тяжкого вреда здоровью) в следующей редакции: «ч. 3. То же деяние, совершенное с использованием информационно-телекоммуникационной сети, в том числе сети «Интернет»[1].

[1] Амирова Д. К., Куницына Ю. В К вопросу об установлении уголовной ответственности за кибербуллинг // Ученые записки Казанского юридического института МВД России. 2022. № 1 (13). С. 12—16.

Таким образом, проблемы кибербуллинга и киберпреследования требуют всестороннего внимания со стороны общества и государства.

Необходимо принять эффективные меры для предотвращения этих явлений и защиты потенциальных жертв. Одним из важных аспектов борьбы с этими видами преступлений является информирование общественности о последствиях преступлений и способах защиты от них. Это включает в себя проведение просвещение населения (в том числе проведение бесед в образовательных учреждениях с привлечением сотрудников правоохранительных органов) и создание специализированных центров поддержки и консультаций.

2. Киберпреступления, направленные на имплантируемые медицинские устройства и другие формы киберпреступлений, которые могут серьезно повлиять на физическое и психологическое здоровье людей.

Важно отметить, что вопрос кибербезопасности в сфере здравоохранения является гораздо более значимым, чем просто нарушение конфиденциальности личных данных. Здесь возможно не только причинение вреда жизни и здоровью человека, но и летальный исход. При этом угроза может быть, как результатом преднамеренных действий (включая террористические атаки), так и в виде неосторожности (начиная от технической ошибки до сбоя в компьютерной системе).

Имплантируемые медицинские устройства активно применяются для эффективного лечения хронических заболеваний, включая сердечную аритмию и диабет[1]. Сложившаяся ситуация требует повышенного внимания к безопасности имплантируемых медицинских устройств в связи с их распространением и быстрым развитием функций беспроводной связи.

В настоящее время имплантируемые медицинские устройства способны взаимодействовать с внешним программным обеспечением и считывателем по

[1] Перепечина И. О., Перепечин Д. В. Криминалистическое прогнозирование и криминалистическая превенция киберпреступлений в сфере здравоохранения // Пробелы в российском законодательстве. 2020. № 5. С. 265—278.

беспроводной сети. Однако, несмотря на все преимущества, возникает серьезная угроза в виде возможных атак на имплантируемые медицинские устройства, которые могут повлечь прямой вред для пациентов и вызывать серьезные последствия, включая гибель человека. Незаконный доступ, кража, модификация данных или даже отказ в обслуживании этих устройств могут привести к смерти пациентов.

В 2008 году команда исследователей из медицинского центра Бет Исраэль Дьяконесс обнаружила потенциальную уязвимость в системе дефибрилляторов и кардиостимуляторов, которую можно было бы использовать для взлома. Им удалось перепрограммировать эти устройства, что приводило к отключению сердечного ритма или выдаче смертельного электрического разряда. Недавно известный хакер Барнаби Джек продемонстрировал способность задействовать радиосигналы для вмешательства в работу инсулиновых помп. Его эксперименты заключались в том, чтобы вынудить помпу подавать пациенту смертельную дозу инсулина[1].

Поэтому безопасность имплантируемых медицинских устройств становится одной из ключевых проблем, на которую следует обращать особое внимание и предпринимать соответствующие меры для защиты пациентов.

Благодаря стремительному прогрессу технологий, современные имплантируемые медицинские устройства достигли невероятных высот в функциональности. Сегодня пациенты имеют возможность беспроводного управления своими имплантатами с помощью смартфона. Это может быть осуществлено либо путем непосредственного соединения двух устройств посредством Bluetooth, либо с помощью сети «Интернет».

Риск причинения серьезного вреда большинству отдельных пациентов из-за нарушений кибербезопасности их имплантатов в настоящее время незначителен, однако быстрое распространение их использования в сочетании с постоянным развитием функционала значительно увеличивает риск в несколько раз.

[1] Русскевич Е. А. Уголовное право и информатизация // Журнал российского права. 2017. № 8 (248). С. 73—80.

Некоторые пациенты, такие как выдающиеся общественные деятели, в наибольшей степени подвергаются данной опасности. Так, бывший вице-президент США Дик Чейни попросил врачей отключить беспроводной интерфейс WiFi в своем кардиостимуляторе, чтобы снизить возможность политического убийства через кибератаку на его устройство[1].

Стоит отметить, что успешные атаки могут нанести большой вред пациентам и, если о них сообщат в средствах массовой информации, могут несправедливо запятнать репутацию медицинских имплантатов, спасающих жизни.

Необходимо добавить, что проблема защиты имплантируемых медицинских устройств от сбоев и кибератак не должна ограничиваться мерами лишь технического характера — здесь требуется системный подход, включающий в том числе меры правового регулирования.

Таким образом, необходимо внести некоторые изменения в законодательство, а именно в виде дополнения к ч. 2 п. «и» ст.105 УК РФ (Убийство) в следующей редакции: «совершенное с помощью IT-технологий с целью выведения из строя имплантируемых медицинских устройств». Аналогичной нормой необходимо дополнить ч. 2 ст. 111 УК РФ, ч. 2 ст. 112 УК РФ, ч. 2 ст. 115 УК РФ.

Рассмотрев две группы преступлений против жизни и здоровья человека, совершенных с использованием IT-технологий, отметим, что для борьбы с подобными преступлениями в целях обеспечения безопасности граждан, законодателю необходимо внести изменения в действующие нормы УК РФ.

Предложенное позволит урегулировать вопросы обеспечения охраны жизни и здоровья человека путем установления уголовного запрета на использование информационных технологий в качестве средства совершения преступлений.

Стоит отметить, что для эффективной борьбы с преступлениями в исследуемой сфере, необходимы специалисты с глубокими познаниями в области информационных технологий и кибербезопасности. Обучение сотрудников в

[1] Дик Чейни // Комсомольская правда : сайт. URL: https://www.kp.ru/daily/26148.5/3037351/ (дата обращения: 29.10.2023).

области кибербезопасности, проведение исследований и разработка новых методов анализа данных — все это является необходимой составляющей успеха в борьбе с преступлениями против жизни и здоровья человека, совершенные с использованием компьютерных технологий. Кроме того, необходимо создавать специализированные подразделения, которые будут проводить расследование преступлений, совершенных и использованием сети «Интернет».

Важным аспектом борьбы также является сотрудничество с другими государствами и международными организациями. Преступления, совершаемые с использованием информационных технологий, зачастую носят международный характер и требуют совместных усилий для их раскрытия и привлечения виновных к ответственности. Обмен информацией, опытом и методами работы поможет эффективно бороться с этим видом преступности.

УДК 343

А. А. КУЛЬПИН[1]

К ВОПРОСУ ОБ ИНФОРМАЦИИ ОБ УЧАСТНИКАХ СВО В СИСТЕМЕ ОБСТОЯТЕЛЬСТВ, ПОДЛЕЖАЩИХ ИССЛЕДОВАНИЮ И ДОКАЗЫВАНИЮ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 207.3 УК РФ

В течение последних полутора-двух лет трудно переоценить важность противодействия публичному распространению заведомо ложной информации о действиях Вооруженных Сил Российской Федерации, государственных органов, добровольческих формирований, организаций, а также граждан в ходе проведения специальной военной операции на территории Украины (далее по тексту — СВО).

В условиях лавинообразного потока информации дискредитирующего характера (обвинений в использовании новой формы экстремисткой деятельно-

[1] Научный руководитель — КОРШУНОВА Ольга Николаевна, заведующий кафедрой прокурорского надзора и участия прокурора в рассмотрении уголовных, гражданских и арбитражных дел Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, профессор.

сти, якобы имевших место убийствах мирных граждан, массированных обстрелах населенных пунктов, уничтожении либо повреждении жизненно важных объектов инфраструктуры, жестоком обращении с военнопленными, мародерстве и др.) перед государством встала серьезная задача, связанная с обеспечением необходимой правовой защиты прав и законных интересов участников СВО, а также их родственников.

Думается, что особую опасность распространение ложной информация представляет для наиболее уязвимых в этом смысле групп населения, прежде всего - молодежи и подростков, которые в силу возраста оказываются наименее защищенными от воздействия манипулятивных техник. Особенно активно указанная деятельность осуществляется с использованием различных Интернет-ресурсов.

Как справедливо отмечают исследователи С.П. Синявская и Е.Н. Панкова, молодые люди нередко становятся жертвами целенаправленного внушения и обмана со стороны распространителей фейков, что приводит к их дезориентации и социальной изоляции. В результате подростки оказываются вовлеченными в деструктивную деятельность и сами начинают тиражировать ложную информацию[1].

Фейковые новости об СВО используются как инструмент пропаганды, направленной на подрыв доверия граждан к легитимности действий государства. Неконтролируемое распространение такой дезинформации несет угрозу национальной безопасности и социальной стабильности. Как справедливо подчеркивает О.Н. Коршунова, особая опасность экстремизма и любых проявлений экстремистской деятельности обусловлена тем, что он нацелен на подрыв основ конституционного строя, межнационального и межконфессионального согласия[2].

[1] Синявская С. П., Панкова Е. Н. Особенности анализа экстремистского дискурса на современном этапе // Криминалистъ. 2022. № 2 (39). С. 110.

[2] Коршунова О. Н. Противодействие экстремизму, терроризму и их финансированию как комплексное направление деятельности органов прокуратуры // Вопросы российского и международного права. 2020. Том 10, № 11А. С. 122–139.

Одним из наиболее оптимальных решений указанных проблем явилось дополнение УК РФ статьей. 207.3, установившей ответственность за преступное публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами государства своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации.

Указанное решение, а также дополнение Кодекса об административных правонарушениях Российской Федерации статьей 20.3.3, установившей ответственность за аналогичные действия, если они не содержат признаков уголовно наказуемого деяния, явились своеобразным стимулом для оперативного формирования практики противодействия недостоверной информации деструктивного характера об участниках СВО и их действиях на территории Украины, о чем свидетельствуют официальные статистические данные, согласно которым с начала спецоперации возбуждено 180 уголовных дел по признакам преступления, предусмотренного ст. 207.3 УК РФ[1].

Вместе с тем, результаты изучения правоприменительной практики дают основание для вывода о существенных проблемах, возникающих в ходе расследования рассматриваемого преступления. Причиной сложившейся ситуации явилась как относительная новизна ст. 207.3 УК РФ, так и недостаточная разработанность научно обоснованных рекомендаций по расследованию этого противоправного деяния.

Правовая природа расследования преступлений предполагает неукоснительное следование нормам закона и принципу верховенства права. В этой связи представляется очевидным, что легитимность процессуальных решений на стадии предварительного расследования напрямую обусловлена корректным определением ключевых параметров (предмета и пределов) доказывания. С учетом изложенного, полагаем обоснованной позицию ряда ученых о том, что в рамках прокурорского надзора приоритетной задачей является проверка

[1] С начала спецоперации в РФ возбудили 180 дел о дискредитации армии // Право. РУ : сайт. URL: https://pravo.ru/news/244599/ (дата обращения: 08.11.2023).

обоснованности действий следователя в части формулирования предмета и границ доказывания. Лишь после подтверждения правомерности данных действий представляется возможным объективно оценить законность и обоснованность последующих процессуальных решений, принятых по итогам досудебного производства[1].

Само рассмотрение прокурором материалов уголовного дела о преступлении, связанном с распространением фейков о СВО, требует оценки полноты установления ряда ключевых обстоятельств. На начальной стадии расследования сведения об этих обстоятельствах носят, как правило, фрагментарный характер. Однако к моменту утверждения обвинительного заключения они должны быть исследованы и подтверждены в максимально возможном объеме, поскольку отсутствие в материалах дела тех или иных данных (доказательств) будет свидетельствовать о пробелах предварительного расследования в части установления и доказывания подлежащих исследованию обстоятельств.

Но что же из себя представляет данное явление, получившее в последние годы название — фейк? Под фейковыми новостями (англ. fake news) понимается заведомо ложная информация, имеющая ярко выраженную негативную коннотацию, преднамеренно распространяемая под видом достоверных новостей с целью введения аудитории в заблуждение и манипулирования общественным мнением[2].

Их структурными признаками являются: намеренное искажение действительности; имитация формата подлинных новостных сообщений; эмоциональная окрашенность контента; отсутствие ссылок на источники информации.

Руководствуясь результатами изучения судебно-следственной практики, полагаем, что система обстоятельств, подлежащих исследованию и доказыванию, о такой информации может быть представлена следующим образом:

---

[1] Особенности прокурорского надзора за законностью выявления и расследования преступлений, связанных с размещением экстремистских материалов в сети «Интернет» : учебное пособие / О. Н. Коршунова, Е. Л. Никитин, Е. Б. Серова ; под общ. ред. О. Н. Коршуновой. 2-е изд., перераб. и доп. СПб., 2013. С. 45.

[2] Галяшина Е. И., Никишин В. Д., Богатырев К. М., Пфейфер Е. Г. Фейковизация как средство информационной войны в интернет-медиа : научно-практическое пособие. М., 2023. С. 19.

1. Имел ли место факт публичного распространения под видом достоверной заведомо ложной информации, указанной в диспозиции ст. 207.3 УК РФ:

1.1. Информация о чьей деятельности публично распространена под видом достоверной:

— Вооруженных Сил Российской Федерации, в том числе конкретного подразделения (подразделений), принимающего участие в СВО;

— государственного органа Российской Федерации, деятельность которого имеет непосредственное отношение к СВО (в частности, Росгвардии);

— добровольческого формирования, принимающего участие в СВО;

— военной либо иной организации, участвующей в СВО (например, частной военной компании «Вагнер»);

— конкретного военнослужащего (военнослужащих), иного физического лица-участника (участников) СВО.

1.2. Каково содержание указанной информации:

— о целях проведения СВО (например, что она проводится с целью захвата территории Украины, ликвидации ее независимости, изменения политического и общественного строя);

— характере боевых действий на территории Украины (например, что они носят фашистский характер);

— гибели, в том числе массовой, мирного населения в результате проведения СВО;

— актов насилия в отношении мирного населения Украины, совершенных конкретными подразделениями Вооруженных Сил Российской Федерации (военнослужащими, иными участниками СВО);

— числе жертв среди российских граждан в результате действий Вооруженных Сил Украины;

— числе взятых в плен российских солдат в результате действий Вооруженных Сил Украины;

— количестве уничтоженной и поврежденной российской военной техники;

— «победоносных» действиях Вооруженных Сил Украины и (или) «провале» СВО Вооруженными Силами Российской Федерации как в целом, так и в ходе конкретных боевых действий (операции);

— иная информация[1].

1.2. В чем выражается заведомая ложность информации, указанной в диспозиции ст. 207.3 УК РФ:

— была ли размещена (опубликована) официальная информация о событии (событиях), связанном с проведением СВО (например, об участии конкретного подразделения Вооруженных Сил Российской Федерации в той или иной боевой операции), источник этой информации и ее содержание;

— предшествовало ли публичное распространение заведомо ложной информации о событии (событиях), связанном с проведением СВО (например, о результатах конкретной боевой операции) размещению (опубликованию) официальной информации об этом же событии. Если нет, то каков временной интервал между размещением (опубликованием) официальной информации и распространением заведомо ложной информации.

Так, одно из уголовных дел по признакам преступления, предусмотренного ст. 207.3 УК РФ, было возбуждено после размещения в сети «Интернет» на одном из городских форумов Нижнего Новгорода видеоролика о событиях в городе Буча (апрель 2022 года). Предварительным расследованием установлено, что видеоролик был размещен до официального опровержения Министерством обороны Российской Федерации информации о событиях, произошедших в городах Ирпень и Буча. Указанное обстоятельство, а также отсутствие у подозреваемого умысла на распространение фейков о действиях российской армии на территории Украины явилось основанием для прекращения уголовного дела[2].

---

[1] Кульпин А. А. К вопросу о личности преступника в системе обстоятельств, подлежащих установлению, при расследовании преступления, предусмотренного ст. 207.3 УК РФ // Вопросы Российской юстиции. 2023. № 27. С. 435—436.

[2] В России впервые прекратили дело о фейках о действиях армии // РИА Новости : сайт. URL: https://ria.ru/20221027/feyki-1827242649.html (дата обращения: 08.11.2023).

— в чем конкретно выражается несоответствие официальной и заведомо ложной информации о событии (событиях), связанном с проведением СВО;

1.3. В чем выражается публичность распространения заведомо ложной информации, указанной в диспозиции ст. 207.3 УК РФ о событии (событиях), связанном с проведением СВО.

Результаты изучения судебно-следственной практики свидетельствуют о том, что при определении понятия «публичность» правоприменители руководствуются разъяснениями Верховного Суда Российской Федерации, согласно которым распространение заведомо ложной информации, указанной в диспозициях ст. 207.1 и 207.2 УК РФ, следует признавать публичным, если эта информация адресована группе или неограниченному кругу лиц и выражена в любой доступной для них форме (например, в устной, письменной, с использованием технических средств)[1].

Таким образом для того, чтобы определить, является ли распространение указанной в диспозиции ст. 207.3 УК РФ информации публичным, необходимо установить:

— кому была адресована заведомо ложная информация: группе, состоящей из двух и более человек или неограниченному кругу лиц;

— в какой форме она была выражена: устной (например, в ходе выступления, беседы), письменной (например, путем ее опубликования в средствах массовой информации, листовках), с использованием технических средств (например, посредством размещения в сети «Интернет»[2]).

Приведенный перечень обстоятельств, подлежащих установлению, не является исчерпывающим. В зависимости от способа совершения преступления и складывающейся в процессе расследования следственной ситуации может

[1] Обзор по отдельным вопросам судебной практики, связанным с применением законодательства и мер по противодействию распространению на территории Российской Федерации новой коронавирусной инфекции (COVID-19) № 2: утв. Президиумом Верховного Суда Российской Федерации 30 апреля 2020 г. Доступ из справ.-правовой системы «КонсультантПлюс.

[2] Кульпин А. А. Использование высоких технологий для публичного распространения заведомо ложной информации, предусмотренной ст. 207.3 УК РФ// Вопросы Российской юстиции. 2023. № 26. С. 357.

возникнуть необходимость установления иных обстоятельств. Вместе с тем, представляется, что использование указанного перечня следователем при планировании расследования и прокурором при изучении материалов уголовного дела, поступивших с обвинительным заключением, будет способствовать обеспечению необходимого уровня законности предварительного расследования по всем фактам противоправного поведения виновных, а также уровня эффективности прокурорского надзора в данном направлении.

УДК 343

К. А. ЛЕБЕДЕВА[1]

СОВЕРШЕНСТВОВАНИЕ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ (часть 2 статьи 128.1 УК РФ)

Согласно официальным данным МВД России, каждое третье преступление совершается с использованием информационно-коммуникационных технологий. В этой сфере зарегистрировано на 29,2% преступлений больше, чем в январе-сентябре прошлого года[2].

К преступлениям, совершаемым в данной сфере, можно отнести мошенничество, вмешательство в работу компьютерных сетей, несущее вредоносный характер (установка вредоносного программного обеспечения, взлом паролей и иных конфиденциальных сведений, и др.), а также распространение противоправной информации (клевета, материалы, содержащие порнографический характер в отношении несовершеннолетних, ложное сообщение о терроризме и др.)[3].

---

[1] Научный руководитель – ВАСИЛЬЕВ Федор Юрьевич, доцент кафедры уголовного процесса Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь–сентябрь 2023 года. URL: https://xn--b1aew.xn--p1ai/reports/item/42989123/ (дата обращения: 01.11.2023).

[3] Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб., 2018. С. 8.

Сложность квалификации деяний, предусмотренных ч. 2 ст. 128.1 УК РФ, заключается в выявлении факта клеветы, а также в привлечении к ответственности преступника, поскольку существует значительное количество серверов, благодаря которым лица совершают преступные деяния и остаются анонимными или возраст преступника не позволяет привлечь его к ответственности.

В связи с массовостью использования социальных сетей частыми стали случаи безнаказанного поведения лиц, которое заключается в распространении информации, которые, так или иначе, негативно сказываются в отношении других лиц, тем самым, посягают на их честь и достоинство, причем далеко не всегда преподносимая медиа пространству информация является достоверной.

Для правильной квалификации данного преступления стоит обозначить, что клеветой признается распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

В судебной практике очень остро стоит вопрос о привлечении к уголовной ответственности именно по ч. 2 ст. 128.1 УК РФ. Явление клеветы перемежается с такими явлениями как честь, достоинство и репутация, которые подразумевают защищаемые законом, социальные блага, нарушение которых наносит серьезный моральный вред свободе действий и общественному положению посредством создания неблагоприятного впечатления[1].

При этом, стоит отметить, что, учитывая важность данных понятий, на которые посягает преступник, они не закреплены и в законе, и в словаре понятия «честь» и «достоинство» отождествляются.

Отдельное внимание стоит уделить месту распространения клеветы, согласно рассматриваемому составу преступления. На данный момент социальные сети, мессенджеры закрепились в жизни общества. Согласно данным,

[1] Стриганова Т. М. Защита чести, достоинства и деловой репутации граждан // Вестник науки : международный научный журнал. 2022. № 1 (46), Т. 4. С. 194.

опубликованным в инструментах планирования рекламы ведущих социальных медиа платформ, на начало 2023 года в России насчитывалось 91,50 млн пользователей в возрасте 18 лет и старше, что соответствует 79,9 % от общей численности населения в возрасте 18 лет и старше[1].

Исходя из указанных данных можно сделать выводы о том, что преимущественное количество населения пользуется социальными сетями, а также зарегистрированных в социальных сетях несовершеннолетних пользователей 20,1 %, что может послужить значительному росту преступлений в данной сфере.

В качестве субъекта данного преступления выступает физическое вменяемое лицо, достигшее ко времени совершения преступления шестнадцатилетнего возраста.

В связи с развитием информационных технологий, вовлеченность пользователей, которые, на момент познания ими окружающей их среды, не достигли возраста уголовной ответственности также заметно прогрессирует. Не приобретая в полной мере навыков коммуникации, общих принципов нравственности и морали, дети начинают познавать ту оболочку сети, которая является самой легкодоступной - социальные сети, «Интернет», иные информационно-телекоммуникационные сети. Из-за этого восприятие мира складывается иначе и девиантное поведение среди подростков прогрессирует.

Из-за неполностью сформировавшейся психики у несовершеннолетних, они легко поддаются оказываемому на них влиянию, вследствие чего могут принимать необдуманные решения и совершать преступные деяния, не подозревая того, что могут совершать что-то противоправное.

Представление заведомо ложной информации посредством информационно-телекоммуникационных сетей стало куда более доступно. И в данном

[1] Цифровой портал: Цифра 2023: Российская Федерация. https://datareportal.com/reports/digital-2023-russian-federation (дата обращения: 30.10.2023).

случае речь идет не просто о текстовых перепалках в комментариях, а об информации, которая напрямую посягает на свободу, честь и достоинство личности.

Чаще всего необдуманные, в порыве гнева написанные или изложенные в виде аудио- или видеоматериала информация, содержащая ложные сведения, может привести к тяжким последствиям. Причем касается это не только обычных пользователей, но и лиц, для которых пользование информационно-телекоммуникационных сетей представляет из себя деятельность, направленную на получение заработка. В данном случае речь идет про блогеров – людей, занимающихся ведением «блога», и систематически публикующих в нем записи[1].

Занимаясь публичной деятельностью, блогеры имеют большое влияние на людей, которые за ними наблюдают – подписчики, заключающееся в том, что подписчики следят за жизнью этих людей, оказывают им поддержку в виде моральной, а порой и в виде материальной составляющей.

К сожалению, далеко не всегда публичное положение сказывается положительно для блогера и его аудитории. Неизбежны конфликтные ситуации как между подписчиками, так и между медийными лицами. Учитывая отсутствие жесткой цензуры в социальных сетях некоторые пользователи позволяют себе отстаивать свои интересы или интересы лица, за которым они следят, в не самой приятной манере, переходя на личности, а порой распространяя ложную информацию, несущую вредоносный характер, посягающую на честь и достоинство человека.

Исходя из изложенного автором предлагается внесение следующих изменений, позволяющих усовершенствовать уголовную ответственность за совершение преступления по ч. 2 ст. 128.1 УК РФ:

1) Снижение возраста привлечения к уголовной ответственности с шестнадцати до четырнадцати лет;

[1] Толковый словарь русского языка / С. И. Ожегов. URL: https://ozhegov.textologia.ru/definit/bloger/?q=742&n=206422 (дата обращения: 31.10.2023).

2) Увеличение санкции для лиц, занимающихся деятельностью направленную на получение заработка в социальных сетях, поскольку публично распространяя ложную информацию, они оказывают негативное влияние на лица, в отношение которого данная информация использована, а также в отношение аудитории, которая, под воздействием чужого влияния, может вести себя неадекватно и также совершать противоправные действия (т. е. в данном случае блогер будет являться подстрекателем, а пользователь исполнителем).

Благодаря данным изменениям в уголовном законодательстве пользователи социальных сетей будут следить за тем, что они распространяют в массы и понимать всю суть ответственности, которая может возникнуть в случае игнорирования установленных норм.

УДК 343

В. В. МАКАЕВА[1]

ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ

XXI век — это век развития технологий. С каждым годом человечество совершенствуется в области науки и техники, достигает новых высот. Популярность интернета и социальных сетей растет, люди размещают там фотографии, делятся новостями и знакомятся с другими. Однако на просторах социальных сетей мы можем встретить злоумышленников, пользующихся такой информацией в личных, и чаще всего в корыстных целях. Огромное количество противоправной информации, находящейся в сети «Интернет», ежедневно просматривается миллионами пользователей, к числу которых относятся несовершеннолетние.

Чем же обуславливается огромный ущерб от преступлений в социальных сетях. Мы можем выделить несколько обстоятельств:

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

1) Отсутствие цифровой грамотности у людей. Человек нередко забывает основные правила безопасного пользования сетью интернет, благодаря чему и становится легкой «добычей» для злоумышленников.

2) Большой охват аудитории. Популярность социальных сетей растет с каждым днем, включая не только подростков, но и более взрослое поколение. Например, аудитория социальной сети «ВКонтакте» в России составляет 89,18 млн человек в месяц.

3) Относительная анонимность в соцсетях. Социальные сети «дарят» людям возможность скрыть страну, возраст и даже имя, чем часто пользуются мошенники.

4) Огромной проблемой также является не всегда эффективная блокировка страниц с противоправной информацией, а именно быстрое появление новых сайтов. Все как у гидры, отрезаешь одну голову-вырастает три вместо нее.

В наше время социальные сети могут выступать в двух аспектах: в качестве способа совершения преступления и в качестве места совершения противоправных деяний.

Возможно выделить наиболее часто совершаемые преступления с использованием социальных сетей:

Мошенничество — это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием (ст.ст. 159 и 159.6 УК РФ). Это, пожалуй, один из самых распространенных видов преступления в социальных сетях. Схемы злоумышленников различны, они могут взломать страницу вашего знакомого и написать вам с просьбой дачи денег или написать от имени руководителя сообщества о возможности выигрыша и это лишь некоторые примеры их схем. Всегда стоит помнить о правилах собственной безопасности, чтобы не попасться на уловки мошенников.

В середине 2010-х годов нашу страну захлестнула волна «групп смерти»: «Синий кит», «Разбуди меня в 4:20» и многие другие группы, основной целью которых было доведение подростков до самоубийства. Всех участников направляли кураторы в социальных сетях и давали различные задания. При

попытке выхода из игры ребята получали угрозы себе и своим близким. Одним из наиболее известных организаторов является Филипп Лис, осужденный по ст. 110. 1 УК РФ за склонение к совершению самоубийства. Несмотря на действия правоохранительных органов, данные группы существуют и в наше время, хоть и не предаются широкой огласке.

В современном мире также преступлением будут клевета и оскорбление в социальных сетях. Под оскорблением понимаются действия, которые характеризуются унижением достоинства человека, выражающаяся в неприличных фигурах речи часто с использованием нецензурной брани. Клеветой называется распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

Как понятно из определения, данного в статье УК РФ, клеветой будет признаваться только опубликование сведение, ложность которых знал распространитель. Часто люди не осознают, что социальная сеть — это тоже общественное пространство, где за оскорбление другого человека или клевету тебя могут привлечь к ответственности.

Одним из наиболее опасных преступлений, совершаемых с использованием социальных сетей, будет распространение экстремистских материалов.

Понятие экстремизма определено в Федеральном законе от 25.07.2002 № 114-ФЗ (ред. от 28.12.2022) «О противодействии экстремистской деятельности», из которого мы можем выделить, что экстремизмом признается некая приверженность к крайним, радикальным взглядам или позициям, выражающаяся в деяниях, не пересекающих определенные конституцией рамки, но также в общественно опасных деяниях, которые подрывают устои общества и государства, угрожают жизни и здоровью человека.

В социальных сетях создаются различные группы экстремисткой направленности, ведется вербовка лиц. Наиболее печально то, что молодежь, которая является основной аудиторией в сети «Интернет», подвергается влиянию этой информации и идет на поводу у злоумышленников, не осознавая, чем это может закончится (ст. 280 УК РФ).

Также в социальные сети перешли преступления, связанные с оборотом наркотических и психотропных веществ. Согласно статистике МВД Российской Федерации, число данных деяний на просторах сети «Интернет» составило почти 7 тысяч, что показывает рост показателя по сравнению с прошлым январем на 85,1 %[1].

Нередко люди, не только не знают о вреде наркотиков для здоровья человека, но и мне понимают, что российским уголовным законодательством за незаконное приобретение, хранение, перевозку, изготовление, переработку наркотических средств, психотропных веществ или их аналогов, а также за их незаконное производство, сбыт и пересылку предусмотрена уголовная ответственность по ст. 228-228.1 УК РФ.

Выделив наиболее популярные и часто совершаемые преступные деяния в социальных сетях, возникает вопрос, как же в таком случае пользователю обезопасить себя? Мы можем предложить некоторые рекомендации:

— Не размещайте большое количество личной информации в социальных сетях. Именно этим чаще всего и пользуются злоумышленники.

— Перед тем, как принять приглашение о вступлении в какое-либо подозрительное сообщество, проверьте информацию по нему.

— Если вам написали со страницы вашего знакомого, например с просьбой о деньгах, то лучше поговорите лично с этим человеком или отправьте ему сообщение в другой мессенджер. В таком случае, вы не только обезопасите свои средства, но и уведомите друга о взломе его страницы.

— Повысьте свою правовую культуру. Почитайте статьи в интернете, различную нормативную литературу, все это поможет вам правильно анализировать, как действия окружающих, так и свои собственные.

Борьба с преступностью в социальных сетях ведется ежедневно. Однако не всегда быстро можно обнаружить те или иные нарушения законодатель-

[1] Балабаева Е. В России растет наркоторговля в интернете // Парламентская газета. 2023. 4 марта. URL: https://www.pnp.ru/social/v-rossii-rastet-narkotorgovlya-v-internete.html (дата обращения: 09.11.2023).

ства. Но несмотря на данные факты, с каждым годом правоохранительные органы работают все эффективнее, что помогает выявлять и предупреждать все большее количество преступлений.

Следует также повышать «цифровую грамотность населения», так как большое количество преступлений, особенно в сфере мошенничества, происходят из-за незнания граждан правил, которые помогут защитить их от злоумышленников.

Важным аспектом является совершенствования в сфере законодательства, направленные на предупреждение совершения преступлений с использованием социальных сетей.

УДК 343

У. П. МАЛЬЦЕВА,
В. Д. ФАБРИЧНОВА[1]

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК СПОСОБ НАРУШЕНИЯ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ: ПРОБЛЕМЫ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ

Статья 23 Конституции Российской Федерации закрепляет право человека на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, что подразумевает под собой ее охрану от любого внешнего вмешательства, в том числе и путем установления в ст. 137 УК РФ ответственности за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Исходя из буквального толкования диспозиции данной нормы, под частной жизнью законодатель понимает как личную, так и семейную тайны. По

[1] Научный руководитель — РАХМАНОВА Екатерина Николаевна, заведующий кафедрой уголовного права Северо-Западного филиала Российского государственного университета правосудия, доктор юридических наук, доцент.

этому поводу представляет интерес позиция Конституционного суда Российской Федерации, выраженная в Определении Конституционного Суда Российской Федерации от 28.06.2012 № 1253-О[1].

В нем закреплено, что в понятие «частная жизнь» включена та область жизнедеятельности человека, которая относится к конкретному лицу, касается только его и не подлежит контролю со стороны общества и государства. Следовательно, только само лицо вправе определить, какие именно сведения должны оставаться в тайне, а потому и сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия данного лица, как того требует закон. Правомерным является собирание и распространение сведений о частной жизни лица только в установленном законном порядке и лишь в отношении тех данных, которые уже официально кому-либо доверены самим лицом. Иное приводило бы к произвольному, не основанному на законе, вторжению в сферу частной жизни лица, сужало бы понятие частной жизни и объем гарантий ее защиты.

В теории разрешение поставленного вопроса относительно понятно, но приходится признать, что в реальной жизни установить границы личной неприкосновенности, достаточно сложно. Исходя из позиции Конституционного суда Российской Федерации, создается впечатление, что законом охраняются только те сведения, которые человеком не доверены никому. Получается, что близкие, друзья, коллеги и иные лица, которые получили эту информацию в ходе разговора с человеком и распространили ее неопределенному кругу лиц, не подлежат ответственности ввиду того, что данные сведения уже не являлись охраняемой законом тайной.

Из разъяснений Конституционного Суда Российской Федерации остается неясным, что понимать под сведениями, которые «официально кому-либо доверены» и каким образом другой человек должен понять «границы» частной жизни лица, с которым он, например, ведет диалог или переписку

[1] Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации : Определение Конституционного Суда Российской Федерации от 28 июня 2012 г. №1253-О. Доступ из справ.-правовой системы «КонсультантПлюс.

в социальной сети. Более того, в каких случаях мы можем говорить о том, что согласие лица на распространении личной информации о нем презюмируется — достаточно ли просьбы лица не оглашать какие-либо данные о нем, чтобы нарушение такого пожелания стало основанием для привлечения к уголовной ответственности?[1].

На бытовом уровне чаще всего это не влечет за собой каких-либо негативных последствий. Но разрешение подобных вопросов имеет особое значение для публичных личностей – как для государственных и муниципальных служащих, так и для знаменитостей в сфере шоу-бизнеса, поскольку их жизнь часто представляет особый интерес для большого количества людей, а нарушение личной и семейной тайны таких лиц может повлечь за собой серьезные последствия, в том числе и для их близких.

Таким образом, пределы частной жизни являются субъективной и оценочной категорией, устанавливаемой либо самим человеком, чьи права и законные интересы могут быть нарушены, либо при рассмотрении уголовного дела судом.

Мы согласны с дефиницией, приводимой А.А. Аведяном, который сформулировал рассматриваемое понятие, как совокупность личных, духовных и физиологических составляющих жизни конкретного лица, не противоречащих действующему законодательству, определяемых самим человеком в своем сознании как тайну[2].

Данная проблема актуализировалась в последние годы в связи с вмешательством в личную жизнь посредством информационно-телекоммуникационных сетей[3]. И делается это буквально «в один клик»: город проживания, место

---

[1] Конорезов Н. А. Уголовно-правовая характеристика нарушения неприкосновенности частной жизни в сети «Интернет» // Гуманитарные, социально-экономические и общественные науки. 2023. № 3. С. 143.

[2] Аведян А. А. Юридическая природа обеспечения права на неприкосновенность частной жизни // ЮП. 2012. № 2 (51). С. 96.

[3] Рахманова Е. Н. Уголовно-правовые способы защиты персональных данных личности // Уголовная политика и правоприменительная практика : сборник статей по материалам X Международной научно-практической конференции (Санкт-Петербург, 27 октября 2023 г.) / под ред. Е. Н. Рахмановой. СПб., 2023. С. 159—166

работы и учебы, семейное положение, внешность человека и его близких и многое другое[1].

Киберпространство является своеобразным «хранилищем» сведений о большинстве людей. Причем, далеко не каждый пользователь осознает, что он подвергает опасности свои данные, регистрируясь на различных платформах, вводя «безобидные» сведения на сайты и т.п. За последние годы получили распространение самые разнообразные способы нарушения неприкосновенности частной жизни с использованием киберпространства. В числе наиболее распространенных способов совершения таких деяний - взлом страниц в социальных сетях и отдельных приложений с личными данными, рассылка электронных писем и текстовых сообщений под видом надежного источника с вредоносной ссылкой, которая копирует все данные устройства и др.

Ввиду этого возникает вопрос о законности собирания таких данных. Проблема состоит в том, что подобные действия не подпадают под диспозицию ст. 137 УК РФ, так как, по сути, хранятся в общем доступе. Например, в Сети есть различные сервисы по «проверке» любого автомобиля по государственному номеру, позволяющие узнать собственника, его дату рождения, историю покупки и иных сделок с машиной, случаи дорожно-транспортных происшествий вплоть до минут их совершения. Общедоступными являются фотографии искомого автомобиля как на дороге, так и около мест жительства или работы владельца. Также существуют приложения, определяющие по номеру телефона имя того, кому он принадлежит, и то, как данный пользователь записан в контактах у других абонентов.

То же самое можно сказать и о еще одном способе нарушения указанного права, которым служит рассылка личных фотографий, чаще всего – интимного характера, определенным лицам, которые знакомы с предполагаемым потерпевшим.

[1] Ильина М. Г., Биличенко И. В. Уголовно-правовые аспекты нарушения неприкосновенности частной жизни с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») // The Newman in Foreign policy. 2021. № 60 (104). С. 28.

Одной из последних инноваций последних лет является использование искусственного интеллекта. Искусственный интеллект — комплекс программ, способных имитировать поведение человека, выполнять задачи и функции творческого характера и постепенно обучаться, применяя для этого собранную информацию[1].

С помощью правильно заданного запроса, в том числе, с указанием того, что и в каком формате требуется получить, нейросеть способна раскрыть личные данные другого человека. Причем, технологии все равно, какую информацию запрашивает пользователь, важен лишь верно заданный формат, и сведения в ответе будут предоставлены без каких-либо ограничений, в том числе, нежелательные для огласки.

В результате использования искусственного интеллекта для личных целей возникает ситуация, когда человек может сам себя скомпрометировать, с его помощью отправляя изображения, тексты и другие материалы, поскольку эти данные становятся рабочим материалом искусственного интеллекта. Что, в свою очередь, позволяет другим лицам получить и использовать их, в том числе, и в преступных целях.

Сложность защиты личных данных, полученных при помощи искусственного интеллекта, состоит в том, что законодательного регулирования пока нет, а это приводит к серьезным проблемам в сфере защиты личных прав человека.

На данный момент использование искусственного интеллекта регулируется «мягким правом» путем принятия различных международных документов рекомендательного характера. Среди них можно отметить Рекомендации по искусственному интеллекту Организации экономического сотрудничества и развития 2019 года, Заявление министров экономики стран-участниц G20, в котором были одобрены принципы развития искусственного интеллекта, выдвинутые в упомянутых выше Рекомендациях, Окинавскую хартию глобального информационного общества 2000 года[2].

---

[1] Пройдаков Э. М. Современное состояние искусственного интеллекта // Науковедческие исследования : сборник научных трудов / отв. ред. А. И. Ракитов. М., 2018. С. 130.

[2] Рахманова Е. Н., Пономарева Е. В. Европейская конвенция по искусственному интеллекту: предпосылки создания и перспективы // Актуальные проблемы законодательства

В нашей стране делаются только первые шаги в данном направлении. Так, Федеральный закон «О персональных данных» содержит специальные положения об обработке персональных данных с участием искусственного интеллекта[1], принимаются законы в сфере здравоохранения, образования и т.д. Создана рабочая группа по созданию закона о регулировании искусственного интеллекта.

Что же касается сферы действия уголовного закона, то нужно отметить, что пока законодатель и ученые не готовы решить вопрос об уголовной ответственности лиц, использующих искусственного интеллекта. Хотя высказываются самые разные предложения, в том числе, признать искусственного интеллекта субъектом преступления, или рассматривать использование искусственного интеллекта как способ/место совершения преступления и т. п.[2]

Мы полагаем, что ошибочно считать совершение преступлений в киберпространстве или с помощью искусственного интеллекта признаком, характеризующим место совершения противоправного деяния. Как следует из сущности факультативных признаков объективной стороны, данная характеристика преступления относится скорее к способу совершения правонарушения.

Возвращаясь к проблемам использования киберпространства с целью сбора личной информации, проблема, на наш взгляд, состоит в том, что хотя с помощью IP-адреса, определяющего конкретную сеть и устройство, достаточно легко идентифицировать местоположение любого пользователя, но благодаря развитию цифровых технологий, лицо, совершившее правонарушение, может с легкостью, не обладая специальными знаниями, скрыть свое местоположение. Это способствует анонимной преступности в Сети и затрудняет раскрытие и расследование подобных нарушений закона[3].

и правоприменительной практики в Республике Казахстан и зарубежных странах : материалы Международной научно-практической конференции, посвященной 30-летию университета «Туран» (Алматы, университет «Туран», 11 ноября 2022 г.). Алматы, 2023. С. 24.

[1] О персональных данных : Федерального закона от 27 июля 2006 г. № 152-ФЗ : текст с изм. и доп. 6 февр. 2023 г. Ст. 6. Доступ из справ.-правовой системы «Консультант-Плюс».

[2] Хилюта В. В. Искусственный интеллект и уголовное право: приемлем ли палингенезис в условиях цифровизации //Журнал российского права. 2023. № 9. С. 90—103.

[3] Рахманова Е. Н. К вопросу об определении места совершения киберпреступления // Следственная деятельность: наука, образование, практика : тезисы докладов III Международной научно-практической конференции (Минск, 9 июня 2023 г.). Минск, 2023. С. 69.

Проблема состоит еще и в том, что потерпевший может даже не догадываться о совершаемых в отношении него противоправных действиях. Поэтому угрозу для охраняемых законом интересов представляют умышленные действия лица в целях получения тех или иных сведений о частной жизни человека, которые совершаются в качестве подготовительной стадии к совершению более опасного деяния. К примеру, сбор информации о предполагаемой жертве упрощает совершение таких преступлений, как убийство, изнасилование, вымогательство, похищение человека и другое.

Для распространения, как части объективной стороны преступления, предусмотренного ст. 137 УК РФ, могут использоваться следующие способы: публикация мультимедиа данных или информации, содержащей личную или семейную тайну, в Интернет-пространстве, впоследствии чего такие сведения становятся доступными неограниченному кругу лиц, которые имеют возможность их сохранить и распространить в дальнейшем.

Хотелось бы еще отметить существование некоторой коллизии между ст. 24 Конституции Российской Федерации и ст. 137 УК РФ, диспозиция которой не содержит такие действия как хранение и использование информации о частной жизни лица, что представляется нам нелогичным. Ведь собирание сведений само по себе подразумевает их последующее хранение лицом в течение какого-либо периода времени, а вот хранение может осуществляться и без сбора, потому, по нашему мнению, подлежит выделению в качестве самостоятельного альтернативного признака объективной стороны данного преступления.

Аргументом в пользу такой точки зрения служит позиция, выраженная в Определении Конституционного Суда Российской Федерации от 28.06.2012 № 1253-О, в котором установлено недопущение «сбора, хранения, использования и распространения» сведений о частной жизни лица без его согласия. К тому же наличие у человека такой информации впоследствии может лечь в основу распространения ее другими лицами. Например, при любом виде

«утечки» данных с того носителя, на котором они хранятся, часто — с мобильного устройства или компьютера.

Интересным представляется оценка судом характера общественной опасности рассматриваемого правонарушения в отношении разных категорий потерпевших. Суд при разрешении дела должен принимать во внимание все обстоятельства, имеющие отношение к преступлению: преследуемые цели, используемые способы, характер нарушенной тайны и «уровень» ее защиты самим человеком, а также тяжесть наступивших или возможных последствий, его статус и личное отношение пострадавшего к «утечке» данных.

По нашему мнению, правоприменителю необходимо исходить не столько из размера последствий, сколько из субъективной важности нарушенного права для самого потерпевшего, так как в нашем государстве презюмируется равенство прав и свобод всех граждан, а значит, право на неприкосновенность частной жизни публичного человека не может быть поставлено выше такого же права другого лица.

Чаще всего собирание сведений о частной жизни публичного лица осуществляется с корыстной целью, обычно – для совершения в последующем вымогательства, в то время как для других категорий лиц такой сбор служит для облегчения совершения впоследствии других противоправных действий (распространение с целью причинения вреда репутации и другим интересам личности, угрозы различного характера, похищение, кража и другое). К примеру, вымогательству в связи со своей известностью, подверглась телеведущая Ксения Бородина.

Хакеры взломали аккаунт iCloud с интимными фотографиями и личной перепиской девушки и требовали перевести на их счет сумму в один миллион рублей, чтобы они не распространили полученные незаконным способом изображения. Злоумышленники, не получив денег, отправили фотографии в различные издания массовой информации, которые опубликовали их, предав огласке[1].

[1] Лобенко Е. А., Кирилин К. А. Проблема нарушения права личности на неприкосновенность частной жизни российскими журналистами // Медиаисследования. 2020. № 7. С. 423.

Подводя итог исследованию, мы приходим к выводу, что информационные технологии способствуют не только активному и простому собиранию сведений о частной жизни лица без его согласия, но и их быстрому и анонимному распространению. Это предполагает повышенную общественную опасность деяния, в связи с чем представляется целесообразным включить данный способ совершения преступления в качестве квалифицирующего признака в ч. 2 ст. 137 УК РФ, изложив ее в следующей редакции:

«2. Те же деяния, совершенные лицом:

а) с использованием своего служебного положения;

б) с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» и технологии искусственного интеллекта, -…»

УДК 343

Г. З. МАМАЕВА[1]

РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ СЕТЕЙ

В рамках отечественной уголовно-правовой политики предпринимаются меры по противодействию преступлениям в информационной сфере, совершаемым с использованием компьютерных сетей.

Полагаем необходимым выделить базовые группы общественно опасных деяний в информационной сфере в зависимости от предмета посягательства и совершаемых с использованием компьютерных сетей, представляющих существенную опасность для личности, общества и государства, а именно, связанные с:

1) распространением фейковой информации, а также идеологий терроризма, экстремизма и нацизма посредством в информационно-телекоммуникационной сети «Интернет»;

[1] Научный руководитель — ДЖАНТУХАНОВА Милана Висадиевна, преподаватель юридического колледжа Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России).

2) функционированием незаконных рынков сбыта ограниченных (запрещенных) к свободному обороту предметов и веществ, медицинских изделий и биологически активных добавок;

3) получением несанкционированного доступа к охраняемым законом сведениям, осуществление их несанкционированного сбора, распространения и продажи.

Важно указать, что распространением фейковой информации, а также идеологий терроризма, экстремизма и нацизма посредством в информационно-телекоммуникационной сети «Интернет» представляет собой существенную угрозу информационной безопасности общества и государства.

Распространение фальсифицированных сведений, в том числе дискредитирующих деятельность органов государственной (муниципальной) власти и их должностных лиц, а также Вооруженных сил Российской Федерации, представляет собой один из наиболее широко распространенных видов общественно опасных деяний в информационно-телекоммуникационной сети «Интернет»[1].

Подавляющее большинство веб-сайтов обладает количеством посетителей, значительно превосходящим аудиторию классических средств массовой информации. Этим обстоятельством обусловливается возможность осуществления ими подрывной деятельности, посредством внедрения в массовое сознание российского общества ложных сведений.

Бесспорным представляется то, что данная деятельность осуществляется вопреки интересам российского общества и государства. В выступлении Министра внутренних дел Российской Федерации В. А. Колокольцева в рамках «Правительственного часа» в Государственной Думе Российской Федерации указывалось, что на момент середины октября 2022 г. по фактам дискредитации Вооруженных сил Российской Федерации возбуждено количество уголов-

[1] Фейковые новости: кто привлекается к ответственности за их распространение // Гарант.Ру : информационно-правовой портал. URL://https://www.garant.ru/news/1451881/ (дата обращения: 19.09.2023).

ных дел, превышающее 100, пресечено 4,5 тыс. административных правонарушений. В целях противодействия данному пагубному последствию цифровизации законодателем были внесены изменения в ч. 2 ст. 128.1 УК РФ.

В результате проведенных изменений известная норма была изложена в редакции: «...клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», либо в отношении нескольких лиц, в том числе индивидуально не определенных».

Наряду с распространением на веб-сайтах фейковых сведений, направленных на дезинформирование населения, существенную угрозу информационной безопасности общества и государства представляет категория общественно опасных деяний, связанных с пропагандой или оправданием нацизма в рамках информационно-телекоммуникационной сети «Интернет».

Бесспорным представляется то, что данная деятельность осуществляется вопреки интересам российского общества и государства. Ввиду распространения на территории России данных деяний, в целях противодействия данному пагубному последствию цифровизации законодателем были внесены изменения в норму, предусмотренную ст. 354.1 УК РФ (Федеральный закон от 5 апреля 2021 г. № 59-ФЗ): ч. 2 ст. 354.1 УК РФ дополнена п. «в», которой предусматривается уголовная ответственность за совершение известного деяния с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»; ст. 354.1 УК РФ дополнена ч. 4, устанавливающей ответственность за совершение известного преступления группой лиц, группой лиц по предварительному сговору или организованной группой, или с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет» (Федеральным законом от 5 апреля 2021 г. № 59-ФЗ).

Помимо общественно опасных деяний, связанных с пропагандой или оправданием нацизма в рамках информационно-телекоммуникационной сети

«Интернет», имеют место деяния, связанные с распространением экстремистских идей, а также призывов к осуществлению деятельности, направленной против безопасности государства.

Важно подчеркнуть, что под призывами следует понимать обращения к относительно широкому кругу лиц (к массам, толпе), с целью их побуждения осуществить экстремистские действия (деятельность) посредством ИКТ-ресурсов (в том числе информационно-телекоммуникационной сети «Интернет»)[1].

Бесспорным представляется то, что данная деятельность осуществляется вопреки интересам российского общества и государства. Ввиду распространения на территории России данных деяний, в целях противодействия данному общественно опасному деянию законодатель дополнил ст. 280.4 УК РФ. В частности, п. «в» ч. 2 ст. 280.4 УК РФ предусмотрено наличие у деяния квалифицированного признака в виде использования электронных информационно-телекоммуникационных сетей, в том числе Интернет, наряду со средствами массовой информации.

Перейдем к рассмотрению второй группы общественно опасных деяний в информационной сфере. Важно указать, что функционирование незаконных рынков сбыта ограниченных (запрещенных) к свободному обороту предметов и веществ, а также контрафактной (в том числе недоброкачественной, фальсифицированной и незарегистрированной) лекарственной продукции, медицинских изделий и биологически активных добавок, является одним из наиболее широко распространенных видов общественно опасных деяний в информационно-телекоммуникационной сети «Интернет».

Так, отдельную угрозу безопасности граждан сегодня стали представлять, во-первых, интернет-пропаганда употребления наркотических средств, психотропных веществ, а также их аналогов, во-вторых, широкое применение цифровых ресурсов (в том числе Даркнет) для их распространения и доставки.

Установлены многочисленные факты массового склонения с использованием информационно-телекоммуникационных сетей молодого населения к

[1] Кузнецов Р. Д. К вопросу о понятии публичных призывов к осуществлению экстремистской деятельности: проблемы квалификации // Вопросы. 2020. № 6. С. 408—414.

потреблению наркотических средств, психотропных веществ или их аналогов, а также навязывания представителями иностранных государств с использованием вышеуказанных средств информации идеология «безопасности» наркопотребления и «безвредности» опийных наркотиков для беременных женщин.

Наркоситуация в Российской Федерации оценивается как тяжелая, а в некоторых субъектах Российской Федерации как предкризисная. Смертность в России от связанных с наркотиками причин в 2020 г. возросла на 60 % (7316 человек), по сравнению с 2019 г. (4569 человек)[1]; в 2021 г. число смертей выросло на 37 % (превысило 10 тыс.) по сравнению с 2020 г. (7316 человек)[2].

Бесспорным представляется то, что данная деятельность осуществляется вопреки интересам российского общества и государства. В целях противодействия данному пагубному последствию цифровизации законодателем были внесены изменения в уголовное законодательство Российской Федерации путем включения в ч. 2 ст. 230 действующего уголовного закона п. «д» — «с использованием информационно-телекоммуникационных сетей» (Федеральный закон от 24 февраля 2021 г. № 25-ФЗ).

Перейдем к рассмотрению третьей группы общественно опасных деяний в информационной сфере. Она охватывает получение несанкционированного доступа к охраняемым законом сведениям, осуществление их несанкционированного сбора, распространения и продажи. Непосредственным объектом данных деяний являются общественные отношения, которыми обеспечиваются: информационная безопасность; права собственника (иного законного владельца) по реализации своих прав на информацию в порядке и пределах, установленных действующим законом.

Необходимо указать на повышенный уровень общественной опасности рассматриваемых деяний. Так, последствиями таковых могут явиться как мил-

[1] Смертность от наркотиков в России выросла на 60 % на фоне пандемии // РБК : сайт. URL: https://www.rbc.ru/economics/18/07/2021/60f1b7cc9a79472c99206f4d (дата обращения: 16.11.2023).

[2] В России смертность от наркотиков выросла на 37 % // Там же. URL: https://www.rbc.ru/society/09/07/2022/62c82a4e9a7947459362d0d5 (дата обращения: 16.11.2023).

лиардные убытки различных объектов (в том числе военных) и управленческих систем (предприятий, выполняющих функции жизнеобеспечения населения, объектов энергетики, транспорта и др.). Атаки, осуществляемые через ИКТ-ресурсы на их информационную инфраструктуру, могут быть катастрофическими.

Бесспорным представляется то, что данная общественно опасная деятельность осуществляется вопреки интересам российского общества и государства. В целях противодействия ей законодателем были внесены соответствующие изменения: в гл. 28 УК РФ была включена ст. 274.2 УК РФ, предусматривающая наступление ответственности за нарушение правил централизованного управления техническими средствами, противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (Федеральный закон от 14 июля 2022 г. № 260-ФЗ).

Важно подчеркнуть, что перечисленные изменения в действующий уголовный закон отражают только базовые тренды уголовно-правовой политики отечественного государства в информационной сфере. Приведенный в данном материале перечень изменений в российский уголовный закон не является исчерпывающим, поскольку конъюнктурные общественные отношения в информационной сфере меняются стремительно, столь же быстро формируются новые виды преступлений, осуществляемых с использованием информационно-телекоммуникационных технологий.

В действующем уголовном законодательстве не находят в полной мере свое отражение уголовно-правовые нормы, регламентирующие ответственность в информационной сфере. В настоящее время существуют сравнительно новые «цифровые» общественные отношения в виртуальной реальности, искусственного интеллекта, которые принципиально отличаются от отношений, находящихся под уголовно-правовой охраной в главе 28 УК РФ.

УДК 343

П. Д. МАРТЫНЕНКО[1]

НЕЗАКОННЫЕ ПОЛУЧЕНИЕ И РАЗГЛАШЕНИЕ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ, НАЛОГОВУЮ И БАНКОВСКУЮ ТАЙНУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В XXI веке достаточно активно развилась и продолжает развиваться сфера информационных технологий, развиваются социальные сети, интернет-ресурсы, компьютерные программы, защищающие конфиденциальную информацию каждого в обществе, представляющие возможность общаться, получать информацию на расстоянии, хранить ее, а также использовать в преступных целях.

В связи с этим изменяется характер преступности: все чаще преступления совершаются с помощью компьютерных технологий и информационно-телекоммуникационных сетей, позволяющих действовать инкогнито и с любой точки земного шара (государства, города, местности).

Данная категория преступлений только развивается, и поэтому в доктрине уголовного права пока не имеется четкого ее толкования. А.Н. Попов разделяет категорию компьютерных преступлений на три вида: преступления в сфере компьютерной информации, затрагивающие обработку данных и их передачу, к которым относит составы преступлений, предусмотренных главой 28 УК РФ, информационные компьютерные преступления, которые совершаются в сфере использования информационно-телекоммуникационных технологий, например, такие составы преступлений, как ст. 146, 159.6, 183, 242, ч. 2 ст. 228.1 УК РФ, а также киберпреступления, в которых компьютер, компьютерные технологии и сети являются предметом, средством или орудием преступления[2].

[1] Научный руководитель — БЕЗБОРОДОВ Дмитрий Анатольевич, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия кандидат юридических наук, доцент.

[2] Попов А. Н. Преступления в сфере компьютерной информации. СПб., 2018. С. 6—8.

Как ранее уже было отмечено, в соответствии с действующим УК Российской Федерации к такому роду преступлений, помимо главы 28 УК РФ, можно отнести и иные составы преступлений, в частности, состав преступления, предусмотренный статьей 183 УК РФ, который и будет в дальнейшем подробно рассмотрен.

Статья 183 УК РФ предусматривает наказание за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. С точки зрения русского языка тайной является некая информация, скрываемая от других, информация, которая известна не всем[1]. Таким образом, можно вывести более юридический термин – конфиденциальная информация. Конфиденциальная информация всегда привлекает большой интерес у тех, кто ею не обладают, и поэтому имеет большую ценность для злоумышленников. Таким образом, важно обеспечивать безопасность конфиденциальной информации, а в данном случае коммерческой, налоговой и банковской информации, от угроз и преступных посягательств, указанных в рассматриваемой статье.

Что же понимается под каждым видом тайн, охраняемых уголовным законом? Коммерческая тайна — информация, хранящаяся в себе сведения любого характера, а именно производственного, технического, экономического, сведений из научно-технической сферы, позволяющие лицу увеличить доходы, избежать непредвиденных расходов, сохранить положение на рынке, получить коммерческую выгоду[2].

Налоговая тайна – конфиденциальные сведения о налогоплательщике, плательщике страховых взносов, которые получены налоговым, следственным, таможенным органом, органом внутренних дел, органом государственного внебюджетного фонда[3].

---

[1] Большой толковый словарь русского языка: современная редакция. [В 4 т.] / под ред. Д. Н. Ушакова. М., 1935. С. 318.

[2] О коммерческой тайне : Федеральный закон от 29 июля 2004 г. № 98-ФЗ : текст с изм. и доп. на 14 июля 2022 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 04.08.2023). Доступ из справ.-правовой системы «Консультант-Плюс».

Банковская тайна – конфиденциальная информация об операциях, счетах и вкладах клиентов и корреспондентов, а также иные сведения, установленные кредитной организацией, что в обязательном порядке хранят служащие этой организации[1].

Следует отметить особенности состава преступления, предусмотренного ст. 183 УК РФ.

Непосредственным объектом деяния являются общественные отношения, возникающие между субъектами по поводу получения и распространения информации, составляющую коммерческую, налоговую или банковскую тайны, где предметом могут выступать документы, содержащие данную тайну как на бумажном, так и на электронном носителе.

Объективная сторона рассматриваемого состава преступления заключается в незаконном собирании (ч. 1 ст. 183 УК РФ), разглашении или использовании (ч. 2 ст. 183 УК РФ) конфиденциальной информации способом похищения, обмана, шантажа, угроз или подкупа. При этом перечень способов реализации преступного умысла является неисчерпывающим, так как это может происходить с помощью прослушивания телефонных переговоров, копированием информации, фото- и видеосъемка, применение специальных оптических приборов, неправомерный доступ к компьютерной информации, передача информации с использованием сети «Интернет». То есть это совершение действий, непосредственно направленных на завладение и разглашения указанных сведений незаконным способом, которые стали известны третьим лицам. Однако, можно предположить, что разглашение конфиденциальной информации возможно и путем бездействия, когда лицо, которому тайные сведения были доверены в силу служебных обя-

[1] О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-1 : текст с изм. и доп. на 4 авг. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

занностей, не предпринял необходимых мер для безопасности и сохранности секретной информации, исключающие ознакомления с этими сведениями посторонних лиц.

Субъективная сторона незаконного собирания, разглашения и использования коммерческой, налоговой или банковской тайн характеризуется наличием вины в форме прямого умысла. Лицо осознает общественную опасность своих действий, предвидит реальную возможность наступления последствий, а также желает наступления преступных последствий. Мотивами совершения данного преступления могут быть как месть, зависть, продвижение по карьерной лестнице, ненависть, так и другие причины в целеполагании человека. В ч. 3 ст. 183 УК РФ в качестве признака субъективной стороны состава преступления добавляется и корыстный мотив.

Субъектом совершения данного состава преступления будет являться лицо, которое не имеет право на получение такой конфиденциальной информации в силу того, что не является ее собственником, должностным лицом или иным лицом, которому эта информация не доверялось в силу служебного положения. А вот субъект в ч. 2 ст. 183 УК РФ является специальным. То есть это лицо, которому такие сведения были доверены или стали известны по служебной или рабочей необходимости и которому, в силу обязанностей, запрещено их разглашать.

Таким образом, в реалиях стремительного развития компьютерных и информационных технологий увеличивается количество незаконного доступа к персональной информации граждан. В УК РФ для квалификации компьютерных преступлений хоть и отводится отдельная глава, но также имеются и такие составы преступлений, где одним из способов совершения преступлений является использование компьютерных технологий, электронных и информационно-телекоммуникационных сетей.

УДК 343

А. С. МАТЮШКИНА[1]

НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ «ИНТЕРНЕТ-СОБСТВЕННОСТИ»

На сегодняшний день компьютерные игры являются чем-то обыденным, приобретая все большую популярность. Следует отметить, что они уже развились до отдельной специфической спортивной дисциплины — киберспорта[2]. Такое бурное развитие кибер-реальности необходимо рассматривать и с другой стороны: пользователи в процессе игры осуществляют оборот виртуального имущества[3].

В 2021 году компания Juniper Research провела исследование, которое показало, что объем мирового рынка лутбоксов (от англ. loot – «добыча в игре) на тот момент составил 15 млрд долларов, а к 2025 году достигнет 20 млрд, возрастая на 5 % ежегодно. При этом, в исследовании отмечено, что на долю Российской Федерации приходится 1,5% указанной суммы[4]. Таким образом, в современных реалиях виртуальные товары пользуются спросом и могут приносить реальный доход их обладателям.

Виртуальная игровая «собственность» является одной из самых обсуждаемых проблем в области изучения игр. Само по себе такое «имущество» является разнородным, поэтому исчерпывающего перечня не существует. Приведем несколько примеров «интернет-собственности»: персонажи и его экипировка (скин), оружие, виртуальные машины и дома, аккаунты пользователей

---

[1] Научный руководитель — КРАВЧЕНКО Роман Михайлович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

[2] Федерация компьютерного спорта России : офиц. сайт. URL: https://resf.ru/about/resf/ (дата обращения: 17.11.2023).

[3] В данной статье понятия виртуального имущества («собственности»), игровой «собственности», «интернет-собственности» и т. п. используются как синонимичные.

[4] Каткова М. М., Сурьянинова П. А. Виртуальная собственность в компьютерных играх: проблемы регулирования в российском законодательстве // Труды по интеллектуальной собственности. 2022. Т. 43, № 4. С. 93.

игры и так далее. Нужно иметь в виду, что стоимость приведенного «имущества» может достигать тысяч, а порой редкие экземпляры всевозможного оружия реализуются за миллионы рублей. Например, снайперскую винтовку в игре Counter-Strike: Global Offensive продают за сумму от 10 000 до 18 000 долларов (около 890 000 – 1 600 000 рублей)[1].

Необходимо отметить, что на данный момент нет легального определения виртуальной «собственности». В юридической доктрине выделяют три основных признака игрового «имущества»: 1) непосредственно связано с массовыми многопользовательскими ролевыми онлайн-играми (далее – MMORPG); 2) не может существовать вне зависимости от указанного выше объекта; 3) выступает нематериальным объектом, по поводу которого возникают отношения в компьютерной игре и взаимосвязанные с ними отношения. Приведенные признаки позволяют сформулировать дефиницию «интернет-собственности»: нематериальные объекты, которыми пользователи ролевых онлайн-игр посредством своих персонажей могут владеть, пользоваться и распоряжаться только в MMORPG[2].

Игровые платформы и их пользовательские базы становятся «целью» для киберпреступников, так как у них имеется возможность заработать реальные деньги в обмен на виртуальные товары. Однако проблемным вопросом является то, что никакому правовому регулированию и тем более уголовно-правовой защите объекты «интернет-собственности» в компьютерных играх не подлежат. При этом, негативные последствия при посягательствах на такое «имущество» наносят имущественный ущерб их обладателям. Подобный пробел законодательного регулирования исключает уголовную ответственность за хищение тех лиц, которые своими недобросовестными действиями получают

[1] AWP | Gungnir — CSGOSKINS.GG. URL: https://csgoskins.gg/items/awp-gungnir (дата обращения: 20.11.2023).

[2] Гаразовская Н. В. Виртуальное имущество в играх: перспективы правового регулирования // E-Scio. 2020. № 4 (43). URL: https://cyberleninka.ru/article/n/virtualnoe-imuschestvo-v-igrah-perspektivy-pravovogo-regulirovaniya (дата обращения: 19.11.2023).

внутриигровые предметы, принадлежащие другим пользователям, в свое владение, а также имеется возможность нарушения имущественных интересов пользователей (кражи через взлом аккаунта, уклонение от выполнения встречного обязательства по оплате переданного игрового атрибута, блокировка аккаунта и др.)[1].

В то же время, необходимо учитывать, что разработчики MMORPG не заинтересованы в введении законодательного регулирования виртуального «имущества». Объясняется это тем, что на них таким образом будут возложены дополнительные обязанности: материальная ответственность создателей компьютерной игры в случае ее закрытия. Так, отсутствие на данный момент правового регулирования указанного института противоречит основным принципам гражданского права, так как лишает пользователей MMORPG возможности защищать свои права.

Отметим, что законодательство и практика зарубежных судов в подобных случаях идут по пути уголовной ответственности и относят посягательства на «интернет-имущество» к преступлениям против собственности. Например, в Чехии кража внутриигрового предмета является уголовно наказуемой[2]. Также в Китае ведется разработка самостоятельного виртуального права, а на Тайване виртуальная собственность является собственностью в правовом смысле[3].

Безусловно, в рамках действующего гражданского законодательства невозможно рассматривать виртуальную «собственность» как имущество в классическом его понимании, так как оно существует только внутри киберпространства и не имеет физической (материальной) формы в реальном

[1] Казьмина А. Н. Перспективы правового регулирования виртуального игрового имущества. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Каткова М. М., Сурьянинова П. А. Виртуальная собственность в компьютерных играх: проблемы регулирования в российском законодательстве // Труды по интеллектуальной собственности. 2022. Т. 43, № 4. С. 91—100.

[3] Залевский Я. В. Правовая природа внутриигровых объектов // Молодой ученый. 2017. № 13 (147). С. 440.

мире. Так, М. А. Рожкова указывает, что в отечественной цивилистике действует главенствующий постулат – допустимость возникновения вещных прав только лишь на материальные предметы[1]. К тому же, «ценность» таких объектов является условной и определяется только в взаимосвязи с контекстом компьютерной игры.

Судебная практика в России складывается неоднозначно. Так, Арбитражный суд города Москвы приходит к выводу о том, что представление возможности использования дополнительного функционала игры в целях облегчения игрового процесса, в частности, в результате использования таких возможностей персонаж может получать игровые ценности, которые способствуют более быстрому его развитию в компьютерной игре, является по своей сути договором оказания платных услуг[2]. Однако, на наш взгляд, с такой позицией сложно согласиться, так как результаты оказания этой «услуги» не реализуются и не потребляются в процессе осуществления пользования виртуальным «имуществом», а являются лишь предоставлением доступа к какому-либо виртуальному объекту.

Ст. 128 ГК РФ приводится исчерпывающий перечень объектов гражданских прав и, конечно, указания на внутриигровые предметы как отдельного объекта статья не содержит, но, возможно, косвенно законодатель относит виртуальное «имущество» к одному из названных в ГК РФ объектов[3]: появление в 2019 году ст. 141.1 ГК РФ о цифровых правах, которые названы в качестве нового объекта гражданских прав, может лечь в основу законодательного регулирования оборота виртуального «имущества». Однако указанные

[1] Рожкова М. А. Имущественные права на новые нематериальные объекты в системе абсолютных прав // Право цифровой экономики — 2020 (16) // Ежегодник-антология. Серия «Анализ современного права» / руководитель и научный редактор М. А. Рожкова. М., 2020. С. 6.

[2] Решение Арбитражного суда г. Москвы от 24 ноября 2014 г. по делу № А40-91072/2014. // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 14.11.2023).

[3] Комментарий к Гражданскому кодексу Российской Федерации (учебно-практический). Части первая, вторая, третья, четвертая (постатейный) / С. С. Алексеев, А. С. Васильев, В. В. Голофаев [и др.] ; под ред. С. А. Степанова. 2-е изд., перераб. и доп. М., 2009. Доступ из справ.-правовой системы «КонсультантПлюс».

в названной статье признаки цифровых прав («поименованность» в законе в качестве таковых, связанность с определенной информационной системой) не позволяют на настоящий момент в полной мере рассматривать внутриигровые предметы в качестве цифровых прав[1]. Также следует учитывать, что не существует легальной процедуры истребования пользователем его виртуальных предметов. Конечно, если в связи с принятыми в дальнейшем поправками игровое «имущество» отнесут к цифровым правам, то будут все основания рассматривать «интернет-собственность» в качестве предмета хищения, так как имущественные права (как и цифровые) могут являться таковым.

Таким образом, виртуальное «имущество» не может быть предметом преступлений против собственности (ст. ст. 158, 163, 165 УК РФ), так как правовой статус у данных объектов в рамках вещных прав не определен (не подпадает под установленные понятия имущества, собственности), то есть «интернет-собственность» не относится к объекту преступлений, предусмотренных 21 главой УК РФ.

На данный момент преступные посягательства на виртуальное «имущество», являющееся строкой кода (информацией), можно рассматривать лишь в рамках 28 главы УК РФ, которая предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации. В рамках указанной главы предметом преступлений может выступать нематериальный объект. Например, в случаях фишинговых атак, несанкционированного доступа к аккаунту игрока, использования вредоносных программ для хищения виртуальных предметов. При этом, если в результате посягательства на внутриигровое «имущество» вред причиняется не конкретному пользователю компьютерной игры, а ее разработчику, то в данном случае деяние возможно квалифицировать как нарушение авторских и смежных прав по ст. 146 УК РФ.

[1] Розанова А. В., Лежнина К. А., Жевняк О. В. Многопользовательские компьютерные онлайн игры как объекты гражданских прав // Весенние дни науки : сборник докладов Международной конференции студентов и молодых ученых. Екатеринбург, 2022. С. 1391.

Другое дело обстоит в случаях мошенничества, связанного с «хищением» виртуальных предметов или приобретение права на них, которое в последние годы набирает все большую популярность. Связано это с наличием специальных рынков, предполагающих заключение сделок между игроками по поводу оборота внутриигрового имущества, где мошенничество может происходить в виде фальсификации товаров или нелегальной продажи, используя украденные или скомпрометированные аккаунты. В данном случае предметом преступления будет выступать не виртуальное «имущество» (оно может быть использовано как средство совершения преступления), а денежные средства пользователя компьютерной игры.

Однако важно различать характер действий злоумышленника в отношении «интернет-собственности». Так, например, в игре Ultima Online виртуальное воровство запланировано сценарием игры и зависит от навыков пользователей, то есть более опытный игрок может завладеть ценными предметами новичка несмотря на то, что это «имущество» приобреталось им за реальные деньги. В таких случаях игровое «хищение» не может быть уголовно-наказуемым, так как пользователи игры принимают установленные разработчиками правила и участвуют в данном игровом контенте, хотя одному игроку причиняется ущерб, а другой извлекает для себя имущественную выгоду. При этом, конечно, в случае взлома аккаунта пользователя завладение его виртуальным «имуществом» стоит оценивать как противоправное[1].

Получается, что речь о преступлении может идти не только в тех случаях, когда взламывается чужой аккаунт, но и когда завладение чужой «интернет-собственностью» происходит в обход предусмотренных правилами компьютерной игры положениями[2].

---

[1] Останина Е. А. Основание присоединения к многопользовательской онлайн игре — договор с участием потребителей // Право в сфере Интернета : сборник статей / ответственный редактор М. А. Рожкова. М., 2018. С. 342.

[2] Хилюта В. В. Дематериализация предмета хищения и вопросы квалификации посягательств на виртуальное имущество // Журнал российского права. 2021. Вып. 25, № 5. С. 68—82.

Таким образом, с развитием информационных технологий особо остро стоит вопрос необходимости адаптации законодательства и правоприменительной практики к новым институтам, в частности в области защиты прав пользователей компьютерных игр на их «интернет-собственность». На данный момент отраслевое законодательство не признает внутриигровое «имущество» объектом вещных прав, соответственно оно не может быть предметом преступлений против собственности, но может выступать предметом преступлений в сфере компьютерной информации. Отметим, что в данном случае остается не урегулированным вопрос имущественного вреда, который учитывается в рамках преступлений против собственности. Возможными решениями указанного пробела правового регулирования видятся изменения норм гражданского законодательства, которые станут фундаментом для уголовно-правовой охраны виртуальной «собственности».

УДК 343

Д. С. МИЩЕНКО,
Д. С. СОБОЛЕВА[1]

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПОСРЕДНИЧЕСТВА ВО ВЗЯТОЧНИЧЕСТВЕ (статья 291.1 УК РФ), В ТОМ ЧИСЛЕ СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

Коррупция, как социально-правовое явление, является распространенной проблемой, которая каждый год принимает все более изощренные способы. С развитием современных технологий, одними из которых являются информационно-телекоммуникационные сети (включая сеть «Интернет»), взяткодатели, взяткополучатели, а соответственно и посредники во взяточничестве воспользовались данной возможностью действовать в онлайн-среде.

[1] Научный руководитель — СЕРДЮК Павел Леонидович, доцент кафедры уголовного права и криминологии, Санкт-Петербургской академии Следственного комитета Российской Федерации кандидат юридических наук.

Одним из способов борьбы с данным негативным явлением является закрепление уголовной ответственности за посредничество во взяточничестве, введенная Федеральным законом от 4 мая 2011 года № 97-ФЗ в виде новой уголовно-правовой нормы — ст. 291.1 УК РФ.

Первым шагом в анализе данной нормы является определение основного термина. Уголовный кодекс Российской Федерации в статье 291.1. определяет посредничество во взяточничестве как непосредственную передачу взятки по поручению взяткодателя или взяткополучателя либо иное способствование взяткодателю и (или) взяткополучателю в достижении либо реализации соглашения между ними о получении и даче взятки в значительном размере.

Непосредственная передача взятки по поручению взяткодателя или взяткополучателя, представляет собой такое действие пособника, которое состоит в перемещении предмета взятки от одного лица к другому. К тому же для квалификации преступления не обязательно, чтобы предмет взятки был передан сразу получателю взятки, то есть возможно участие нескольких посредников, которые будут передавать взятку между собой.

Иное способствование взяткодателю и (или) взяткополучателю в достижении соглашения между ними о получении и даче взятки может выражаться в следующих действиях:

— помощь в установлении контакта между предполагаемым взяткодателем и взяткополучателем или в создании другого вида взаимодействия между ними;

— посредничество в вознаграждении должностного лица за совершение определенных действий по поручению взяткодателя;

— убеждение должностного лица в необходимости получения взятки по поручению взяткодателя;

— организация и ведение переговоров между потенциальными взяткодателем и взяткополучателем по поводу условий взятки.

Так как предметом взятки могут быть не только деньги, ценные бумаги, иное имущество, имущественные права, а еще и предоставляемые услуги иму-

щественного характера, то взятка с таким предметом не может быть осуществлена при осуществлении посредничества в виде непосредственной передачи взятки. Из этого выходит, если третье лицо оказывает должностному лицу полностью оплаченные взяткодателем услуги или же выполняет какие-либо работы и осознает при этом, что эти услуги являются предметом взятки, то подобное оказание услуг образует вторую форму посредничества: способствование взяткодателю и взяткополучателю в реализации соглашения между ними о получении, даче взятки.

При выполнении объективной стороны посредничества в виде иного способствования в достижении либо реализации соглашения между субъектами взяточничества, состав преступления ст. 291.1 УК РФ будет оконченным с момента совершения любого из указанных действий, направленных на достижение или реализацию соглашения. То есть не является существенным, было ли достигнуто соглашение.

В случае если по соглашению между взяткополучателем и посредником предмет взятки, полученный от взяткодателя, остается у посредника, то преступление окончено с момента получения предмета взятки. В случае, когда взятка передается напрямую, посредничество считается оконченным, если хотя бы часть взятки передана лицу, для которого она предназначена.

Если же лицо заведомо знало и предполагало, что передавать ценности оно не намерено, и получив предмет взяточничества обратило его в свою пользу, то такое преступное действие будет рассматриваться как мошенничество.

Часть 5 ст. 291.1 УК РФ предусматривает уголовную ответственность за обещание или предложение посредничества во взяточничестве, то есть соглашение о сотрудничестве лица с взяткодателем или взяткополучателем.

Предложение посредничества выражается в инициативе потенциального посредника в даче или получении взятки, и представляет собой активное навязывание своих услуг лицом, поиск непосредственных взяткодателей или взяткополучателей. Такое преступление окончено состав с момента

совершения лицом действий, направленных на доведение до сведения сторон взяточничества информации о своем намерении стать посредником во взяточничестве.

Особенностью квалификации в данном случае следует отметить то, что действия лица, обещавшего либо предложившего посредничество во взяточничестве и впоследствии совершившего преступление, предусмотренное ч. 1-4 ст. 291.1 УК РФ, квалифицируются по соответствующей части ст. 291.1 УК РФ без совокупности с частью 5 данной статьи. Из этого можно сделать вывод, что обещание или предложение посредничества представляет собой стадию приготовления к посредничеству во взяточничестве.

Еще одним проблемным аспектом применения ст. 291.1 УК РФ является определение предмета преступления, предусмотренного ч. 5 ст. 291 УК РФ.

В заключении правового управления Аппарата Государственной думы Федерального собрания Российской Федерации от 03.03.2011 № 2.21/650 было отмечено, что «сумма взятки для квалификации данного вида преступления доказыванию не подлежит»[1].

Также законодатель дает разъяснения по данному составу в Постановлении Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях». Обращаясь к данному Постановлению Пленума Верховного Суда Российской Федерации, можно сделать вывод, что уголовно наказуемым признается посредничество во взяточничестве, совершенное в значительном, крупном и особо крупном размере, а лицо, оказавшее посреднические услуги при передаче взятки на сумму, не превышающую двадцати пяти тысяч рублей, не может нести ответственности как соучастник в получении и даче взятки, мелком взяточничестве со ссылкой на статью 33 УК РФ[2].

---

[1] Герасимова Е. В. Теоретические и практические проблемы применения ст. 291.1 УК РФ, обусловленные несовершенством ее законодательной конструкции // Пенитенциарная наука. 2019. Т. 13, № 3 (47). С. 340—347.

[2] О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях : Постановление Пленума Верховного Суда Российской Федерации от 9 июля 2013 г. № 24 : текст с изм. и доп. на 24 дек. 2019 г. Пункт 13.3. Доступ из справ.-правовой системы «КонсультантПлюс».

При квалификации деяния следует отграничивать посредника во взяточничестве непосредственного от самого взяткодателя. В этом случае, важно понимать, что посредник действует и передает предмет взятки взяткополучателю или другому посреднику, от имени и за счет имущества взяткодателя. Взяткодатель же, передавая предмет взятки, использует при этом принадлежащее ему или незаконно приобретенное им имущество.

Ответственность за посредничество во взяточничестве наступает независимо от времени получения должностным лицом взятки - до или после совершения им действий (бездействия) по службе в пользу взяткодателя или представляемых им лиц, а также независимо от того, были ли указанные действия (бездействие) заранее обусловлены взяткой или договоренностью с должностным лицом о передаче за их совершение взятки.

Рассматривая совершение посредничества во взяточничестве, совершаемое с использованием средств информационно-телекоммуникационных сетей (включая сеть «Интернет»), которое в настоящее время является довольно распространенным и стремительно развивающимся, можно отметить следующие способы, которыми пользуются субъекты взяточничества:

1. Информационно-телекоммуникационная сеть (включая сеть «Интернет») выступает для данных лиц в качестве платформы, с использованием которой посредник во взяточничестве может предложить свои услуги предполагаемому взяткодателю или взяткополучателю.

Рассматривая судебную практику, обратимся к приговору Канавинского районного суда г. Нижнего Новгорода. Так, Макарова занималась, по своей инициативе, сбором документации для оформления лицензий на осуществление медицинской деятельности коммерческими организациями в Нижегородской области, за что получала от представителей таких организаций денежное вознаграждение. Одним из эпизодов ее преступной деятельности является следующее преступное деяние.

К Макаровой обратилась ранее ей незнакомая Иванова, являющаяся руководителем ООО «Логмеком», которая нашла ее резюме бухгалтера на интернет-ресурсе «AVITO», с целью проведения собеседования на замещение

данной должности в ООО «Логмеком». В ходе устного разговора Иванова сообщила Макаровой о том, что осуществляет сбор необходимых документов для получения лицензии на право осуществления медицинской деятельности. В этот момент у Макаровой возник преступный умысел, направленный на предложение посредничества во взяточничестве.

С целью реализации своего преступного умысла Макарова сообщила Ивановой о том, что имеет возможность в сокращенные сроки организовать получение ООО «Логмеком» лицензии в министерстве здравоохранения Нижегородской области на осуществление медицинской деятельности без проведения фактической проверки, поскольку располагает связями с должностными лицами, которые занимаются оформлением таких лицензий, предложив ей, таким образом, посредничество во взяточничестве, то есть, предложила через нее непосредственно передать предмет взятки в виде денег, в размере 35 000 рублей должностному лицу - главному специалисту сектора лицензирования управления по правовой и кадровой работе Министерства здравоохранения Нижегородской области лицу. После этого Макарова в ходе личной встречи с Ивановой договорились об осуществлении ею посреднических действий между вышеуказанными лицами[1].

На данном примере судебного делопроизводства можно увидеть, как с помощью информационно-телекоммуникационной сети «Интернет», а именно интернет-ресурса «AVITO», было совершено посредничество во взяточничестве, путем предложения посредником своей услуги на «AVITO».

2. Информационно-телекоммуникационная сеть (включая сеть «Интернет») выступает для данных лиц в качестве платформы, с использованием которой взяткодатель или взяткополучатель может осуществлять поиск посредника во взяточничестве.

Так, согласно приговору Ленинского районного суда г. Магнитогорска Челябинской области гражданин Сидоровов, подлежал призыву на военную

[1] Приговор Канавинского районного суда г. Нижний Новгород от 6 декабря 2017 г. по делу № 1-562/2017 // Канавинский районный суд г. Нижний Новгород : офиц. сайт. URL: https://kanavinsky--nnov.sudrf.ru (дата обращения: 23.11.2023).

службу в Вооруженные Силы Российской Федерации. О факте призыва на военную службу Сидоров рассказал своему отцу – Сидорову А.И., у которого возникло желание любым способом освободить своего сына от призыва на военную службу. С этой целью Сидоров А.И. через информационно-телекоммуникационную сеть «Интернет» на интернет-сайте Комитета солдатских матерей России подыскал контакты ранее ему незнакомой и являвшейся ранее председателем общественной организации солдатских матерей гражданки Косолаповой , с которой 6 декабря 2018 года созвонился и рассказал о данном факте, после чего они договорились о личной встречи.

В ходе указанной встречи Сидоров А.И., достоверно зная, что гражданка Косолапова являлась председателем общественной организации солдатских матерей, соответственно, знакома с различными должностными лицами военного комиссариата попросил ее оказать содействие по освобождению его сына от прохождения военной службы по состоянию здоровья, получению военного билета с отметкой о негодности к прохождению военной службы по состоянию здоровья.

Косолапова согласилась оказать помощь Сидорову, и выполняя свои посреднические действия, встретилась с Ивановым и, оказывая иное способствование взяткодателю и взяткополучателю в достижении и реализации соглашения между ними о получении и даче взятки в значительном размере, сообщила ему, с какой просьбой к ней обратился Сидоров А.И.

В ходе указанного разговора Иванов осознавая, что Косолапова будет являться посредником во взяточничестве, согласился совершить входящие в его должностные полномочия действия в пользу предоставляемого взяткодателем лица — призывника, связанные с освобождением последнего от призыва на военную службу и выдачу ему военного билета с отметкой об освобождении от призыва на военную службу по состоянию здоровья, за взятку в виде денег в значительном размере в сумме 100 000 рублей.

Непосредственно после достигнутой договоренности с Ивановым, Косолапова сообщила Сидорову А.И. о необходимости передать взятку в сумме

130 000 рублей, то есть в значительном размере, которые она решила распределить следующим образом: 100 000 рублей Иванову за его действия, планируя передать их при личной встрече, а остальные денежные средства в сумме 30 000 рублей оставить себе в качестве вознаграждения за посреднические услуги во взяточничестве. Данные денежные средства в ходе личной встречи были переданы Сидоровым Косолаповой, а в последующем Косолаповой Иванову[1].

Таким образом, в данном случае взяткодатель, с помощью интернет-сайта в сети «Интернет» нашел контакты лица, которому впоследствии предложил осуществить посреднические услуги, а также найти взяткополучателя, то есть лица, которое сможет осуществить необходимое ему требование.

3. Информационно-телекоммуникационная сеть (включая сеть «Интернет») выступает для данных лиц в качестве платформы, с использованием которой посредник во взяточничестве, а также взяткодатель или взяткополучатель могут производить общение.

Так, согласно приговору Нижегородского районного суда г. Н. Новгород по делу № 1-36/2022 от 11.04.2022, Попов А.Ю. осужден по п. «б» ч. 3 ст. 291.1 УК РФ.

Так, у лица по имени «Александр», действующего в интересах неустановленных лиц, организующих хищение материальных ценностей из нефтепродуктопровода акционерного общества «Солнышко», возник преступный умысел, направленный на дачу взятки в виде денег через посредника должностному лицу АО в крупном размере, за совершение последним заведомо незаконных действий в виде предоставления информации о планируемых мероприятиях по диагностике и внутритрубному обследованию участков нефтепродуктопроводов АО, бездействие в виде непринятия им и подчиненными ему сотрудниками поисково-технических групп Общества мер реагирования в

[1] Приговор Ленинского районного суда г. Магнитогорска Челябинской области от 16 июля 2020 г. по делу № 1-353/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 23.11.2023).

случае выявления фактов преступных посягательств и нарушениях нормального функционирования трубопроводов АО.

Во исполнение своего преступного умысла, «Александр» обратился к ранее незнакомому лично Попову с просьбой за неопределенное денежное вознаграждение оказать содействие в виде способствования в достижении реализации и соглашения о передаче и получении взятки между ним и иными неустановленными лицами, организовывающими вышеуказанное деяние.

В это же время в ходе разговора с неустановленным лицом по имени «Александр» у Попова возник преступный умысел на посредничество во взяточничестве за совершение заведомо незаконных действий и за бездействие между взяткодателем.

Следствием установлено, что лицо, получавшее взятку, неоднократно созванивался с Поповым и обменивался сообщениями, используя интернет-мессенджер «WhatsApp». Содержанием данных переписок являются договоры о встречах, обмен контактными данными, ход действий Попова. Также был зафиксирован телефонный разговор, состоявшийся между ним и Поповым через интернет-мессенджер «WhatsApp». В ходе данного разговора он сообщил Попову в соответствии с ранее достигнутой договоренностью о том, что началась опрессовка трубы, чтобы те закрыли кран на врезке[1].

Таким образом, данный пример из судебной практики демонстрирует использование сети «Интернет», а именно интернет-мессенджер «WhatsApp», как возможности способа общения между посредником и лицом, которому будет передан предмет взятки.

4. Также стоит рассмотреть такой способ как использование посредником онлайн-платформы для проведения транзакций и сделок. Эти платформы, которые часто предлагают «конфиденциальные услуги», могут быть использованы для перечисления денежных средств - взяток. Посредник здесь играет

[1] Приговор Нижегородского районного суда г. Нижний Новгород от 11 апреля 2022 г. по делу № 1-36/2022 // Нижегородский районный суд г. Нижний Новгород : офиц. сайт. URL: https://nizegorodsky--nnov.sudrf.ru (дата обращения: 23.11.2023).

роль агента, связывающего стороны и стремящегося получить выгоду от каждой транзакции. Примером данной платформы является платформа для купле-продажи криптовалюты Binance, OKX, BitMex, а также анонимные электронные кошельки «Яндекс.Денеги», QIWI, WebMoney, PayPal, VK Pay.

5. Однако законодательство не стоит на месте, и в отношении последних в 2020 году были внесены поправки в закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ, ограничивающий внесение наличных денежных средств на данные кошельки. Данный способ посредничества во взяточничестве характеризуется низким показателем раскрытия такого уголовного деяния в связи со сложностью установления личности отправителя и получателя при использовании таких платформ.

Таким образом, использование информационно-телекоммуникационных сетей (включая сеть «Интернет») в посредничестве во взяточничестве причиняет следующие последствия:

Во-первых, оно способствует и позволяет посредникам оперировать с большим количеством участников, помогает осуществлять их поиск, взаимосвязь с ними, усиливая таким образом их взаимодействие.

Во-вторых, такой вид посредничества во взяточничестве способствует нарушению законодательства о безопасности и защите данных. Посредники могут получать доступ к персональной информации о коммерческих и государственных сделках, что создает значительные угрозы для конфиденциальности и безопасности информации личности и организаций.

И в-третьих, посредничество во взяточничестве, совершаемое с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет», в целом, как и само взяточничество, приводит к неправильному распределению ресурсов и обострению неравенства в обществе и нарушает нормальную деятельность. Посредники, преследуя свои собственные интересы, могут манипулировать справедливым доступом к ресурсам и благам, предоставляемые в том числе должностными лицами, вытесняя тех, кто выполняет свою деятельность законным путем.

УДК 343

И. С. НАЗАРЕНКО[1]

ПРОБЛЕМЫ КВАЛИФИКАЦИИ РЕАБИЛИТАЦИИ НАЦИЗМА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ» (статья 354.1 УК РФ)

В настоящее время растет количество мнений и взглядов на решения, установленные Международным военным трибуналом в Нюрнберге. Заключение Нюрнбергского трибунала состоит в осуждении нацизма как запрещенной преступной идеологии. Данные взгляды по поводу Нюрнбергского процесса могут быть выражены как в пассивной, так и в активной форме, последняя из которых состоит из совершения противоправных действий, связанных с нацизмом.

Если говорить о термине «реабилитация нацизма», то под ним подразумевается восстановление в прежнем состоянии невиновного лица, необоснованно привлеченного к уголовной ответственности; действие с целью оправдания репутации нацизма и признания данной идеологии правильной[2].

На законодательном уровне современной России признаны и закреплены положения, выступающие следствием проведения Международного военного трибунала. Так, в результате принятия Федерального закона от 5 мая 2014 г. № 128-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» была введена ст. 354.1, которая содержит положения по реабилитации нацизма. Данная статья предусматривает уголовную ответственность за отрицание фактов, установленных Международным военным трибуналом, наказания главных военных преступников европейских стран, а также

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

[2] Мараева А. В. Вопросы толкования термина «реабилитация нацизма» применительно к ст. 354. 1 УК РФ // Вестник Московского Университета МВД России. 2019. № 4. С. 103.

за одобрение данных противоправных деяний и распространение ложной информации о деятельности СССР в годы Второй мировой войны.

В первой части вышеуказанной статьи закреплено четыре самостоятельных состава преступления. Во второй же части ст. 354.1 УК РФ установлено четыре квалифицирующих признака, а именно: «использование своего служебного положения», «группа лиц, группа лиц по предварительному сговору или организованная группа», «с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»», «с искусственным созданием доказательств обвинения».

Третья часть включает в себя оскорбление памяти защитников Отечества, распространение таких сведений о днях воинской славы или о памятных датах России, выражающих неуважение к обществу.

Часть четвертая ст. 354.1 УК РФ была введена позже Федеральным законом от 05.04.2021 № 59-ФЗ, которая предусматривает два квалифицирующих признака: совершение преступления группой лиц, группой лиц по предварительному сговору или организованной группой; с использованием сети «Интернет». Исходя из вышесказанного, можно заметить сложную конструкцию данной статьи, в связи с чем возникает ряд проблем с квалификацией преступных деяний.

Объективная сторона ст. 354.1 УК РФ предусматривает отрицание фактов, одобрение преступных действий, а также распространение ложной информации.

Исходя из этого, можно привести пример совершения противоправных действий, связанных с данным составом преступления. Так, лицо было осуждено за покушение на одобрение преступлений, установленных приговором Международного военного трибунала. Преступные действия он совершил в 2020 году, которые заключались в публикации в приложении «Бессмертный полк онлайн» фотоизображения Гитлера.

Лицо осознавало, что на данной платформе публикуются участники Великой Отечественной войны, защитники Отечества. Он также понимал, что

его действия были направлены на публикацию во всеобщий доступ изображения нацистского преступника. Его действия были пресечены, данную фотографию не опубликовали, то есть лицо не смогло довести до конца преступление по независящим от него обстоятельствам, благодаря блокировке модератором его заявки на публикацию.

Состав данного преступления является формальным, в связи с чем он считается оконченным с момента совершения действий, составляющих объективную сторону, а наличие или отсутствие последствий не влияет на момент его окончания.

То есть лицо из данного примера выполнило действия, составляющие объективную сторону состава преступления, он одобрил преступления нацистских преступников, установленных приговором Международного военного трибунала.

При контекстуальном анализе ст. 354.1 УК РФ можно проследить, что фраза «заведомо ложные сведения» выражает прямой умысел субъективной стороны данного состава преступления. Несмотря на то что возникали судебные споры по поводу соответствия данной нормы и квалификации по ней с положениями Конституции РФ, а именно принципам свободы, равенства, Конституционный Суд РФ пришел к выводу, что государство «чтит память защитников Отечества, обеспечивает защиту исторической правды».

В ст. 354.1 УК РФ одним из элементов объективной стороны является отрицание фактов, установленных Международным военным трибуналом. Термин «отрицание фактов» означает то, что лицо исключает справедливость данного решения и придерживается непризнания таких фактов.

«Одобрение преступлений» подразумевает под собой заявление неопределенному кругу лиц о правильности совершенных преступлений, в данном случае преступлений нацистских преступников, при этом считая, что они заслуживают уважения и поддержки.

Если лицо осуществляет принцип свободы, равенства, но при этом нарушает права и свободы других, то он должен быть привлечен к ответственности за свои противоправные действия для защиты интересов всех граждан. По причине того, что фашизм закреплен как недопустимая форма проявления, согласно Федеральному закону от 19 мая 1995 г. № 80-ФЗ «Об увековечении Победы советского народа в Великой Отечественной войне 1941-1945 годов», то за распространением данной идеологии будет следовать уголовная ответственность.

Признаком объективной стороны ст. 354.1 УК РФ является публичность. Публичность подразумевает использование технических средств, средств массовой информации, включая сеть «Интернет», например на различных сайтах, форумах, а также выступления на собрании, митинге, вывешивание и демонстрация плакатов, дискредитирующих Вооруженные Силы Российской Федерации [1]. Данный признак объективной стороны предусмотренного состава преступления означает открытость совершающихся действий, то есть в присутствии публики, их обращенности к неопределенному кругу лиц[2], а также в возможности публики к получению данной информации.

Исследуя правоприменительную практику квалификации преступлений по ст. 354.1 УК РФ, устанавливаются определенные трудности. Так, например, после размещения в сети «Интернет» фотографии скульптуры «Родина-мать зовет!», на голову которой была нанесена краска зеленого цвета, тем самым публично осквернив символ воинской славы России. Опубликованное изображение было просмотрено более 900 раз, что свидетельствует о публичности совершенных действий. Органы предварительного следствия квалифицировали данные противоправные деяния по ч. 3 ст. 354.1 УК РФ как публичное «осквернение символов воинской славы России».

---

[1] Мурадян С. В. Вопросы применения статьи 280.3 УК РФ о дискредитации использования Вооруженных Сил Российской Федерации или исполнения государственными органами своих полномочий // Криминологический журнал. 2023. № 1. С. 87—94.

[2] Большой толковый словарь русского языка: современная редакция / Д. Н. Ушаков. М., 2008. 959 с.

Но суд указал, что лицо осквернило скульптуру, которое входит в состав объекта культурного наследия федерального значения «Мемориальный комплекс «Героям Сталинградской битвы»»[1], то есть данное скульптурное сооружение посвящено участникам борьбы с фашизмом и расположено на месте их захоронения, то есть оно совершило преступление, предусмотренное составом п. «б» ч. 2 ст. 244 УК РФ («уничтожение или повреждение воинских захоронений, а также памятников стел, обелисков, других мемориальных сооружений или объектов, увековечивающих память погибших при защите Отечества или его интересов либо посвященных дням воинской славы России»).

В результате Верховный Суд Российской Федерации отменил решения нижестоящих судов и отправил данное уголовное дело на новое разбирательство[2].

Таким образом, в заключение необходимо сказать, что проблема квалификации преступных действий по реабилитации нацизма с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», предусмотренной ст. 354.1 УК РФ, является актуальной и порождает все большие вопросы у правоприменителей.

Несмотря на принятие специализированного Федерального закона от 7 апреля 2020 г. № 112-ФЗ проблема квалификации и разграничения составов преступления ст. 354.1 УК РФ и 243.4 УК РФ в судебной практике сохраняется. В связи с этим возможным решением данной проблемы может быть разграничение на законодательной уровне путем разъяснения Постановлением Пленума Верховного Суда Российской Федерации.

---

[1] Денисова А. В. Проблемы квалификации преступных действий по реабилитации нацизма (ст. 354.1 Уголовного кодекса Российской Федерации) // Вестник Томского государственного университета. 2022. № 482. С. 239—243.

[2] Определение Верховного Суда Российской Федерации от 18 мая 2021 г. по делу № 80-УДП21-3-А4. Доступ из справ.-правовой системы «КонсультантПлюс».

УДК 343

П. С. НУРМАГОМЕДОВА[1]

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

Актуальность темы обусловлена тем, что компьютеризация современного общества, несомненно, имеет положительное влияние на развитие и становление общества, но вслед за положительным воздействие глобализация несет в себе расширение потенциальных источников социальной опасности, связанных с криминогенными элементами общества. Стремительный рост числа преступлений с сети «Интернет» свидетельствует о том, что преступники теперь используют цифровую/виртуальную среду также активно, как и реальный мир, что создает для них новую специализацию в преступной сфере: в 2021 году в Российской Федерации было зарегистрировано более 2 004 404 преступлений, из которых 517 722 (25,8 %) были преступлениями с использованием информационно-телекоммуникационной сети[2].

В геометрической прогрессии возрастает количество преступлений, совершенных с использованием сети «Интернет», ущерб от этих преступных посягательств стремительно растет. Преступность с использованием сети «Интернет» с каждым днем приобретает все новые формы проявления, начиная от всем известных простых мошеннических схем до проявления преступных комбинаций транснационального характера.

Преступления с использованием сети «Интернет» приобретают организованную структуру с разработанными методами и способами конспи-

[1] Научный руководитель — КЕРИМОВА Заира Абдурахмановна, преподаватель юридического колледжа Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России).

[2] Краткая характеристика состояния преступности в Российской Федерации за январь—декабрь 2021 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/28021552/?ysclid=lbj5rjtmww506921643 (дата обращения: 01.11.2023).

рации, что в свою очередь усложняет работу по раскрытию и расследованию этих видов преступлений. На сегодняшний день существует необходимость полноценного исследования классификации преступлений, совершаемых в сети «Интернет».

Повышение количества общеуголовных преступлений с применением информационно-телекоммуникационных технологий свидетельствует о необходимости принятия адекватных мер по противодействию этому виду преступности. Одним из путей повышения эффективности раскрытия и расследования рассматриваемых преступлений явилось создание специализированных подразделений по борьбе с киберпреступлениями в структуре МВД РФ.

Министр внутренних дел России В.А. Колокольцев отметил, что масштабы распространения этого вида преступности, разнообразие схем и методов их совершения, отсутствие единого алгоритма раскрытия обусловливают необходимость обеспечения новых подразделений не только и не столько кадрами, сколько современными коммуникационными технологиями.

Стоит обратить внимание на значительные задержки в расследовании всех преступлений в этой области, отсутствие достаточного количества следственной и судебной практики по таким делам, а также проблемы, связанные с выявлением «виртуальных следов». Основными недостатками являются отсутствие единой и общепризнанной программы борьбы с киберпреступностью, трудности в обеспечении безопасности данных и неопытность следователей, сталкивающихся с очень специфической информацией при исследовании различных форм доказательств, таких как электронные письма и вебсайты. Эти проблемы задерживают или затрудняют работу правоохранительных органов и требуют срочного решения.

Анализ характеристик позволяет разработать оптимальные методы и приемы для решения следственных ситуаций, представления и проверки следственных теорий.

Проблемы квалификации преступлений, связанных с информационно-телекоммуникационной сетью и интернет-пространством заключаются в основ-

ном в недостаточности разработки норм уголовного права, а также недостаточности судебной практики. Так ч. 1 ст. 159.3 УК РФ является мошенничество с использованием платежных карт достаточно тяжело разграничить с п. «г» ч. 3 ст. 158 УК РФ, а именно кража в отношении электронных денежных средств, с банковского счета. Законодатель прямо указывает в п «г» ч. 3 ст. 158 УК РФ, что деяние имеет место быть квалифицированно так, если нет признаков, указывающих на квалификацию ч. 3 ст. 159 УК РФ.

Возникает вопрос, как разграничить данные составы преступлений, что именно отнести к электронному мошенничеству, а что к краже. К мошенничеству стоит относить действия лица, направленные на хищение чужого имущества в качестве поддельной, либо принадлежащей иному лицу карты путем обмана работника кредитной, торговой организации. Кража, как правило, осуществляется в отношении физических «не бдительных» лиц, путем сообщения потерпевшим данных о карте, либо переходе на «вирусный сайт, ссылку». То есть квалифицирующими признаками будет являться способ совершения, объект посягательства и возможность противодействия преступнику со стороны потерпевшего[1].

На наш взгляд, самым распространенными преступлениями в сети «Интернет» являются хищения. Именно в сфере информационных технологий хищение развилось достаточно хорошо и поэтому имеет множество видов. Одним из таких является «кардинг», иначе говоря, хищение, связанное с банковскими картами.

«Фишинг» — это особо опасное преступление, связанное с ложными уведомлениями от банков, администраторов платежных систем либо рассылка сообщений в социальных сетях и др.

Большое распространение в настоящее время приобретает хищение, связанное с бесконтактной оплатой, т. е. благодаря NFC, технологии беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии 4 сантиметров.

[1] Теппеев А. А. Способы совершения и проблемы квалификации преступлений, совершаемых с использованием сети «Интернет» // Право и управление. 2023. № 3. С. 130—133.

Данная технология сейчас присутствует почти в каждых банковской карте и смартфоне и позволяет оплачивать покупки до определенной суммы лишь прикладывая банковскую карту без ввода пароля. Смысл работы преступников состоит в перехвате NFC-сигналов, используя незаконные устройства-считыватели.

Если говорить об уголовной ответственности за выше перечисленные виды хищения, то можно отметить, что суд часто дает неправильную квалификацию данных деяний, определив их как обычную кражу, однако в апелляционном процессе, как показывает практика, дают более точную квалификацию данным преступным деяниям.

Так, например, Лукьянов и Блинов были приговорены к лишению свободны по п. «а», «в» ч. 2 ст. 158 и ч. 2 ст. 273 УК РФ, хотя в их действиях наблюдались все элементы состава преступления, которые описаны в ст. 159.6 УК РФ, а именно данные лица совершали кражу денежных средств путем установления вредоносной программы, которая была установлена на их персональном компьютере, но оказывала воздействие на систему пострадавших за счет перехода ими по вредоносной ссылке на удаленный сайт, который блокировал компьютер пострадавшего и открывал полный доступ к нему злоумышленникам, которые узнав персональные данные вошли в систему банка, откуда были переведены денежные средства на их личные счета. Рассмотрев апелляционную жалобу, суд частично удовлетворил требования осужденных, переквалифицировав преступные деяния лиц с п. «а», «в» ч. 2 ст. 158 на ч. 2 ст. 159.6 УК РФ[1].

Таким образом, необходимо сделать вывод о том, что в настоящее время нельзя создать единую и четкую систему преступных деяний, совершенных с использованием информационно-телекоммуникационных сетей, в связи со следующими обстоятельствами:

1. Отсутствием наличия общего подхода к квалификации преступлений и его криминализации, которые совершаются с помощью информационно-телекоммуникационных сетей.

[1] Николаева Е. Р. Проблемы противодействия преступлениям, совершаемые в сети «Интернет» // Вопросы российской юстиции. 2019. Вып. 4. С. 419—424.

2. Перечнем деяний, которые совершаются посредством информационно-телекоммуникационных сетей, содержащийся в Особенной части УК РФ, не может охватывать все преступления, где используются подобного рода технологии.

Развитие институтов сетевой телекоммуникации, а также, их широкое применение в противоправной деятельности не позволяет представить целостную систему преступлений, совершаемых посредством использования информационно-телекоммуникационной сети «Интернет»[1].

УДК 343

Д. В. ПЕРОВ[2]

ОСОБЕННОСТИ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ПОМОЩЬЮ СОЦИАЛЬНЫХ СЕТЕЙ

В нынешнее время социальные сети используют как средство передачи информации и знаний, а также способ общения и знакомства между людьми. К сожалению, бывают случаи, когда социальные сети используют люди для совершения преступления, или его подготовки, а также для сбора и распространения запрещенной информации и материалов.

И для того, чтобы доказать причастность того или иного гражданина в совершении данного преступления, нужно получить доказательства из социальных сетей, а именно: переписку, подтверждение передачи личных данных, фотографий, документов и т. д.

В статье 13 УПК РФ регламентируется вопрос об изъятии информации, но в ст. 63 Федерального закона «О связи» от 07.07.2003 № 126-ФЗ (ред. от 04.08.2023) регламентируется вопрос права тайны переписки, телефонных разговоров и передачи информации в целом. Сразу же возникает вопрос: в ходе каких процессуальных действий возможно изъятие данной ин-

[1] Нескородова И. С., Кислицын Н. А. Проблема систематизации преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет» // Гуманитарные, социально-экономические и общественные науки. 2020. № 12-2. С. 120—122

[2] Научный руководитель — КРАСНОВА Кристина Александровна, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

формации и какова процедура данного изъятия, так чтобы не нарушать положения Конституции, федеральных законов и кодексов, а также основных источников российского законодательства.

Социальная сеть представляет из себя многопользовательский веб-сайт, где люди общаются, обмениваются информацией и т. д.

Передача информации в социальных сетях представляет собой обмен информацией, которая осуществляется зачастую между людьми, имеющие между собой различного рода связи. Связь в основном бывает 3 видов:

— дружеская связь. Люди добавлены друг у друга в социальных сетях, в качестве контактов, друзей, тем самым они видят большую часть информации профиля своего собеседника, а также беспрепятственно способны передавать друг другу информацию;

— связь между участниками групп или сообществ. Данная связь возникает, если люди состоят в какой-то группе, которая создана в социальной сети для людей с общими интересами (соседи, родители и т. п.);

— связи между людьми, имеющими определенную информацию в профиле. Данная информация позволяет нам по определенным критериям, с легкостью найти себе собеседника по интересам, что очень сильно экономит наше время.

Все это образует некую систему, которая позволяет нам общаться и передавать информацию, называется она информационная система, то есть совокупность информации и технологии, которые помогают нам обработать данную информацию.

При необходимости изъятия переписки, информации, документов и т. д. из социальных сетей, нужно провести следственное действие, как наложение ареста на переписки и телефонные разговоры, согласно ст. 185 УПК РФ. Но в ст. 185 УПК РФ нет четкого регламента, как проводить данное изъятие так, чтобы не нарушать другие законы.

Из этого следует, что нужно организовать оперативно-следственную работу, которая не будет противодействовать нормативно правовым актам,

Подводя итог, основываясь на изложенную информацию выше можно сделать вывод, что правоохранительные органы могут изымать электронную

переписку и телефонные разговоры различными способами, но законодательной базы, регламентирующей данный процесс, не существует.

Следовательно, многие процессуальные действия, связанные с получением электронных переписок и телефонных разговоров, как доказательной базы причастности того или иного лица к причастности преступления, очень сильно затрудняется из-за того, что законодательство, а именно уголовный кодекс Российской Федерации не развивается в этом направлении и не обеспечивает быстроту следственных действий в рамках уголовных дел.

Следовательно, необходимо регламентировать этот вопрос в УПК РФ, а если быть точнее, внести изменения или дополнения в ст. 185 УПК РФ, чтобы оптимизировать решение вопроса об изъятии информации из социальных сетей.

А также необходимо дополнить ст. 74 УПК РФ термином «цифровое доказательство» и включить его в перечень видов доказательств. В результате данных изменений должным образом будет развито данное направление, ускорен процесс по получению доказательств для раскрытия уголовных дел, связанных с уголовными преступлениями производимых с помощью социальных сетей и иных средств массовой информации.

УДК 343

А. А. ПЕТРУХИНА,
А. А. СИВЦЕВА[1]

ИСПОЛЬЗОВАНИЕ СЕТИ «ИНТЕРНЕТ» ПРИ СОВЕРШЕНИИ ГОСУДАРСТВЕННОЙ ИЗМЕНЫ

На данный момент геополитическая обстановка вокруг Российской Федерации значительно накаляется. Заметно обостряются военно-политическая и экономическая сферы. Вследствие длительного продолжения Специальной военной операции, преступления против общественной безопасности нашей страны становятся все более частыми.

Недружественные страны активно показывают негативное отношение к действиям Российской Федерации, вводя политические и экономические

[1] Научный руководитель — ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

санкции, касающихся различных сфер жизни российского общества и государства. Данное обстоятельство несомненно наносит серьезный ущерб имиджу и авторитету страны в международном сообществе. По словам политических лидеров, такие обстоятельства могут стать толчком к развитию глобального военного конфликта. В свете этих событий проблема обеспечения внешней безопасности Российской Федерации приобретает особую актуальность.

Так, 17 марта 2023 года, Вторая Палата предварительного производства Международного уголовного суда (далее – МУС) выдала ордера на арест двух лиц в контексте ситуации в Украине: президента страны Владимира Владимировича Путина и уполномоченной при президенте по правам ребенка Марии Алексеевны Львовой-Беловой[1].

Как заявила официальный представитель МИДа Мария Захарова, решения Международного уголовного суда для России не имеют никакого значения, в том числе с правовой точки зрения. «С данным органом Россия не сотрудничает, а возможные «рецепты» на арест, исходящие из Международного суда, будут для нас юридически ничтожными», — заявила она.

Пресс-секретарь президента России Дмитрий Песков, комментируя решение МУС, заявил, что саму постановку вопроса в Кремле считают «возмутительной и неприемлемой». «Россия, как и целый ряд государств, не признает юрисдикцию этого суда и, соответственно, любые решения подобного рода являются для Российской Федерации с точки зрения права ничтожными», — заявил он[2].

Эти события, в том числе, в определенной степени дестабилизируют общество и наталкивают некоторых российских граждан на совершение преступления, предусмотренного статьей 275 УК РФ.

Само определение понятия «государственная измена» всегда вызывало дискуссии среди ученых. Под ним в первую очередь понимается посягательство на безопасность страны, совершение действий, направленных против суверенитета

[1] Международный уголовный суд : сайт. URL: https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and (дата обращения: 18.09.2023).

[2] РБК : сайт. URL: https://www.rbc.ru/politics/17/03/2023/641486bf9a79479594d1fb8a (дата обращения: 29.10.2023).

и обороноспособность, целостность и неприкосновенность территории Российской Федерации [1].

Важно учитывать, что способов совершения госизмены в наши дни множество. Способ выступает одним из элементов состава преступления. Нормативного толкования способа совершения общественно-опасного деяния не предусмотрено, однако в теории уголовного права существует множество дефиниций этого термина.

Нельзя не согласиться с определением, который приводит в своих работах Н. И. Панов. Он определяет способ как определенный порядок, метод, последовательность движений и приемов, применяемых лицом в процессе осуществления общественно опасного посягательства на охраняемые уголовным законом общественные отношения, сопряженные с избирательным использованием средств совершения преступления[2].

Тенденции современного мира, когда информационные и компьютерные технологии охватывают все сферы жизни людей, обусловливают также возникновение новых способов совершения преступного деяния, в том числе при государственной измене. Использование сети «Интернет» представляется весьма актуальным и часто встречающимся способом совершения рассматриваемое общественно-опасное посягательство.

Так на сегодняшний день в виртуальной сети доступны десятки онлайн-платформ, призванных существенно упростить организацию, координацию и исполнение государственной измены посредством быстрой и технологичной коммуникации, оперативной передачи информации и планирования действий. Кроме того, огромным преимуществом для преступников является возможность подобных платформ обеспечить анонимность и конфиденциальность личных данных участников, а также масштабируемость деяния, что в определенной степени повышает общественную опасность рассматриваемого преступления.

---

[1] Комментарий к Уголовному кодексу Российской Федерации / Университет прокуратуры Российской Федерации ; под общ. ред. О. С. Капинус ; науч. ред. В. В. Меркурьев. М., 2018. С. 1096.

[2] Лозовский Н. А. Значение способа совершения преступления для квалификации преступлений // Молодой ученый. 2022. № 51 (446). С. 514—516.

Среди таких платформ выделяют социальные сети и мессенджеры, многие из которых имеют функцию шифрования данных пользователей, а также интернет-блоги и онлайн-форумы. Первые обеспечивают возможность общения лиц и обмена информацией между ними, а посредством вторых создается виртуальное пространство для обсуждения и анализа политических вопросов, имеющих непосредственное отношение к государственной измене. Помимо этого, в интернет-пространстве существуют платформы, специализирующиеся непосредственно на организации общественных протестов и анализе статистики, необходимой для осуществления преступного умысла.

Интернет-технологии позволяют вовлекать в совершение госизмены все большее число участников. Подтверждением этому могут служить данные Федеральной службы безопасности о том, что по сравнению с 2022 годом за аналогичный период 2023 года количество обвинительных приговоров по ст. 275 УК РФ увеличилось втрое. Такие данные могут свидетельствовать о том, что информация о готовящихся преступлениях этой направленности распространяется в разы быстрее и охватывает значительное число пользователей, в чем, несомненно, прослеживаются преимущества Интернет-платформ.

Стоит также отметить, что в связи с редакцией ст. 275 УК РФ и указанием в ней на тот факт, что госизменой будет считаться оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности Российской Федерации, возможности использования сети «Интернет» в совершении данного деяния существенно расширяются. Например, передача в онлайн-формате иностранной разведке сведений, заведомо не имеющих грифа секретности, но интересующих ее (военно-техническая информация, сведения о научных разработках, данные о промышленности и транспорте, работе спецслужб и так далее).

Так в 2020 году было предъявлено обвинение в госизмене руководителю отдела Центра информационной безопасности ФСБ России Сергею Михайлову, его подчиненному, сотруднику «Лаборатории Касперского». По данным следствия, посредством сети «Интернет» они регулярно передавали информацию иностранным спецслужбам.

С распространением совершения государственной измены с использованием сети «Интернет» появились некоторые проблемы в правоприменительной практике. Так, к примеру, некий пользователь может часто выкладывать в свои аккаунты в социальных сетях фотографии военных самолетов на специализированных аэродромах, которые, предположим, видно из окна его дома, но уголовной ответственности за это не последует. Вместе с тем, в случае если лицо сделает это по просьбе представителей иностранного государства, которым интересно расположение и модель данной техники, то размещение фотографий в Интернет-пространстве станет способом совершения государственной измены, что повлечет уголовную ответственность, предусмотренную ст. 275 УК РФ.

Особое внимание следует обратить на то, что некоторые онлайн-платформы применяют особые коды шифрования данных, которые значительно затрудняют установление субъекта преступления. К примеру, по заказу представителей недружественных стран в свободном доступе сети «Интернет» появляется анонимная статья, содержащая данные о технических характеристиках военных самолетов, использующихся Вооруженными силами Российской Федерации. Автор статьи использовал сложные коды шифрования, отследить его по которым невозможно. В таком случае определить лицо, виновное в совершении государственной измены, будет весьма затруднительно.

Другими словами, можно говорить о том, что совершение преступления, предусмотренного ст. 275 УК РФ с использованием сети «Интернет» имеет определенные особенности в квалификации. Необходимо четко определить по

чьей инициативе передавались или размещались сведения в онлайн-пространстве: по заказу представителей иностранных государств или же по инициативе самого автора или адресанта сведений.

Таким образом, можно говорить о том, что интернет-пространство открывает широкие возможности для совершения преступного деяния, предусмотренного ст. 275 УК РФ, что определенно представляет существенную угрозу безопасности Российской Федерации.

УДК 343

С. Р. РАБАДАНОВА[1]

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ РЕЛИГИОЗНОМУ ЭКСТРЕМИЗМУ В СЕТИ «ИНТЕРНЕТ»

Актуальной проблемой организационно-правовых основ противодействия религиозному экстремизму в сети «Интернет» является то, что сеть «Интернет» является глобальным пространством, где информация может свободно передвигаться и публиковаться.

Религия является одним из основных компонентов культуры и оказывает влияние на многие сферы жизни человека. Однако, как и любое явление, она может быть и «инструментом» для достижения целей. Одной из таких целей является использование религиозной идеологии для оправдания экстремистского поведения.

Религиозный экстремизм, по нашему мнению, — это использование религиозных убеждений и идеологии для оправдания насилия и дискриминации, а также для подрыва основных прав и свобод.

Религиозный экстремизм в сети «Интернет» — это распространение и пропаганда радикальных религиозных идеологий, которые могут подстрекать к насилию, ненависти и дискриминации на основе религиозности. Сеть «Ин-

[1] Научный руководитель — СЕЛИМОВА Анара Маратовна, доцент кафедры теории государства и права Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук.

тернет» стала мощным инструментом для распространения идеологий и создания онлайн-сообществ, где радикальные элементы могут поддерживать друг друга и распространять свои идеи.

Сегодня сеть «Интернет» играет огромную роль в жизни человека. В настоящее время практически все аспекты жизни связаны с интернетом. Он стал неотъемлемой частью работы, образования, развлечений и коммуникации. Так же в глобальной сети размещаются и незаконные пропагандистские материалы, направленные на разжигание ненависти и вражды. Они могут использовать социальные сети, видео-хостинги, блоги и форумы для пропаганды своих убеждений. Создают и распространяют материалы, содержащие призывы к насилию, экстремистскую риторику или призывы к дискриминации определенных групп людей[1].

Рассмотрим причины проявления религиозного экстремизма в сети «Интернет»:

— Из-за нехватки достаточных знаний о религии, особенно среди молодежи, возникает одна из главных причин. В данном случае, отсутствие правильного понимания целей и внутренней системы религии приводит к слепой вере в ее правоту.

— Проблема воспитания в семье. Всем известно и доказано, что личность и индивидуальность человека формируются с раннего возраста. Наибольшее влияние на него оказывают родители. В нашей стране много несовершенных и неблагополучных семей. В таких семьях родители часто испытывают ненависть друг к другу или к своим детям.

— Достаточно открытый доступ к информации, связанной с религией и экстремизмом, в сети «Интернет».

В сети «Интернет» существует множество сайтов, на которых можно легко и просто найти призывы к осуществлению тех или иных экстремистских акций, различные пропагандистские ролики, искаженное толкование любого первоисточника (например, Библии или Корана) и т.д.

[1] Кочубей М. А., Мареев П. Л., Смирнов А. А., Сутормина Е. В. Профилактика терроризма и экстремизма в молодежной среде. СПб., 2018. 96 с.

Так же в интернете могут появляться материалы, которые выражают ненависть к определенным религиозным группам или верованиям. Это может способствовать разжиганию напряженности между различными общностями и приводить к конфликтам.

Сеть «Интернет» также может служить платформой для планирования и координации террористических актов. Кроме того, экстремисты могут использовать кибератаки для нарушения коммуникаций, получения конфиденциальной информации и повреждения инфраструктуры[1].

— Радикализация и вербовка: Онлайн-платформы предоставляют удобную среду для экстремистов для распространения своей идеологии и вербовки новых членов. Это может привести к радикализации и росту числа приверженцев экстремистских групп.

— Психологические последствия: Религиозный экстремизм в интернете может оказывать негативное влияние на молодых людей, сказываясь на их психологическом здоровье. Интернет может усиливать идеологическую индоктринацию и отчуждение, что может приводить к чувству изоляции и потери реальности.

Чтобы справиться с последствиями религиозного экстремизма в интернете, необходимо принимать меры для просвещения, противодействия радикализации, сотрудничества между правительством, организациями и интернет-провайдерами, а также развития медицинской и психологической поддержки для потенциальных жертв экстремизма.

Решение проблемы религиозного экстремизма в сети «Интернет» требует комплексного и скоординированного подхода.

Предлагаем некоторые меры, которые, по нашему мнению, могут быть предприняты для борьбы с этой проблемой:

1. Сотрудничество между правительством, интернет-провайдерами и социальными медиа-платформами: Разработка и реализация согласованной стратегии для обнаружения, блокировки и удаления контента, связанного

[1] Кожушко Е. П. Современный терроризм. Анализ основных направлений / под ред. А. Е. Тараса. Минск, 2010. С. 368.

с религиозным экстремизмом. Усиление мер безопасности и мониторинга на онлайн-платформах для предотвращения вербовки и распространения экстремистской идеологии. Например, в США FBI активно работает на предотвращение онлайн-рекрутинга и радикализации[1].

2. Профилактика и просвещение: Усилия по просвещению широкой публики о рисках религиозного экстремизма и его последствиях. Разработка программ и мероприятий для предотвращения радикализации и пропаганды экстремистской идеологии в интернете.

3. Поддержка гражданского общества и локальных сообществ: Помощь и поддержка для отдельных лиц и общин, вовлеченных в процесс религиозной радикализации, а также активное участие неправительственных организаций и религиозных лидеров в противостоянии религиозному экстремизму.

4. Усиление правового регулирования: Разработка более строгого законодательства для пресечения онлайн-экстремизма, а также преследование и судебное привлечение к ответственности лиц, занимающихся вербовкой или пропагандой религиозного экстремизма в интернете.

5. Технологические решения: Разработка и использование специализированных технологий и алгоритмов для автоматического обнаружения и удаления контента, связанного с религиозным экстремизмом. Развитие и внедрение инструментов для улучшения безопасности и фильтрации контента в сети «Интернет».

В заключение хочется сказать, что религиозный экстремизм в сети «Интернет» является серьезной проблемой, которая требует внимания и содействия со стороны правительств, интернет-провайдеров, социальных медиаплатформ, организаций гражданского общества и обычных пользователей.

Сеть «Интернет» предоставляет платформу для быстрого распространения идеологий экстремизма, привлекая молодых людей и искажая их веру, и это может привести к росту насилия, терроризма и радикализации.

[1] Бидова Б. Б. Уголовное законодательство зарубежных государств и международные стандарты в сфере противодействия молодежному экстремизму // Вестник Ессентукского института управления, бизнеса и права. 2011. №°4. С. 60—61.

Однако, при борьбе с религиозным экстремизмом в сети «Интернет» необходимо учитывать принципы свободы слова и свободы выражения, чтобы не затерять баланс между борьбой с экстремизмом и уважением к правам и свободам индивидуальных пользователей.

УДК 343

Р. Л. РАХМАТУЛЛИН,
Н. О. ТУРКОВСКИЙ[1]

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ВИРТУАЛЬНОЙ СОБСТВЕННОСТИ

Актуальность исследования проблемы уголовно-правовой охраны виртуальной собственности обусловлена рядом причин. Во-первых, статистические данные МВД России свидетельствуют о том, что за последние годы значительно возросло число преступных посягательств, совершаемых с использованием сети «Интернет». Особый прирост подобных деяний пришелся на 2018, 2019 и 2020 гг.[2].

Во-вторых, сегодня остается неопределенным правовой статус виртуальной собственности в нашем законодательстве несмотря на то, что с каждым годом растет количество хищений подобных элементов, в частности игровых аккаунтов и предметов, находящихся на данных аккаунтах (например, виртуального оружия).

К примеру, согласно информации, представленной на официальном сайте МВД России, недавно в г. Красноярске полицейскими были задержаны злоумышленники, которые напали на участника компьютерного турнира с целью хищения у него виртуального оружия – «светового меча» стоимостью более 20 тысяч рублей.

---

[1] Научные руководители — ДВОРЖИЦКАЯ Марина Андреевна, старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук; ПИСАРЕВСКАЯ Елена Анатольевна, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

[2] Состояние преступности в Российской Федерации за январь–декабрь 2018, 2019, 2020, 2021, 2022 года // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 20.10.2023).

По данному факту было возбуждено уголовное дело по признакам состава преступления, предусмотренного ч. 2 ст. 162 УК РФ[1]. Иначе говоря, возбуждая уголовное дело, уполномоченные органы признали предметы компьютерной игры имуществом. Однако судебного решения по данному уголовному делу не последовало, что, с большой вероятностью, говорит о том, что оно было прекращено и не дошло до суда, поскольку отсутствовали признаки предмета хищения. В иных подобных выявленных практических примерах правоохранительные органы либо не усматривали состава преступления, поскольку исходя из положений политики конфиденциальности и пользовательского соглашения в онлайн-игре, все предметы и аккаунты принадлежат компаниям, а не пользователям, которые выступают заявителями о краже. Либо хищение виртуальной собственности в результате неправомерного доступа к компьютерной информации было квалифицировано при наличии предусмотренных признаков по ст. 272 УК РФ.

В-третьих, виртуальную собственность невозможно материализовать, что также затрудняет определение права собственности.

В-четвертых, сегодня достаточно активно развивается игровая индустрия и, например, в 2021 году был проведен турнир по компьютерной игре с призовым фондом более 40 миллионов долларов[2].

Это указывает на то, что указанные игры занимают важную роль в развлекательном сегменте, как и другие виды деятельности людей. Кроме того, еще в далеком 2012 году продажи компьютерных игр опередили по продажам фильмы в кинотеатрах[3].

---

[1] Министерство внутренних дел Российской Федерации : сайт. URL: https://xn--b1aew.xn--p1ai/news/item/9145331 (дата обращения: 20.10.2023).

[2] Призовой фонд в киберспорте // TELE 2. Черным по белому : журнал. URL: https://msk.tele2.ru/journal/article/the-biggest-prize-funds-in-cybersport-matches (дата обращения: 20.10.2023).

[3] Продажи компьютерных игр опередили по продажам фильмы в кинотеатрах // Cinemaplex : сайт. URL: https://cinemaplex.ru/2013/04/17/games-vs-cinema.html (дата обращения: 25.10.2023).

В-пятых, в настоящее время активно развивается киберспорт. В частности, киберспорту сегодня уделяется особое внимание и недавно Министерство спорта Российской Федерации выпустило приказ об изменении стандартов подготовки киберспортсменов[1].

Вместе с этим по итогам экономического форума 2023 года, в нашей стране ожидается новый «рывок» в игровой индустрии[2].

Далее обратимся к теории уголовного права. Так, Л.Д. Гаухман определял «предмет преступления», как предмет материального мира, по поводу которого совершается преступное посягательство или на который оказывается непосредственное воздействие со стороны преступника[3].

На первый взгляд, при незаконном изъятии виртуального имущества на него также осуществляется воздействие. Виртуальные игровые предметы можно покупать, продавать, обменивать на деньги. Предмет хищения, в свою очередь, должен обладать набором соответствующих свойств.

В теории уголовного права выделяется три группы этих свойств: физические, экономические и юридические[4]. С одной стороны, возможно установление экономического признака похищаемых виртуальных предметов, поскольку многие из них имеют стоимость более 2 500 рублей, соответствующую сумме, с которой начинается уголовная ответственность за простое хищение.

С другой стороны, виртуальные предметы не являются материализованными, что указывает на отсутствие физического признака хищения. Хотя в то же время в п. «г» ч. 3 ст. 158 УК РФ законодатель делает исключение в отно-

---

[1] О внесении изменений в федеральный стандарт спортивной подготовки по виду спорта «компьютерный спорт» : Приказ Министерства спорта Российской Федерации от 11 января 2022 г. № 938. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Перечень поручений по итогам Восточного экономического форума // Президент России : офиц. сайт. URL: https://www.kremlin.ru/acts/assignments/orders/72740 (дата обращения: 25.10.2023).

[3] Гаухман Л. Д., Максимов С. В. Ответственность за преступления против собственности. 3-е изд., испр. М., 2002. С. 13.

[4] Юсефи М. Х. Проблемы соотношения объекта и предмета хищения имущества в уголовном законодательстве // Вектор науки тольяттинского государственного университета. серия: юридические науки. 2013. № 1 (12). С. 49.

шении данного правила, предусматривая уголовную ответственность за хищение безналичных денег, которые также не являются материальными (осязаемыми). Кроме того, вызывает сложности установление юридического признака хищения виртуального имущества в игре, в частности установление его собственника.

С одной стороны, виртуальные предметы в игре можно рассмотреть через призму иного имущества, указываемого в статье 128 ГК РФ. Однако единого подхода к пониманию названного термина не сложилось. Как предполагает М.А. Корчагин словосочетание «иное имущество» добавлено в перечень объектов гражданских прав на всякий случай[1].

К примеру, в случаях если в гражданском обороте появятся те элементы, которые вроде бы попадают в сферу интересов гражданского права, однако, не подпадают под признаки закрепленных объектов гражданских прав, указанных в ст. 128 ГК РФ. Однако обращение к ч. 2 ст. 144.1 ГК РФ позволяет сделать вывод о том, что право собственности на виртуальное имущество принадлежит компаниям, на которых производится обмен, продажа и возврат товаров.

С другой стороны, исследование пользовательских соглашений таких компаний (к примеру, Steam[2], VK Play[3], Epic Games[4]) позволило прийти к выводу, что виртуальная собственность в пользовательском соглашении игры обозначается не иначе как «Подписка», «Вознаграждение», «Виртуальная ценность». Кроме того, в соглашениях непосредственно прописывается, что права собственности на предметы торговой площадки (Визуальные эффекты и раскраски) не принадлежат пользователям. Вместе с тем в указанных соглашениях отмечается, что пользователям принадлежат только лицензионные права.

[1] Карчагин М. А. Иное имущество как объект гражданских прав // Вопросы российской юстиции. 2020. № 6. С. 142.

[2] URL: https://store.steampowered.com/subscriber_agreement/ (дата обращения: 25.10.2023).

[3] URL: https://documentation.vkplay.ru/terms_vkp/tou_vkp (дата обращения: 25.10.2023).

[4] URL: https://store.epicgames.com/ru/eula (дата обращения: 25.10.2023).

Исследование лицензионного договора, регламентируемого ст. 1235 ГК РФ свидетельствует о том, что обладатель исключительного права на интеллектуальные права или средство индивидуализации предоставляет или обязуется предоставить другой стороне право использования. В части 2 этой же статьи говорится, что данный договор обязательно должен быть заключен в письменной форме, в ином случае он не будет считаться недействительным.

Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) «Об электронной подписи» утверждает, что электронный документ может быть признан равнозначным документам на бумажном носителе, подписанным собственноручной подписью[1].

В ст. 1254 ГК РФ указано, что лицензиат наряду с другими способами защиты может защищать свои права. Также имеется Приказ Минпромторга России от 21.07.2023 № 2701 «Об утверждении перечня товаров (групп товаров), в отношении которых не применяются положения статей 1252, 1254, п. 5 статьи 1286.1, статей 1301, 1311, 1406.1, подпункта 1 статьи 1446, статей 1472, 1515 и 1537 ГК РФ при условии введения указанных товаров (групп товаров) в оборот за пределами территории РФ правообладателями (патентообладателями), а также с их согласия» в котором не указано лицензионных соглашений или «Подписок» на какие либо товары.

Также стоит отметить, что в настоящее время на территории Российской Федерации, согласно п. 7 ст. 14 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[2], ограничена возможность пополнения кошелька онлайн-сервиса цифрового распространения компьютерных игр и программ «Steam».

Однако в пользовательском соглашении указывается на то, что «Кошелек «Steam» не является ни банковским счетом, ни любым другим инструментом

[1] Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ : текст с изм. и доп. на 4 авг. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ : текст с изм. и доп. на 4 авг. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

платежа, так как предназначен для заказа контента и услуг после его предварительного пополнения». Как следует из пользовательского соглашения, кошелек Steam не является цифровой валютой. Вместе с тем, на основании п. 3 ст. 1 Федерального закона от 31.07.2020 № 259-ФЗ (ред. от 14.07.2022) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1], средства на кошельке «Steam» вполне подпадают под понятие цифровой валюты. Учитывая то, что положения вышеуказанного пользовательского соглашения не соответствуют в полной мере российскому законодательству, то такой договор будет считаться недействительным на территории нашей страны, а все последствия такого договора – ничтожными.

На основании вышеизложенного, можно сказать, что современные технологии повсеместно развиваются. Виртуальные игровые предметы сегодня покупаются, продаются, обмениваются на деньги и похищаются. Причем некоторые из этих элементов приобретаются за большую стоимость. Однако сегодня охрана виртуального имущества в игре затрудняется по ряду причин, в частности, это связано с отсутствием понятия виртуальной собственности, пользовательским соглашением онлайн-игры, которое заключается между компанией и пользователем-игроком, несоответствием указанных соглашений российскому законодательству. В итоге за пользователями закреплены права пользования, поскольку согласно соглашению, право собственности остается за компанией. Все это, на наш взгляд, затрудняет защиту прав физических лиц, чье игровое имущество похищается.

Таким образом, сегодня складывается неопределенная ситуация, связанная с защитой виртуальной собственности в онлайн-игре, в том числе уголовно-правовыми средствами. Ни гражданское, ни уголовное законодательство не адаптированы к развитию таких технологий, хотя игровая виртуальная индустрия масштабно развивается в нашей стране. В результате, хищение предметов в он-

[1] Там же.

лайн-играх пока в нашей стране остается не урегулированным. Это, в свою очередь, приводит к тому, что правоохранительные органы не имеют необходимых инструментов защиты виртуальной собственности. В этой связи предлагается несколько путей решения указанной проблемы: 1) конкретизация перечня иного имущества в гражданском праве (ст. 128 ГК РФ), к которому можно было бы отнести предметы виртуальной собственности в игре или включение виртуальных активов в качестве самостоятельного объекта гражданского права; 2) создание подразделения в правоохранительных органах, специализирующегося на раскрытии и расследовании уголовных дел в области хищений виртуальных предметов; 3) введение международных и/или государственных стандартов или инструкций по содержанию пользовательских соглашений.

УДК 343

Д. С. РОГАНОВА[1]

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЦ, СОВЕРШАЮЩИХ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

В настоящее время государственная политика Российской Федерации направлена на совершенствование системы обеспечения безопасности общественных отношений с использованием электронных или информационно-телекоммуникационных сетей. Анализ данных официальной статистики показал, что удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации от общего числа зарегистрированных преступлений за январь-ноябрь 2018 года составил 8,5 % (156 307 преступлений); за этот же период 2019 г. – 14 % (261 208); 2020 г. – 24,4 % (461,2 тыс.); 2021 г. – 26,7 % (494 тыс.); 2022 г. – 25,8 % (470,1 тыс.)[2].

[1] Научный руководитель — ЗИМИРЕВА Людмила Александровна, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

[2] Ежемесячный сборник о состоянии преступности в России // Портал правовой статистики : портал. URL: https://crimestat.ru/analytics (дата обращения: 01.11.2023).

Следует сделать вывод о том, что количество преступлений в этой сфере за январь-ноябрь 2018–2021 гг. увеличилось, однако в 2022 г. произошли некоторые изменения в статистике, свидетельствующие о снижении уровня зарегистрированных преступных деяний. Отметим, что, несмотря на данную динамику, это не свидетельствует об уменьшении степени опасности в области информационных технологий.

Необходимо акцентировать внимание на том, что в современном мире стремительно модернизируются информационные технологии, которые имеют важное значение в жизнедеятельности человека в целом. Научно-технический прогресс способствует распространению и использованию электронных операций буквально во всех сферах общества. Так, преступлениям в сфере компьютерной информации было определено отдельное место в самостоятельной главе УК РФ, введенным в действие Федеральным законом от 13.06.1996 № 64-ФЗ. Уголовно-правовая охрана компьютерных сведений в период совершенствования информационной инфраструктуры представляет один из существенных элементов в обеспечении информационной безопасности государства. Обозначим, что в научной литературе среди ученых ведутся дискуссии не только о составах преступлений в рассматриваемой нами сфере, но и о лицах, которые их совершают.

В криминологии личность преступника является значимым объектом изучения механизма противоправного деяния. Проблемы, связанные с личностью человека, совершающего преступление, является центральной в криминологии и вызывает наибольшие дискуссии среди ученых. Это связано с тем, что именно в этом исследуемом нами понятии пересекаются во взаимодействии объективные и субъективные факторы детерминации преступного поведения[1].

Так же необходимо обозначить, что некоторые особенности личности имеют черты, отличные от иных лиц, совершающих другие преступления. Ра-

[1] Криминология : учебник для вузов / В. И. Авдийский [и др.] ; под ред. В. И. Авдийского, Л. А. Букалеровой. 2-е изд., перераб. и доп. М., 2023. С. 69.

бота по изучению личности преступника производится с целью предупреждения, пресечения, выявления, устранения, профилактики правонарушений и правотворчества, связанным с криминализацией и декриминализацией деяний.

С каждым годом происходит модернизация информационных технологий, электронной техники, компьютерных программ, компьютеризации общества в целом, что обуславливает появление новых способов совершения преступлений в этой сфере. Вследствие этого рассмотрение вопросов, связанных с характеристикой лиц, совершающих преступления в сфере компьютерной информации, вызывает наибольший интерес, как с теоретической, так и практической стороны. Так, в ходе получения реального образа жизни личности в данной области необходимо обращать внимание на комплексный подход к ее формированию посредством биологических, социальных и экономических факторов, включая, например, социально-демографические, психологические, нравственные, образовательно-технические особенности, цели и мотивы преступного выбора[1].

В научной литературе нет единого мнения о возрасте преступника, совершающего преступления в сфере информационных технологий. Некоторые авторы приводят следующие данные, а именно 16–25 лет[2], возраст до 35 лет[3], до 50 лет[4]. Как отмечает Д.Д. Перфильева, личности преступника в сфере компьютерной информации присущи следующие черты: замкнутость; склонность к депрессии, переживаниям, неврозам, обидам[5]. Преступник может действовать

[1] Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общ. ред. О. С. Капинус. 2-е изд., перераб. и доп. М., 2023. С. 1010.

[2] Евдокимов К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) // Сибирский юридический вестник. 2011. № 1 (52). С. 89.

[3] Криминология : учебник для вузов / О. С. Капинус [и др.] ; под общ. ред. О. С. Капинус. 2-е изд., перераб. и доп. М., 2023. С. 1013.

[4] Родивилин И. П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 28.

[5] Перфильева Д. Д. Частные психологические характеристики личности киберпреступника // Актуальные вопросы юриспруденции : сборник статей VII Международной научно-практической конференции (г. Пенза, 25 мая 2021 г.). Пенза, 2021. С. 239.

импульсивно или готовиться заранее, продумывать каждый свой шаг[1]. Полагаем, что анализ психологических аспектов в большинстве случаях позволяет определить цели и мотивы совершения преступления, что положительно отражается на правильной квалификации деяния. При подготовке или в ходе совершения преступного деяния в исследуемой нами области у человека появляются потребности, выражающиеся в самоутверждении, превосходстве над окружающими, повышении карьерного роста, ненависти, мести, обиде, ревности, завладении имуществом, любопытстве, политических мотивах, хулиганских побуждениях, недобросовестной конкуренции; поддержании дружеских отношений.

Например, К.С. Квятковский приходит к выводу о том, что личность характеризуется «правовым нигилизмом, нежеланием жить по правилам, установленным обществом, руководство корыстными, хулиганскими или иными мотивами, испытывают чувство безнаказанности и превосходства в связи с обезличенностью персоны в киберпространстве»[2]. Думается, что правовой нигилизм неразрывно связан с правосознанием, которое формирует в определенном направлении отношение человека к праву. Следовательно, это негативное явление нуждается в способах профилактики и его искоренения.

Одним из важных факторов, учитываемых при характеристике личности, выступает наличие профильного образования и обладание навыками работы с информационными технологиями. Обратимся к примерам судебной практики. В приговоре Октябрьского районного суда г. Ростова-на-Дону отражено, что лицо, обладая познаниями и навыками компьютерного программирования, используя личные средства компьютерной техники, в том числе ЭВМ с подключенными носителями информации посредством программирования, удовлетворяя свой интерес к познаниям в области информационной безопасности, желая получать доход от деятельности в данной сфере, создало

[1] Ефремов К. А. Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. 2016. № 7. С. 94.

[2] Квятковский К. С. Особенности личности преступника, совершающего преступления в сфере компьютерной информации // Молодой ученый. 2022. № 43 (438). С. 116.

компьютерную программу, предназначенную для проверки состояния учетных записей, которую продолжало модифицировать с использованием указанной компьютерной техники[1].

В другом приговоре Фрунзенского районного суда г. Саратова у лица, обладающего специальными познаниями в области компьютерной техники и программного обеспечения, возник преступный умысел, направленный на использование компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности, в целях облегчения совершения другого преступления, а именно неправомерной модификации компьютерной информации игровой консоли «Xbox 360», совершенное из корыстной заинтересованности[2].

Одновременно с вышеизложенным, лица, совершающие преступления в сфере компьютерной информации, характеризуются стремлением получить выгоду, в том числе совершая противоправные деяния с использованием своего должностного положения.

В приговоре Ленинского районного суда г. Саратова зафиксировано, что у лица, находящегося в салоне (на рабочем месте), возник преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ПАО «МТС» и их лицевых счетов, путем модификации данной информации, из иной личной заинтересованности, выразившейся в оказании помощи знакомому, материалы в отношении которого выделены в отдельное производство, для дальнейшего поддержания с ним дружеских отношений[3].

---

[1] Приговор Октябрьского районного суда г. Ростова-на-Дону от 1 декабря 2017 г. № 1-613/2017 // Судебная практика : сайт. URL: https://sud-praktika.ru (дата обращения: 01.11.2023).

[2] Приговор Фрунзенского районного суда г. Саратова по делу № 1-116/2017 // Судебная практика : сайт. URL: https://sud-praktika.ru (дата обращения: 01.11.2023).

[3] Приговор Ленинского районного суда г. Саратова по делу № 1-395/2017 // Судебная практика : сайт. URL: https://sud-praktika.ru (дата обращения: 01.11.2023).

Таким образом, исходя из вышеизложенного, мы пришли к следующему выводу, который с нашей точки зрения имеет, как теоретическое, так и практическое значение. Личность преступника в сфере компьютерной информации — субъект преступления, обладающий следующими основными особенностями: замкнутость; склонность к переживаниям; определенными мотивами и целями, выражающимися в самоутверждении, превосходстве над окружающими, повышении карьерного роста, ненависти, мести, обиде, ревности, завладении имуществом, любопытстве, политических мотивах, хулиганских побуждениях, недобросовестной конкуренции, поддержании дружеских отношений; низким уровнем правовой культуры; правовым нигилизмом; образованием и навыками работы с информационными технологиями; чувством безнаказанности и вседозволенности. Знание криминологической характеристики личности имеет важное значение не только для формирования доказательственной базы, правильной квалификации деяния в практической деятельности, но и определения мотивов, целей, способов совершения преступлений в данной области с целью их предотвращения и профилактики.

УДК 343

В. А. САРАПКИН[1]

О НЕКОТОРЫХ ВОПРОСАХ КВАЛИФИКАЦИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЯ) ДЕНЕЖНЫХ СРЕДСТВ ИЛИ ИНОГО ИМУЩЕСТВА, ПРИОБРЕТЕННЫХ ПРЕСТУПНЫМ ПУТЕМ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»

В современных условиях неурегулированности правового статуса криптовалюты у правоприменителя возникают сложности при квалификации деяний, предусмотренных ст.ст. 174, 174.1 УК РФ, совершенных с использованием этого средства, особенно в сфере незаконного сбыта наркотических средств, психотропных веществ или их аналогов.

[1] Научный руководитель —ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент.

Актуальность рассмотрения данного вопроса обусловлена тем, что в настоящее время «сбыт наркотических средств чаще всего осуществляется бесконтактным способом, при помощи сети «Интернет», это также упрощает возможность легализации (отмывания) денежных средств, приобретенных от такой преступной деятельности»[1].

Пленум Верховного Суда Российской Федерации в п. 1 Постановления № 32 от 07.07.2015 г. (ред. 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» обращает внимание правоприменителя на то, что предметом легализации могут являться денежные средства, преобразованные в виртуальные активы (криптовалюту), приобретенных в результате совершения преступления[2].

Данная правовая позиция Верховного Суда Российской Федерации явилась следствием ратификации Российской Федерацией Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма, а также Рекомендации 15 ФАТФ.

С учетом транснационального характера легализации Верховный Суд Российской Федерации справедливо стремится привести национальную судебную практику в русло международных стандартов в целях эффективного противодействия отмывания денежных средств или иного имущества, приобретенных преступным путем.

Тем не менее Постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 г. (ред. 26.02.2019) № 32 «О судебной практике по

---

[1] Лупырь М. В. Уголовно-правовая оценка легализации (отмывания) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1 УК РФ) : автореф. ... канд. юрид. наук. Омск, 2019. С. 4.

[2] О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем : Постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 : текст с изм. и доп. на 26 февр. 2019 г. Доступ из справ.-правовой системы «КонсультантПлюс».

делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» не разрешает главных задач, стоящих перед следственными органами и прокурором при квалификации преступлений, предусмотренных ст.ст. 174, 174.1 УК РФ.

Так, ни в одном законодательном акте не содержится определения криптовалюты, что в свою очередь порождает проблемы при расследовании преступлений, предусмотренных ст.ст. 174, 174.1 УК РФ, их квалификации и последующей инкриминации лиц.

Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ апеллирует понятием «цифровая валюта», запрещая ее использования в качестве средства оплаты товаров и услуг на территории России.

Исходя из законодательной конструкции диспозиции ст. 174 УК РФ предметом легализации являются денежные средства или иное имущество, то есть объекты гражданских прав, указанные в ст. 128 ГК РФ. С учетом открытого перечня видов имущества в данной норме, некоторые суды относят криптовалюту именно к имуществу[1].

Так, по кассационному представлению прокуратуры города Санкт-Петербурга были отменены приговор районного суда и апелляционное определение городского суда по уголовному делу, по которому суды пришли к выводу о том, что криптовалюта «не является объектом гражданских прав, так как не может быть отнесена к вещам, включая наличные деньги и документарные ценные бумаги, иному имуществу, в том числе безналичным денежным средствам, бездокументарным ценным бумагам, имущественным правам; результатам работ и оказания услуг; охраняемым результатам интеллектуальной деятельности

[1] Малаховский А. 9-й ААС признал криптовалюту имуществом // Право.Ру : сайт. https://pravo.ru/story/202325 (дата обращения: 23.10.2023).

и приравненным к ним средствам индивидуализации (интеллектуальная собственность), в связи с чем не может выступать предметом хищения»[1].

Не согласившись с данной позицией судов, прокуратура города обжаловала судебные акты в Третий кассационный суд общей юрисдикции, который определил, что цифровая валюта могла быть принята в качестве средства платежа, продана и конвертирована в рубли, которыми противоправно завладели фигуранты уголовного дела. В ходе нового судебного рассмотрения данного уголовного дела районный суд согласился с позицией государственного обвинителя о том, что криптовалюта является предметом хищения[2].

Поскольку применение уголовного закона по аналогии не допускается признание криптовалюты имуществом по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, является достаточно противоречивым суждением.

Так, оценить стоимость легализованной криптовалюты в настоящее время не представляется возможным. Исходя из смысла абз. 4 п. 1 Постановления Пленума Верховного Суда Российской Федерации от 07.07.2015 (ред. 26.02.2019) № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» предлагаемая методика оценки легализованного имущества «из фактической стоимости имущества, составляющего предмет данных преступлений» не реализуема на практике. Например, оценить рыночную фактическую (рыночную) стоимость наркотиков невозможно. В то же время ВС РФ предусмотрел возможность привлечения экспертов

[1] Апелляционное определение Санкт-Петербургского городского суда от 23 ноября 2020 г. по делу № 1-95/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] В г. Санкт-Петербурге криптовалюта признана предметом хищения на основании решения суда, вступившего в законную силу // Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://epp.genproc.gov.ru/web/proc_78/mass-media/news?item=73895418.

и специалистов к оценке легализованного имущества. Думается, что специалистов по оценке криптовалюты в экспертно-криминалистических центрах МВД России явно недостаточно.

По данным судебной статистики за 2022 год в России по преступлениям, предусмотренным ст.ст. 174, 174.1 УК РФ было осуждено всего 17 человек[1]. В то время как по данным Росфинмониторинга ежегодно в нашей стране легализуется 250–300 млрд рублей преступных доходов[2]. В 2022 году Генеральный прокурор Российской Федерации отметил, что в минувшем году удалось доказать факты легализации на 40 млрд рублей[3]. Данные свидетельствуют о высокой латентности данных преступлений.

Думается, что одной из проблем, по которой органы предварительного расследования и прокурор не включают в объем обвинения легализацию преступных доходов от совершения предикатного преступления является сложность определения предмета преступлений, предусмотренных ст.ст. 174, 174.1 УК РФ.

По нашему мнению, это может объясняться тем, что в действующем законодательстве отсутствует легальное определение понятия «криптовалюта», поэтому однозначно отнести ее к «денежным средствам» или «иному имуществу» нельзя.

А.В. Зарубин справедливо полагает, что признание криптовалюты предметом легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем является недопустимым, поскольку определенная в п. 8 Постановления Пленума № 32 специальная цель (криминообразующий признак), заключающая в придании правомерного вида владению, пользованию и распоряжению денежными средствами или иным

[1] Данные о назначенном наказании по статьям УК РФ // Судебная статистика РФ : сайт. URL: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 (дата обращения: 19.10.2023).

[2] Халитова, Р. Р. Актуальные вопросы противодействия легализации (отмыванию) денежных средств, добытых преступным путем // Международный Молодежный научный форум «Ломоносов 2021» : материалы / отв. ред. И. А. Алешковский, А. В. Андриянов, Е. А. Антипов, Е. И. Зимакова. М., 2021.

[3] Краснов И. В. Борьба с отмыванием доходов и финансированием терроризма: итоги работы и основные задачи // Финансовая безопасность. 2023 № 37/2023. С. 6.

имуществом, приобретенными преступным путем (в результате совершения преступления) в случае покупки криптовалюты достигнута не будет[1].

В аспекте проблематики данного вопроса необходимо подчеркнуть, что непризнание предметом легализации криптовалюты не означает, что «отмытые» денежные средства при совершении лицом предикатного преступления не будут учтены судом при назначении наказания.

В случае перевода «отмытых» денежных средств в криптовалюту «предметом легализации по-прежнему будут выступать вырученные в результате проведения финансовых операций денежные средства, приобретенные преступным путем»[2].

Данная точка зрения видится нам наиболее обоснованной и находит свое отражение в позиции Верховного Суда Российской Федерации.

Так, приговором Рязанского областного суда К. был признан виновным всовершении преступлений, предусмотренных ч. 2 ст. 228.3 УК РФ и ч. 5 ст. 228.1 УК РФ и оправдан по п. «б» ч. 2 ст. 174.1 УК РФ за отсутствием в его действиях состава преступления. Также Судебной коллегией по уголовным делам Первого апелляционного суда общей юрисдикции К. был оправдан по п. «б» ч. 4 ст. 174.1 УК РФ. В ходе предварительного расследования было установлено, что К. принимал оплату за сбыт наркотических средств в биткоинах, затем конвертировал их в рубли и переводил на счет своего доверенного лица (в общей сложности 8,2 млн рублей).

Вышеизложенное, несомненно, позволяет нам сделать вывод о том, что в действиях К. по конвертации криптовалюты в рубли усматривается специальная цель (криминообразующий признак) легализации, о котором мы говорили ранее.

---

[1] Зарубин А. В. Некоторые вопросы квалификации легализации (отмывания) денежных средств, приобретенных преступным путем с использованием криптовалюты // Уголовное законодательство: вчера, сегодня, завтра : материалы ежегодной Всероссийской научно-практической конференции (Санкт-Петербург, 18–19 мая 2021 года) / под ред. Т. А. Огарь, Д. М. Кокина ; сост.: Т. А. Огарь, Д. М. Кокин. 2021. Ч. 1. С. 115.

[2] Сарапкин В. А. Некоторые проблемы определения момента окончания преступлений, предусмотренных ст.ст. 174, 174.1 УК РФ // Уголовное право: актуальные вопросы теории и практики : сборник докладов Всероссийского студенческого научно-практического круглого стола с международным участием (Санкт-Петербург, 17 февраля 2023 г.) / под ред. Е. Н. Рахмановой, Е. А. Писаревской, М. А. Дворжицкой. СПб., 2023. С. 124.

В кассационном определении по данному делу Верховный Суд Российской Федерации указал, что «зачисление денежных средств на подконтрольный виртуальный счет - криптовалюту «биткоин», дальнейшее ее конвертирование через различные виртуальные обменники в рубли, перевод денежных средств на банковские карты, зарегистрированные на другое лицо и их обналичивание через банковские терминалы, свидетельствует о наличии у осужденного цели легализовать денежные средства»[1].

Приговор Рязанского областного суда и апелляционное определение Первого апелляционного суда общей юрисдикции в отношении К. в части оправдания по п. «б» ч. 4 ст. 174.1 УК РФ был отменен Верховным Судом Российской Федерации.

Резюмируя вышеизложенное, мы можем сделать вывод, что сам факт перевода преступно добытых денежных средств в криптовалюту нельзя квалифицировать по ст. 174.1 УК РФ поскольку в данном случае специальная цель легализации достигнута не будет. Тогда как конвертация криптовалюты в рубли свидетельствует об окончании преступления, предусмотренного ст. 174.1 УК РФ так как данная финансовая операция маскирует связь легализуемых денежных средств с преступным источником их происхождения (предикатным преступлением).

Предлагается внести изменения п. 1 Постановления Пленума Верховного Суда Российской Федерации от 07.07.2015 г. (ред. 26.02.2019) № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» в целях уточнения предмета преступлений, предусмотренных ст.ст. 174, 174.1 УК РФ. Поскольку правовой статус криптовалюты в Российской Федерации до конца не определен, ее не следует приравнивать к электронным денежным средствам как предмету легализации.

[1] Кассационное определение Верховного Суда Российской Федерации от 8 июня 2023 г. по делу № 6-УДП23-6-А1. Доступ из справ.-правовой системы «КонсультантПлюс».

Данная позиция коррелируется с нормативными положениями статьи 27 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в которой содержится прямой запрет выпуска на территории Российской Федерации денежных суррогатов[1].

Данные изменения, по нашему мнению, будут способствовать установлению единообразия судебной практики и отвечать принципу неотвратимости наказания.

УДК 343

Р. В. СЕРДЮКОВ[2]

НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Одним из пунктов стратегии национальной безопасности Российской Федерации, является положение, согласно которому противодействие и искоренение коррупции является одним из главных приоритетов гражданского общества и правоохранительных органов[3].

Как и любое явление коррупция развивается вместе с обществом, участники организованных преступных сообществ ищут, способы реализации своего преступного умысла преследуя свои корыстные и иные цели. Зачастую каждый из них желает избежать наказания и скрывает следы преступлений, уничтожает доказательства и использует высокие технологии во зло, для того чтобы облегчить свою преступную деятельность.

---

[1] О Центральном банке Российской Федерации (Банке России) : Федеральный закон от 10 июля 2002 г. № 86 : текст с изм. и доп. на 4 авг. 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Научный руководитель — КАЛИНКИНА Анна Борисовна, старший преподаватель кафедры уголовного права и криминологии академии Следственного комитета Российской Федерации.

[3] О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 г. № 400. Доступ из справ.-правовой системы «КонсультантПлюс».

Одним из самых сложных и популярных инструментов современной высокотехнологичной преступности являются криптовалюты, поскольку они обеспечивают: анонимность и высокую скорость переводов больших денежных масс, цифровые носители крипто валют легко хранятся в труднодоступных местах или вовсе не имеют физического воплощения в материальном мире.

Сам процесс расследования преступлений в сфере криптовалют называется crypto-investigation, мы не будем вдаваться в подробности методологии анализа Blockchain, а раскроем несколько тактических приемов при расследовании коррупционных преступлений с использованием криптовалют.

Одним из главных вопросов расследования коррупционных преступлений являются установления механизма получения, места хранения и способа распоряжения предметом взятки. В случае с крипто валютами, мы часто сталкиваемся со следственной ситуацией, когда субъект преступления уже обладает крипто валютами и может распоряжаться ими, либо владеет ключами и аккаунтами, которые позволяют ему де-факто владел криптоактивами.

Мы предлагаем заострить свое внимание исследовании цифрового следа участника уголовного-судопроизводства, а именно: на цифровых кошельках (аккаунтах на централизованных крипто биржах), и аккаунтах в мессенджере Telegram.

Наш научный интерес обоснован тем, что холодный кошелек (техническое устройство), хранящее в себе сид-фразу (приватный ключ самого кошелька), может быть найден в ходе обыска, а искусство его отыскания и изъятия не отличается от обыска сходных преступлений. Но на текущей момент методология отыскания цифровых кошельков не концептуализирована.

Множество бирж покинуло юрисдикцию Российской Федерации и не позволяет как вывести крипто-активы, так и распоряжаться ими, однако в правоприменительной практике есть случаи, когда взяточник покидал территорию Российской Федерации[1].

[1] Челябинского депутата Госдумы лишили мандата спустя год после приговора за взятку в 3 миллиарда // 74.RU : сайт.URL: https://74.ru/text/criminal/2023/11/13/72909011/ (дата обращения: 13.11.2023).

Если преступник получит вид на жительство, той или иной страны, где находится представительство юридического лица централизованной крипто-биржи он может открыть счет в банке и получить доступ к преступно нажитому имуществу.

Поэтому кроме стандартных форм запросов судебных и правоохранительных органов доступных, например, в Binance, или KuCoinследователю стоит обратиться к формам восстановления аккаунтов[1].

Множество централизованных крипто бирж позволяют восстановить пароль от аккаунта, при вводе мобильного телефона, указанного при регистрации, данный набор действий позволяет установить наличие у преступника аккаунта на критобирже[2]. Аналогично может быть использован е-мейл, который также следует использовать в форме восстановления. В любом случае, положительный результат многократно упрощает следственную ситуацию, поскольку служащему органа правопорядка будет известно где могут храниться крипто активы злоумышленника.

Однако стоит уяснить, что при заполнении формы восстановления доступа оповещается сам владелец аккаунта, поэтому необходимо спланировать следственные действия так, чтоб у злоумышленника не было времени вывести свои активы из обнаруженного счета, иначе в результате халатности средства могут быть переданы подельникам на холодный кошелек, который не будет доступен органам правопорядка.

Рассмотрев таким образом актуальный способ установления наличия аккаунтов на крипто биржах нам следует перейти к следующему аспекту установления возможности владения крипто валютами, а именно изучение цифрового следа преступника в мессенджере Telegram.

[1] Система запросов для правоохранительных органов // Binance : сайт. URL: https://www.binance.com/ru/support/law-enforcement (дата обращения: 13.11.2023).

[2] Форма восстановления доступа к аккаунту // Binance : сайт. URL: https://accounts.binance.com/ru/login (дата обращения: 13.11.2023).

Telegram-аккаунт регистрируется на номер телефона, сразу после регистрации аккаунту присевается ID (уникальный идентификационный номер), который нельзя поменять, после этого пользователю предоставляется возможность выбрать себе никнейм. Таким образом следователь при расследовании преступлений коррупционной направленности должен уяснить для себя, что предполагаемый злоумышленник, используя мессенджер Telegram в рамках своего преступного умысла порождает три идентификационных элемента: мобильный телефон, уникальный идентификатор и при желании пользователя никнейм[1].

На основании этой информации мы можем изучать поведение преступника в мессенджере Telegram с помощью нескольких инструментов. Telegram-bot Insight соберет интересы пользователя (они в свою очередь появляются, если пользователь подписывается на различные публичные каналы)[2]. Для примера мы возьмем уникальный идентификатор Telegram (445588014).

При исследовании цифрового следа пользователя нами выявлено, что в его интересах мы можем найти криптовалюту TON. Чаще всего, если преступник сведущ в вопросах криптовалют и он активно пользуется различными сервисами для ее обмена, мы можем найти кластеризацию интересов.

Надлежащим примером будет пользователь с уникальными идентификационным номером 36265675, в его интересах можно найти: nft токены, новости о крипто биржах и так далее. Иными словами, мы увидим интерес не к конкретному крипто активу, но и к сфере цифровых финансов в целом.

Стоит также обратить отдельное внимание на выделение интереса p2p, данной вид торговли обозначает, что пользователь, используя сервис как гарант, обменивает крипто валюту на фиатные деньги непосредственно минуя

[1] Telegram FAQ // Telegram Messenger. URL: https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here (дата обращения: 13.11.2023).

[2] Insight bot // Telegram Messenger. URL: https://t.me/ibhld_bot (дата обращения: 13.11.2023).

какие-либо институциональные сервисы. Эта информация чрезвычайно важна для нас, поскольку при дальнейшем проведении следственных действий мы будем обладать информацией, согласно которой подозреваемый или обвиняемый на своем мобильном устройстве связи или персональном компьютере имеет доступ к соответствующим площадкам, для примера нам стоит указать телеграм-боты: Wallet[1], BTC banker[2]

Таким образом мы можем примерно оценить умения человека распоряжаться крипто активами, также нас может интересовать его активное общение по указанным нами ранее темам, достигается это с помощью нескольких инструментов, а именно: Telesint, Tgscan Robot и FunStat Bot.

Их функционал заключается в возможности изучения активности пользователя в открытых чатах, посвященных различными темам, например используя исследуя уникальный идентификатор 590426254, мы можем найти сообщения пользователя, который интересуется особенностями холодного кошелька[3].

Таким образом, при расследовании коррупционных преступлений мы всегда должны предполагать, что взяточник или взяткодатель может пользоваться крипто валютой для исполнения своего преступного умысла.

В целях повышения эффективности профилактики и расследования таких преступлений, мы предлагаем изучать цифровой след участников уголовного судопроизводства как в прокурорской, так и в следственной, оперативно-разыскной деятельности. Использовать формы восстановления аккаунтов и официальных запросов правоохранительных органов для наиболее результативного пресечения и расследования коррупционных преступлений, связанных с использованием криптовалют.

---

[1] Wallet // Telegram Messenger. URL: https://t.me/wallet (дата обращения: 13.11.2023).

[2] BTC_CHANGE // Telegram Messenger. URL: https://t.me/BTC_CHANGE_BOT (дата обращения: 13.11.2023).

[3] Пример сообщения в открытом сообществе // Telegram. URL: https://t.me/forging_pzm/7423 (дата обращения: 13.11.2023).

УДК 343

М. К. СОЛОВЬЕВА[1]

ЭЛЕКТРОННЫЙ ДОКУМЕНТ КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 327 УК РФ

В связи с развитием электронного документооборота становится актуальным вопрос квалификации преступлений, связанных с подделкой и использованием поддельных электронных документов.

В диспозиции ст. 327 УК РФ, предусматривающей ответственность за подделку, использование и оборот поддельных документов, не указано, являются ли электронные документы предметом данного преступления или речь идет только о письменных документах, но еще до разъяснений Верховного Суда в теории высказывалась точка зрения о том, что электронные документы также могут быть предметом данного состава[2]. Данный подход нашел отражение в Постановлении Пленума Верховного Суда Российской Федерации «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324-327.1 УК РФ», где говорится, что как официальные, так и неофициальные электронные документы являются предметом этих преступлений[3].

Легальное определение электронного документа дано в ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», где электронным документом признается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных

[1] Научный руководитель — ПРЯХИНА Надежда Ивановна, доцент кафедры уголовного права Санкт-Петербургского государственного университета, кандидат юридических наук.

[2] Клепицкий И. А. Документ как предмет подлога в уголовном праве // Государство и право. 1998. № 5. С. 68—75.

[3] О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324—327.1 Уголовного кодекса Российской Федерации : Постановление Пленума Верховного Суда Российской Федерации от 17 декабря 2020 № 43. Доступ из справ.-правовой системы «КонсультантПлюс».

машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах[1].

Для электронного документа характерны следующие особенности: создается в электронной форме, может передаваться с помощью информационно-телекоммуникационных сетей или систем, воспринимается человеком только с помощью технических средств.

Обязательным признаком любого документа являются его реквизиты, и в отношении электронного документа речь идет об электронно-цифровой подписи (ст. 6 Федерального закона «Об электронной подписи»[2]), которая позволяет обеспечить конфиденциальность закрепленной информации, ее целостность, а также аутентификацию автора и иных свойств документа[3].

Как было отмечено ранее, электронный документ, так же, как и бумажный, может быть предметом подделки, но для электронного документа существует еще один способ подделки, помимо тех, которые могут быть совершены в отношении бумажного (материальный - незаконное изменение отдельных частей подлинного документа путем подчистки, дописки, замены элементов, и интеллектуальный - изготовление нового документа, содержащего заведомо ложные сведения). Им является незаконное использование электронно-цифровой подписи для подписания документа от имени другого лица, не осведомленного об этом, при этом ни форма, ни содержание документа не являются поддельными[4].

---

[1] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Булгакова В. Р. Подделка или оборот поддельного электронного сертификата о вакцинации от COVID-19: проблемы законодательной регламентации и правоприменения // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3 (92). С. 83—92.

[4] Коваленко Т. М. Электронный документ: понятие, признаки и способы его защиты от подделки // Актуальные вопросы права, экономики и управления : сборник статей XXIII Международной научно-практической конференции (Пенза, 10 декабря 2019 года). В 2 ч. Ч. 2. 2019. С. 173—176.

Диспозиция ст. 327 УК РФ предусматривает альтернативные действия, которые признаются преступными. В научной литературе существуют различные подходы к трактовке некоторых из названых действий в отношении электронных документов. Преступность подделки и использования электронного закреплены в позиции Верховного Суда и не вызывают вопросов, но в отношении иных действий существуют различные точки зрения. Согласно одной из них, другие альтернативные действия (например, приобретение, сбыт) в отношении электронных документов совершаться не могут[1]. Она базируется на том, что, поскольку форма предоставления таких документов электронная, физически их нельзя приобрести либо сбыть.

Действительно, фактически приобрести или сбыть электронный документ невозможно, но, если лицо оказывает услуги по оформлению документов в электронной форме и отправляет их третьим лицам, юридически данные действия могут быть рассмотрены как сбыт, соответственно, вторая сторона будет нести ответственность за приобретение такого документа. Представляется, что в отношении электронного документа не может быть совершена перевозка, так как без электронно-вычислительных машин и иной техники документ не может быть представлен. Лицо может перевозить компьютер или иные материальные носители, где он хранится, но перевозка непосредственно самих документов невозможна.

В судебной практике существуют следующие проблемы квалификации подложных электронных документов.

Первой является проблема определения предмета преступления. Для квалификации необходимо в первую очередь решить, является ли то, что подделано лицом, документом, и если да, то относится ли данный электронный документ к официальным или нет. Следует разграничивать документы с иными предметами подделки, например, с платежными поручениями. Можно

[1] Стяжкина С. А. Электронный документ как предмет уголовно-правовой охраны // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 1. С. 178—184.

встретить примеры, когда лицо, пользуясь своим служебным положением, оформляет поддельные платежные поручения с завышенными данными о заработной плате и иных выплатах сотрудникам с целью хищения денежных средств, и деньги, превышающие тот размер, который причитается сотрудникам, остаются на счетах лица, их похитившего.

Например, приговором Троицкого городского суда Челябинской области Н. была осуждена за мошенничество, выразившееся в том, что она неоднократно оформляла поддельные реестры зачисления денежных средств и платежные поручения, а суммы, превышающие размер выплат, положенных сотрудникам, поступали на ее счет как лица, занимающего должность бухгалтера, которыми впоследствии она распоряжалась по своему усмотрению[1].

В данном случае в действиях Н., помимо хищения, содержится состав преступления, предусмотренного ст. 187 УК РФ (незаконный оборот средств платежа), так как подделка платежных поручений преследовала цель неправомерного осуществления перевода денежных средств. При подобных обстоятельствах необходимо вменять данный состав по совокупности с хищением[2].

Несмотря на то, что были подделаны электронные документы, ст. 327 УК РФ в данном случае мы вменить не можем, потому что предметом преступления являлись средства платежа, и для них есть специальная статья в УК РФ.

Для квалификации имеет значение, является ли поддельный документ официальным или нет, так как в зависимости от этого предусмотрена дифференциация уголовной ответственности.

Примером подделки официального электронного документа является Постановление Пограничного районного суда Приморского края, где было пре-

[1] Приговор Троицкого городского суда Челябинской области от 11 февраля 2020 г. по делу № 1-59/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 19.10.2023).

[2] О судебной практике по делам о мошенничестве, присвоении и растрате : Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

кращено уголовное дело на основании ст. 25 УПК РФ по признакам преступлений, предусмотренных ст. 159 УК РФ и ст.327 УК РФ за несколько эпизодов. И., занимающая должность специалиста по кадрам в воинской части, при помощи персонального компьютера внесла изменения в электронный документ проекта приказа командира воинской части, завысив в два раза размер выплат, которые были положены ее знакомой с целью обогащения последней.

Суд указал, что предметом подделки был электронный официальный документ, так как в той части, где приказами устанавливаются оклады денежного содержания, они являются официальным документом по признаку предоставления права, в частности на получение денежного содержания[1]. В данной ситуации виновная совершила и хищение денежных средств, и подделку официального документа, который сама подделала, и квалификация по совокупности преступлений является верной. Если же лицо составляет подложный электронный документ, который не является официальным, с целью хищения денежных средств, дополнительное вменение ст.327 УК РФ не требуется, так как за подделку неофициального документа уголовной ответственности не предусмотрено.

Например, гражданско-правовые договоры официальными документами не являются[2], и судебная практика стоит на этой позиции. Так, в приговоре Батайского городского суда Ростовской области указывалось, что М., являясь администратором салона связи, обладая возможностью доступа к своему рабочему персональному компьютеру, используя известный ей ключ электронного доступа к системе, оформила фиктивный кредитный договор на сумму 37 тысяч рублей на лицо, не осведомленное о ее преступных намерениях.

---

[1] Постановление Пограничного районного суда Приморского края от 28 мая 2020 г. по делу № 1-41/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 19.10.2023).

[2] О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных статьями 324—327.1 Уголовного кодекса Российской Федерации : Постановление Пленума Верховного Суда Российской Федерации от 17 декабря 2020 г. № 43. Доступ из справ.-правовой системы «КонсультантПлюс».

На деньги, перечисленные в качестве кредита, М. купила себе мобильный телефон. Приговором суда была осуждена по ч. 3 ст. 159 УК РФ за мошенничество, и дополнительно ст. 327 УК РФ вменена не была[1].

Существует проблема квалификации действий лица, которое грубо подделало официальный электронный документ и выдало его за настоящий лицам, обратившимся к нему за услугой по оформлению документов. Судебная практика противоречива, и при похожих обстоятельствах в одном случае суд квалифицировал действия лица только по ст. 159 УК РФ как мошенничество, а в другом – по совокупности преступлений, предусмотренных ст. 159 УК РФ и ст. 327 УК РФ, как мошенничество и подделка официального документа. В обоих случаях речь шла о незаконной выдаче полиса ОСАГО. Стоит отметить, что полис ОСАГО является официальным документом[2], и существуют правила его выдачи как официального документа. После уплаты страховщиком денежных средств полис ОСАГО, подписанный усиленной квалифицированной электронной подписью страховщика, направляется по указанному им адресу электронной почты и размещается в личном кабинете страхователя (ст.15 Федерального закона «Об обязательном страховании гражданской ответственности владельцев транспортных средств»).

Так, в постановлении Бабаевского районного суда Вологодской области указано, что лицо оказало потерпевшему «услугу оформления полиса ОСАГО», сбыв ему поддельный электронный документ, и суд квалифицировал действия по совокупности ст. 159 УК РФ и ст. 327 УК РФ[3].

---

[1] Приговор Батайского городского суда Ростовской области от 29 января 2020 г. по делу № 1-37/2020 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 19.10.2023).

[2] Верховный Суд Российской Федерации в определении Судебной коллегии по уголовным делам от 25 декабря 2008 г. № 49-Д08-106, указал, что полис ОСАГО является важным личным документом, соответственно, тем более он является официальным документом, так как важный личный – это вид официальных документов.

[3] Постановление Бабаевского районного суда Вологодской области от 22 января 2020 г. по делу № 1-215/2019 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 19.10.2023).

При аналогичных условиях в апелляционном постановлении Тюменского областного суда суд посчитал, что осужденная виновна только в мошенничестве в следующей ситуации. А., выдавая себя за сотрудника страховой компании, которым в действительности не была, сообщала потерпевшим, желающим приобрести страховой полис ОСАГО, о намерении оказать им услуги по оформлению указанного полиса. Не зная о преступных намерениях, потерпевшие передавали ей свои документы и платили деньги за оказываемые услуги.

У А. на ее персональном компьютере были в распоряжении электронные документы в виде страхового полиса ОСАГО различных страховых компаний, где с помощью неустановленной программы она удаляла из электронных страховых полисов информацию о прежних владельцах, внося вместо этого данные потерпевших, изготовив таким образом поддельные полисы, она передавала их потерпевшим.

В данном случае следует обратить внимание на следующий вывод. По мнению суда, здесь не будет ст. 327 УК РФ, так как «при помощи этих полисов нельзя было реализовать право на возмещение убытков и ущерба при повреждениях автомобилей и авариях, поскольку их подделка была заведомо очевидна для представителей страховых организаций»[1].

Таким образом, имела место грубая подделка, и возникает вопрос, было ли данное деяние направлено против порядка управления или только против отношений собственности, так как лица, заплатив деньги за полис ОСАГО, не могут воспользоваться правами, которые он должен предоставлять. Единого мнения по этому поводу нет, и вопрос является дискуссионным, но точка зрения, изложенная во втором постановлении, представляется более правильной.

Она базируется на аналогии в толковании с похожей ситуацией, рассмотренной при квалификации преступлений в сфере оборота фальшивых денег.

[1] Апелляционное постановление Тюменского областного суда Тюменской области от 25 февраля 2020 г. по делу № 1-443/2019 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 19.10.2023).

В Постановлении Пленума Верховного Суда Российской Федерации «О судебной практике по делам об изготовлении или сбыте поддельных денег или ценных бумаг» говорится, что в тех случаях, когда явное несоответствие фальшивой купюры подлинной, исключающее ее участие в денежном обращении, свидетельствует о направленности умысла виновного на грубый обман ограниченного числа лиц, такие действия могут быть квалифицированы как мошенничество[1]. В приведенном выше постановлении Тюменский областной суд, по-видимому, как раз проводит аналогию в толковании с указанным положением из Пленума.

Исходя из этого, можно сделать вывод, что, если имела место грубая подделка официального документа, направленная на обман ограниченного числа лиц, стоит согласиться с тем, что лицо, подделавшее такой документ, будет нести ответственность только за мошенничество. Аргументом в пользу этой позиции является то обстоятельство, что предметом ст. 327 УК РФ является порядок управления, и если указанный поддельный документ не посягает на порядок управления, а является способом хищения денег посредством обмана лиц, не разбирающихся в том, каким образом должен быть оформлен документ, то оснований для квалификации действий по ст. 327 УК РФ не имеется.

Поскольку при подделке электронного документа используется электронная техника, встает вопрос о квалификации действий по совокупности с преступлениями в сфере компьютерной информации.

Есть точка зрения о том, что всегда при совершении неправомерных действий с электронными документами нужно дополнительно вменять ст. 272 УК РФ, потому что преступник при внесении изменений в компьютерную информацию, являющуюся официальным документом, посягает одновременно на два объекта – порядок управления и правоотношения в сфере компьютерной информации. В рассматриваемой ситуации информация, которая

[1] О судебной практике по делам об изготовлении или сбыте поддельных денег или ценных бумаг : Постановление Пленума Верховного Суда Российской Федерации от 28 апреля 1994 г. № 2. Доступ из справ.-правовой системы «КонсультантПлюс».

подвергается искажению, имеет две составляющие – это форма ее представления и содержание[1]. Следует частично согласиться с указанной точкой зрения, но при этом отметить, что мы не можем вменить ст. 272 УК РФ, если не будет установлен неправомерный доступ к этой компьютерной информации.

Если, например, лицо осуществляет незаконные действия с электронными документами со своего личного компьютера, данного состава не будет, так как доступ лица к своему собственному компьютеру или иному гаджету является правомерным, и лицо вправе самостоятельно пользоваться и распоряжаться им по своему усмотрению.

В настоящее время как в доктрине, так и в практике преобладающей является позиция, что неправомерным доступом к компьютерной информации признается не только «классический» неправомерный доступ, когда лицо не имело право работать или иным образом знакомиться с этой информацией, но и если лицом, которое было допущено к этой информации, например, в силу занимаемой должности, был нарушен порядок работы с ней, что повлекло ее незаконное копирование, уничтожение, блокирование или модификацию[2]. В рассмотренных выше приговорах следует обратить внимание на то, каким образом лицо оформляло подложные электронные документы. Если документ был подделан с личного компьютера, то квалифицировать дополнительно по ст. 272 УК РФ не нужно, а если лицо это сделало с рабочего компьютера, нарушив порядок работы с компьютерной информацией, данный состав преступления присутствует.

В качестве одного из вариантов разрешения этой проблемы предлагается отнести электронные официальные документы к критической информационной инфраструктуре и квалифицировать незаконные действия с ними по

[1] Стяжкина С. А. Электронный документ как предмет уголовно-правовой охраны // Вестник Удмуртского университета. Серия Экономика и право. 2022. Т. 32, № 1. С. 178—184.

[2] Щепельков В. Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6 (154). С. 70—79.

ст. 274.1 УК РФ (неправомерное воздействие на критическую информационную инфраструктуру)[1].

Следует не согласиться с данной позицией по следующим причинам. В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации»[2] говорится, что к критической информационной инфраструктуре относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, химической промышленности и т. д.

Соответственно, можно сделать вывод, что речь идет об объектах, имеющих крайне важное значение в обеспечении жизненно важных интересов государства, воздействие на которые приведет к значительным негативным последствиям для национальной безопасности в политической, экономической, экологической и других сферах. Например, по этой статье необходимо квалифицировать DDoS-атаки в отношении таких объектов как атомная электростанция, военный объект и т. п. Подделка лицом электронного документа не сопоставима по степени общественной опасности со ст. 274.1 УК РФ, которая относится к категории тяжких преступлений, что говорит о значительно более серьезном характере деяния. Если встать на эту позицию, то подделка бумажного документа будет являться преступлением небольшой тяжести, а подделка электронного документа — тяжким преступлением, что не соответствует принципу справедливости.

Таким образом, можно сделать вывод, что в настоящее время нет единообразия в судебной практике в вопросах квалификации преступлений, касающихся электронных документов. В законодательстве уже в ряде сфер бумажные документы приравнены к электронным, и должно быть единство,

[1] Стяжкина С. А. Указ. соч.

[2] О безопасности критической информационной инфраструктуры в Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

связанное с квалификацией альтернативных действий, совершаемых в отношении электронных документов.

Ответственность за подделку бумажного и электронного документа по ст. 327 УК РФ должна быть равной, но при наличии признаков преступления, предусмотренного за неправомерный доступ к компьютерной информации, также необходимо вменять по совокупности ст. 272 УК РФ, поскольку также причиняется вред данному объекту. В соответствии с действующим законодательством к критически важной информационной инфраструктуре электронные документы отнести нельзя, так как ст. 274.1 УК РФ характеризуется значительно большей степенью общественной опасности, предусматривает более высокую санкцию по сравнению с подделкой документа и влечет ответственность за другой характер деяния, когда осуществляются информационные атаки на объекты, обеспечивающие ключевые интересы общества и государства.

УДК 343

Н. М. СОЛОМАХИН,
Р. М. ЯКОВЛЕВ[1]

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

В наши дни, в век информационных технологий невозможно обособить свою жизнь относительно использования информационно-телекоммуникационных технологий, так как их использование пронзает широкий спектр общественных отношений, а интернет, как элемент системы информационно-телекоммуникационных технологий на сегодняшний день используют на регулярной основе 62,5 % мирового сообщества[2].

[1] Научный руководитель — ФЕДЫШИНА Полина Викторовна, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации.

[2] Global Digital 2022: вышел ежегодный отчет об интернете и социальных сетях — главные цифры. URL: https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472.html (дата обращения: 02.11.2023).

Упомянутый ранее термин включает в себя совокупность технологий необходимых для работы с информацией, которая, в свою очередь, является одним из ценнейших ресурсов.

Использование информационно-телекоммуникационных технологий значительно упрощает ее производство, распространение и обработку, что находит отражение в посягательстве на устойчивые общественные отношения, охраняемые уголовным законодательством Российской Федерации.

Однако, для правовой системы данное явление до 1994 года не регламентировалось законодательно. Обратить внимание на данный пробел в законодательстве способствовал прецедент в виде дела «Хакера № 1».

Преступник взломал крупнейший американский банк и похитил несколько миллионов долларов со счетов клиентов. На территории РФ законодательно были не урегулированы такого рода преступления, в связи с чем привлечение гражданина к уголовной ответственности не представлялось возможным.

Прежде, чем рассматривать явление информационно-телекоммуникационных технологий, в контексте средства совершения преступления, необходимо обратиться к общей теории уголовного права и отграничить средство от смежных понятий, таких как орудие и способ совершения преступления.

Средство преступления является одним из признаков объективной стороны, которая в свою очередь вступает элементом состава преступления.

Отличительной чертой обязательных признаков состава преступления выступает тот факт, что отсутствие как минимум одного из них исключает преступность деяния.

Факультативными (необязательными) являются те признаки, отсутствие которых в составе не является основанием для исключения состава преступления в деянии лица. Главной их функцией является характеристика элементов состава преступления, что помогает учитывать обстоятельства дела при его квалификации и вынесения санкции правоприменителем. Кроме того,

свойство необязательности влечет наличие таких признаков не во всех составах преступлений.

Под способом понимается определенная форма выражения деяния, что законодатель включил в содержание УК РФ (пример: убийство общеопасным способом). Средством выступает то, что позволяет совершить какое-либо общественно-опасное деяние или покуситься на определенные общественные отношения, в данном случае на жизнь в первую очередь[1].

В свою очередь, при выполнении объективной стороны используется орудие, то есть, при реализации деяния и непосредственном совершении преступления (например, ст. 209 УК РФ предусматривает вооружение группы лиц).

Следовательно, УК РФ предусматривает возможность определения средства преступления, как факультативного признака объективной стороны, придавая значение обязательного, образующего состав признака.

Выполнение объективной стороны преступления по статье 159.3 УК РФ возможно только при использовании электронных средств платежа (банковской картой через терминал) и никак иначе.

В данном случае средство совершения преступления является обязательным признаком объективной стороны и при его нарушении объективная сторона будет носить признаки преступления, предусмотренного иной статьей УК РФ.

В контексте изучаемого вопроса, важно сказать о двоякости понятия «средство преступления»[2]. Одно понимание включает в себя все то, что помогает достичь поставленной цели. Второй подход сужает средство преступления до предметов материального мира, которые субъект использует при совершении противоправного посягательства и воздействия на объект.

---

[1] Резник А. А. Понятие средства совершения преступления и его виды // Инновационная наука. 2020. № 5-1. С. 68—70.

[2] Малинин В. Б., Парфенов А. Ф. Объективная сторона преступления. СПб., 2004. С. 218.

Наиболее правильным представляется первый поход, так как в ином случае вопрос соотношения информационно-телекоммуникационных технологий и средства преступления не позволял отнести данное понятие в полном объеме к средствам совершения преступления. В таком случае, правовой интерес будет вызывать скорее компьютерное оборудование, мультимедийные средства, а не сеть «Интернет», которая является неотъемлемой частью данного понятия.

Общая часть Уголовного кодекса Российской Федерации выделяет отдельной статьей перечень обстоятельств, которые ужесточают последующую санкцию, применяемую к правонарушителю. Примечательно, что данный список является исчерпывающим. Это говорит о невозможности правоприменителя пополнить его по своему усмотрению, основываясь на обстоятельствах конкретно рассматриваемого дела.

Аксиомой любой правовой системы является то, что преступность всегда развивается быстрее законодательных норм, призванных регулировать общественные отношения, целостность которых нарушается посредством оказания на них влияния. В виду данных обстоятельств, представляется необходимым говорить о внесении информационно-телекоммуникационных технологий, как средства совершения преступления в ряд отягчающих обстоятельств, предусмотренных ст. 63 УК РФ.

Основанием для закрепления данного обстоятельства в общей части является повышенная степень общественной опасности, относительно аналогично совершаемого посягательства без использования технологий.

Это объясняется массовостью и публичностью, которые обусловлены широкой распространенностью информационно-телекоммуникационных технологий в современном обществе. Со временем количество преступлений возрастет в абсолютном значении, что сделает посягательство на общественные отношения посредством использования информационно-телекоммуникационных технологий более массовым явлением.

Кроме того, важно говорить об анонимности преступника при совершении деяния. Она достигается через использование технологий, маскирующих IP-адрес пользователя, через который процесс деанонимизации злоумышленника правоохранительными органами значительно упрощается.

При сохранении конфиденциальности субъекта правонарушения, компетентными органами будет осложнен процесс задержания и привлечения к уголовной ответственности лица. Это в свою очередь крайне негативно может сказаться на состоянии работы правоохранительных органов, что снижает эффективность их работы по восстановлению законности, охране общественных отношений и привлечении виновных к ответственности.

В настоящее время наиболее остро и актуально стоит проблема использования информационно-телекоммуникационных технологий, а конкретно сети «Интернет» в легализации недобросовестных и «подозрительных» доходов.

В данный момент в среде злоумышленников преобладает следующая форма отмывания денежных средств: продажа имущества, не имеющего материальной формы, следовательно, не существующего в реальности.

Злоумышленник генерирует неопределенное количество аккаунтов на сайтах по продажи товаров с нескольких IP-адресов, что позволяет тому оставаться неизвестным. Далее происходит выставление на сайте различных товаров, фактическим приобретателем которых выступает сам преступник. При этом не существует самого товара. Скупка товаров происходит путем сбыта той денежной массы, которую необходимо легализовать.

Примечательны также следующие технические моменты: правонарушитель осуществляет перевод денежных средств в электронную валюту на заранее созданные фейковые аккаунты электронных денежных систем, происходит перевод денег с этих аккаунтов на электронные кошельки якобы различных покупателей, после чего преступник, осуществляя действия от имени ложного покупателя, совершает приобретение несуществующего товара.

Подтверждением легальности полученного дохода может быть выписка из истории покупок сайта или иные документы, подтверждающие правомерность полученного дохода. Таким образом, злоумышленник осуществляет ряд умышленных действий, представляющих в своей совокупности состав преступления, определенного ст. 174 УК РФ[1].

К сожалению, сеть «Интернет» стала катализатором организации и перехода торговли наркотическими веществами в онлайн-пространство. В контексте данного исследования представляется важным раскрыть роль интернета в системе наркотрафика в Российской Федерации.

В намерении расширения рынка нелегальных психотропных и наркотических веществ участниками наркобизнеса используются ресурсы сети «Интернет». Это становится огромный проблемой для правоохранительных органов на этапе определения субъекта преступления, так как использование информационно-телекоммуникационных технологий позволяет продавцу сохранить свою анонимность и анонимность потенциального покупателя, что становится для многих решающим фактором приобщения к данной противоправной деятельности.

Наиболее популярным средством сбыта наркотиков в интернет-пространстве являются различные сайты и сообщества в социальных сетях, специализированные на этом. Огромной проблемой является регистрация таковых на иностранных серверах с использованием иностранных доменов, что осложняет определение субъекта преступления и мешает полному пресечению деятельности интернет-ресурсов[2].

По вопросу использования информационно-телекоммуникационных технологий в сфере оборота нелегальных наркотиков, существует множество судебной практики.

---

[1] Киданова Н. Л Актуальные проблемы современности – Экономические преступления, совершаемые в киберпространстве // Вестник Белгородского юридического института МВД России. 2018. № 2. С. 26—29.

[2] Дикарев В. Г. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть «Интернет» // Вестник Московского университета МВД России. 2018. № 4. С. 147—152.

Так, например, субъект совершил покушение на незаконный сбыт наркотических средств в крупном размере. Позднее, при даче показаний субъект сообщил, что по совету знакомого он нашел интернет-портал, осуществляющий сбыт наркотиков. Связавшись с администратором, тот изъявил желание осуществлять курьерскую работу. Субъект отметил, что общение и координирование его деятельности руководством осуществлялось через упомянутый выше сайт.

Неустановленными остались личность дилера, администратора и куратора, в то время как известный субъект был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ[1].

Таким образом, мы можем говорить о высокой роли информационно телекоммуникационных технологий, как средства совершения преступления, предоставляющего правонарушителю совокупность возможностей, позволяющих лицу оставаться неизвестным, эффективно действовать в совершении преступлений. Из первого пункта вытекает также и то, что исполнитель остается безнаказанным, так как в таком случае из структуры состава преступления выпадает один из элементов, а именно субъект, что делает невозможным дальнейшее осуществление мер правосудия по отношению к нему.

Кроме того, информационно-телекоммуникационные технологии предоставляет преступнику достаточно широкий перечень общественных отношений, процесс посягательства на которые с их использованием существенно упрощается. Использование информационно-телекоммуникационных технологий, как средства совершения преступления позволяет преступнику оставаться анонимным, что усложняет работу аппарата правоохранительных органов.

Эти и другие причины являются основанием говорить о необходимости пополнения перечня ст. 63 УК РФ отягчающим обстоятельством, предусматривающим использование информационно-телекоммуникационных технологий при совершении преступления.

---

[1] Приговор от 31 августа 2017 г. по делу № 1-653/2017 // Судебные и нормативные акты РФ : сайт. URL: https://sudact.ru (дата обращения: 18.11.2023).

УДК 343

Э. СПИРИДОНОВА,
С. А. ШУКУРОВА[1]

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО В СОВЕРШЕНИЕ ДЕЙСТВИЙ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ НЕСОВЕРШЕННОЛЕТНЕГО, С ПОМОЩЬЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)

В 2017 году Федеральным законом от 07.06.2017 № 120-ФЗ Уголовный кодекс Российской Федерации был дополнен статьей 151.2, которая именуется «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего».

Состав этого преступления звучит следующим образом: склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, путем уговоров, предложений, обещаний, обмана, угроз или иным способом, совершенное лицом, достигшим восемнадцатилетнего возраста, при отсутствии признаков склонения к совершению самоубийства, вовлечения несовершеннолетнего в совершение преступления или в совершение антиобщественных действий.

Как отмечалось в пояснительной записке к законопроекту, принимаемый состав преступления направлен на обеспечение защиты детей от информации, побуждающей к опасному для жизни поведению, что является одной из задач национальной безопасности[2].

Появление нового состава преступления, наряду с внесением дополнений в ст.110 УК РФ, дополнением статьями 110.1, 110.2 УК РФ, стало ответной мерой распространившемуся в 2015 и 2016 гг. явлению так называемых «групп смерти», когда дети в социальных сетях наталкивались на различные группы

[1] Научный руководитель — ФИЛАТОВА Надежда Юрьевна, старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия.

[2] Система обеспечения законодательной деятельности: сайт. URL: https://sozd.duma.gov.ru/bill/118634-7 (дата обращения: 16.11.2023).

и сообщества деструктивного характера. Наиболее ярким примером является «Игра» «Синий кит», прохождение каждого из этапов которой сопровождался физическим (самоувечья) и психическим (просмотр фильмов ужасов, снафф-видео и др.) насилием, конечным итогом игры было самоубийство ребенка.

Анализ статистики, представленной на сайте Судебного департамента при Верховном Суде Российской Федерации, демонстрирует крайне редкое применение рассматриваемой нормы при квалификации деяний на практике[1].

За 5 лет было осуждено всего лишь два человека. На наш взгляд, указанная норма скорее выполняет превентивную функцию. И основная ее превенция направлена именно на информационную безопасность.

Так, действенной мерой предупреждения совершения таких преступлений признается выявление и блокировка Интернет-ресурсов, содержащих сведения, направленные на возбуждение желания у несовершеннолетнего совершить какие-то действия, представляющие опасность для его жизни.

Например, относительно недавно достаточно распространенным среди подростков считался «зацепинг», то есть проезд на крышах вагонов, подножках, между вагонами поездов. По словам начальника Главного управления на транспорте (ГУТ) МВД России Калинкина О.В. ранее зацеперы объединялись с помощью сети «Интернет» в группы, где пропагандировали этот опасный вид «развлечения». Роскомнадзор начал блокировать такие сайты (по Северо-Западному федеральному округу проведена работа по блокировке более 5 тыс. таких интернет-ресурсов)[2].

Стоит отметить, что одним из квалифицирующих признаков является склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, именно с помощью сети «Интернет». Такой способ совершения преступления представляет повышенную общественную

[1] Судебный департамент при Верховном Суде Российской Федерации : офиц. сайт. URL: https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения: 16.11.2023).

[2] В МВД России сообщили о сокращении числа зацеперов за последние годы. https://tass.ru/obschestvo/17146773 (дата обращения: 16.11.2023).

опасность, поскольку позволяет виновному лицу склонить или вовлечь неограниченное (неперсонифицированное) количество несовершеннолетних, что повышает число жертв в разы.

Согласно статистическому отчету по цифровым технологиям, всего в мире в октябре 2023 года 5,3 миллиарда человек являются пользователями Интернета (при этом, по данным ООН в октябре на Земле проживало 8,06 миллиардов человек). Таким образом, 65,7% населения мира используют в своей повседневной жизни Интернет-ресурсы. При этом, число активных пользователей социальных сетей выросло до 4,95 миллиарда человек (61,4%).

Важным является и тот факт, что это число растет с каждым днем. Так, за июль-сентябрь количество активных пользователей увеличилось на 1,6%, и к началу октября 2023 года увеличилось аж на 76 миллионов человек (в среднем, за 90 дней распространение социальных сетей осуществлялось со скоростью 9,6 пользователей в секунду)[1].

Современные технологии предоставляют неограниченные возможности для общения, получения информации и реализации виртуальной активности в различных формах. В то же время, они представляют собой и опасность для пользователей.

Специалисты выделяют факторы, являющиеся причинами неконтролируемости данной среды:

анонимность, состоящая в возможности скрыть свою личность и действовать инкогнито в интернете, что в свою очередь создает благоприятную среду для злоупотреблений и воздействия на уязвимые личности несовершеннолетних;

отсутствие контроля родителей и образовательных учреждений, заключающееся в недостаточном внимании со стороны родителей и образовательных учреждений к онлайн-активности детей, что создает отличную почву для организации противоправной деятельности;

[1] DIGITAL 2023 OCTOBER GLOBAL STATSHOT REPORT. [Электронный ресурс]: URL: https://datareportal.com/reports/digital-2023-october-global-statshot (дата обращения: 16.11.2023).

недостаток навыков цифровой грамотности и критического мышления, что делает детей более уязвимыми перед негативным влиянием онлайн-среды.

Как справедливо отмечает К. А. Чернышева: «Несовершеннолетний, погрузившись полностью в сеть «Интернет», не видит границы допустимого. Если вовремя не приняты меры и ребенку не оказана помощь в том, чтобы он взглянул иначе на ту или иную ситуацию, это может привести к суициду»[1].

Однако, дискуссионным является вопрос о возможности привлекать к уголовной ответственности по рассматриваемому составу преступления за призывы и агитации, обращенные к неопределенно широкому кругу лиц, в том числе несовершеннолетних.

Некоторые авторы указывают на отсутствие признака склонения или вовлечения в данном случае. Коровин Е.П. подчеркивает, что вовлечение должно быть направлено на одного или несколько, но конкретных несовершеннолетних, а публичные призывы не обращены персонально к кому-либо, охватывают, как правило, неопределенно широкий круг лиц и носят общий характер[2].

К аналогичному выводу по смежному составу приходит и Н.Е. Крылова, указывая, что склонение лица к самоубийству при отсутствии «конкретной жертвы» с позиций уголовного права является нонсенсом[3].

Судебная практика идет по другому пути. Одним из примеров, демонстрирующих опасность совершения рассматриваемого преступления, являются дела о призыве несовершеннолетних участвовать в несанкционированных митингах.

В рамках работы по этому направлению, в 2021 году было возбуждено уголовное дело в отношении А. Навального, Л. Волкова в вязи с призывами, размещенными в социальных сетях и обращенными к неопределенно широ-

[1] Чернышева К. А. Вовлечение несовершеннолетних в антиобщественную деятельность в сети «Интернет» // Закон и право. 2021. № 9. С. 218—221.

[2] Коровин Е. П. Некоторые теоретические и практические проблемы квалификации преступления, предусмотренного ст. 151.2 УК РФ // Уголовное право. 2018. № 6. С. 56—65.

[3] Крылова Н. Е. Ответственность за доведение до самоубийства и причастность к самоубийству другого лица по уголовному праву Российской Федерации: оценка законодательных новелл // Уголовное право. 2018. № 1. С. 81.

кому кругу лиц (подписчиками группы являлись, в том числе, несовершеннолетние), участвовать в митингах, официально запрещенных в связи с пандемией короновируса[1].

Кроме того, опасность участия несовершеннолетних в несанкционированных митингах состоит также и в том, что в ходе проведения таких мероприятий его участники могут получить травмы и ранения, если митинг перерастет в массовые беспорядки или если будут применены специальные средства, слезоточивый газ и т. п.

Таким образом, мы приходим к выводу о том, что вовлечение несовершеннолетних в совершения действий, опасных для них самих с помощью сети «Интернет» действительно представляет собой повышенную опасность и требует использования методов уголовной репрессии.

В случае выявления информации, направленной на склонение несовершеннолетних к совершению таких действия, помимо блокировки таких Интернет-ресурсов, на наш взгляд, должен решаться вопрос о возбуждении уголовных дел по ч. 3 ст. 30 и п. «в» ч. 2 ст. 151.2 УК РФ.

УДК 343

К. Б. ТАЙМАЗОВ[2]

ВИКТИМОЛОГИЧЕСКИЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ СОВРЕМЕННОГО РОССИЙСКОГО ОБЩЕСТВА

В современный период все мировое сообщество переживает четвертую технологическую революцию, с которой ассоциируются внедрение цифровых технологий и усиливающаяся цифровизация пространства. Параллельно с этими процессами стремительно меняется общественный уклад, государство, бизнес и повседневная жизнь каждого человека.

[1] После призывов к несовершеннолетним принять участие в несанкционированных акциях в поддержку Навального возбуждено уголовное дело. URL: https://www. 1tv.ru/news/2021-01-23/400391-posle_prizyvov_k_nesovershennoletnim_prinyat_uchastie_v_nesanktsionirovannyh_aktsiyah_v_podderzhku_navalnogo_vozbuzhdeno_ugolovnoe_delo (дата обращения: 16.11.2023).

[2] Научный руководитель — РАДЖАБОВ Шамиль Раджабович, доцент кафедры уголовного права и процесса Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук.

Сегодня цифровизация проникла во все сферы человеческой жизнедеятельности, вышла на глобальный уровень, и охватила не только всю планету в целом, но и все мировое пространство, расположенное далеко за ее пределами (имеется в виду такая цифровизация пространства, куда смог «дотянуться» современный человек). Цифровыми технологиями широко охвачены: экономика и бизнес, образование, медицина, строительство, сельское хозяйство и т. д.

Мощный толчок процессам цифровизации общества дала пандемия, которая возникла в связи с коронавирусной инфекцией нового типа. В условиях работы и организации жизнедеятельности общества в удаленном режиме произошли дальнейшая интеллектуализация общества, диджитализация экономики, а также состоялся переход основной массы потребителей рынка, в том числе и сферы услуг в режим онлайн.

Старт процессу цифровизации дала начатая в 2018 г. в России программа «Цифровая экономика», которая преследует цель улучшить эффективность и конкурентоспособность не только российской экономики, но и социальной сферы и государственного управления в целом. По мнению отдельных экспертов, у цифровой экономики много преимуществ[1].

При этом цифровизацию не следует сводить только к электронным товарам и сервисы, которые осуществляются электронным бизнесом и электронной коммерцией, эксперты утверждают, что она открывает новые источники доходов и возможностей удаленной работы. В этой связи особенно актуализируются способности к самообразованию и овладению новейшими технологиями индивидами и в целом всего населения.

В условиях продолжающейся цифровизации настоятельной потребностью современных реалий становится поиск путей и способов обеспечения кибербезопасности всех и каждого, которые способны обеспечить баланс между прогрессом и защищенностью всех и каждого. Защищенность общества, госу-

[1] Ильченко А. Н., Ильченко К. В. Цифровая экономика как высшая ступень развития инфокоммуникационных технологий // Современные наукоемкие технологии. Региональное приложение. 2018. № 3 (55). С. 57.

дарства и индивидов в условиях цифровизации – межотраслевая проблема, которая лежит в плоскости различных областей знаний: конституционного (государственного) права, гражданского права, административного права, уголовного права, криминологии, а также виктимологии и ряде др.

А между тем внедрение цифровых технологий выявило дисбаланс между ее экономическими и техническими приоритетами с интересами общества в плане его безопасности и неприкосновенности частной жизни. Как нам представляется, внедрение цифровых технологий без контроля или при ненадлежащем контроле со стороны государства чревато множеством проблем и уязвимостей как для населения, так и самого государства, и общества в целом.

Встраивая микрочипы во все вещи, мы превращаем окружающий мир в абсолютную угрозу для нашей безопасности. Взломы и уязвимости, обнаруженные за последние несколько в социальных сетях и мессенджерах, показывают, насколько тяжело поддерживать цифровой контроль даже крупнейшим технологическим компаниям.

В роботизированном мире взломы будут угрожать не только личным данным, но и собственности, жизни и даже национальной безопасности. В частности, по данным «Лаборатории Касперского», 28% всех исследованных индустриальных предприятий мира столкнулись с целевыми хакерскими атаками, с начала 2019 года программами шифровальщиками было атаковано 174 муниципальных образования, что как минимум на 60% больше по сравнению с 2018 годом[1].

В центре виктимологических исследований любого феномена, в том числе цифровизации как неотъемлемого элемента современного общества лежит понятие жертвы преступления.

В теории виктимологии дискуссия по вопросу о понятии жертва не прекращаются по сей день, по этому поводу есть различные точки зрения, которые в своей основе укладываются в рамки широкого его понимания

[1] «Лаборатория Касперского» наблюдает рост числа атак шифровальщиков на органы городской администрации) // Kaspersky : сайт. URL: https://www.kaspersky.ru (дата обращения: 02.11.2023).

(Г.Й Шнайдер)[1] и узкого его значения (данным операциональным понятием пользуются большинство российских виктимологов).[2]

Среди преступлений в цифровой среде наибольшей виктимогенной выраженностью обладают различные виды мошенничества и банковские кражи.

В данном русле цифровизация может рассматриваться как один из факторов виктимизации населения. Так, недостаточная урегулированность и непродуманность решений в сфере новейших высоких технологий и их внедрения существенно увеличивают риски и уязвимости отдельных индивидов, населения, общества и государства. Уязвимость – виктимологическая категория, которая инициирует и сопровождает возможный сценарий причинения вреда личным и общественным интересам, государству в целом.

Риски и уязвимости, которые открываются при переходе экономики и государственного управления в «цифру», вполне сопоставимы с открывающимися возможностями.

Сегодня клонирование сайтов официальных ведомств становится привлекательным средством обмана доверчивых и добросовестных граждан, оно стало своеобразным трендом последних лет в информационной среде.

В информационное пространство вовлечены, как усматривается из изложенного, три основные группы участников: государство, бизнес и физические лица (индивиды).

В этой связи в основе виктимологических исследований цифровизации современного общества лежит широкое понимание жертвы преступления, которое было сформулировано Г.Й. Шнайдером, а пострадавшими от преступлений, обусловленных недостатками и издержками цифровизации могут оказаться как коллективные субъекты: государство, общество, нации, социальные группы, отдельные индивиды, а также вся информационная среда.

---

[1] Шнайдер Г. Й. Криминология / под ред. и с предисл. Л. О. Иванова. М., 1994.

[2] Вишневицкий К. В. Криминологическая характеристика и определение понятий «жертва преступления взаимоотношений» и «личность преступника»// Гуманитарные, социально-экономические и общественные науки. 2018. № 9. С. 73.

Безусловно, наибольший интерес с точки зрения жертвенности представляют отдельные индивиды, они являются основным источником информационных данных, при этом у них меньше всего возможностей осуществлять контроль за тем, как и в каких целях собирают и обрабатывают их данные.

Думается, что данный Регистр по своим признакам должен быть приравнен к объектам критической информационной инфраструктуры, сведения, которые содержатся в регистре в условиях цифровизации общества необходимо на законодательном уровне определить, как составляющие государственную тайну.

Фактором, повышающий виктимность и виктимизацию населения также является уязвимость объектов информационной инфраструктуры и информационных систем.

В основе детерминации уязвимости информационных систем, в том числе ЕФИР, лежат следующие факторы:

недостатки, пробелы и ошибки в их правовом регулировании;

издержки и недостатки в работе регулирующих и контролирующих органов;

ошибки, допущенные непосредственными разработчиками баз данных (к примеру, ошибки в настройках сервера, которые создают возможность для доступа сторонних специалистов и получения ими данных);

копирование недобросовестными и коррумпированными сотрудниками данных для последующей их продажи, либо извлечения выгод для себя.

В этой связи профилактика и предупреждение виктимизации населения в условиях цифровизации общества требует прежде всего обеспечения кибербезопасности, защиты от кибератак, предупреждение возможности утечки информации. В этих целях в Российской Федерации формируется и развивается законодательство в сфере защиты информационных систем и обеспечения их безопасности.

Таким образом, виктимологический аспект цифровизации – относительно новая частная проблема виктимологии. Дуализм данной проблемы выражается в том, что с одной стороны, цифровизация, рассматриваемая как процесс приводит к возникновению новых видов киберпреступлений, жертвы которых

в полной мере не изучены, наряду с этим она повышает уровень виктимности населения, а с другой стороны, цифровизация как совокупность информационных технологий и средств подвержена кибератакам и рискам утечки информации, и в этом значении может рассматриваться как жертва (неконкретное образование).

С целью обеспечения защищенности и безопасности жертв в условиях цифровизации современного общества необходимо создать новый федеральный орган — Агентство национального киберуправления, основными задачами которого, к примеру, будут: изучение угроз, консультирование потенциальных и реальных жертв, координация действий ответственных лиц и IT персонала на возможные кибератаки, взломы и т. д.

В заключение хочется подчеркнуть, что проблемы цифровизации современного российского общества имеют виктимологический аспект, повышают уровень виктимологической выраженности многих преступных посягательств, в том числе тех из них, которые считались наименее виктимными.

Предупреждение виктимизации требует не только формирования гибкого правового регулирования современной информационной инфраструктуры, но и создания механизмов, посредством которых можно обеспечить жесткий контроль за современной информационной инфраструктурой.

УДК 343

Г. В. ФРОЛЕНКОВ[1]

ИГРОВЫЕ ПРЕДМЕТЫ И ОПЕРАЦИИ С НИМИ — УГОЛОВНО-ПРАВОВОЙ АСПЕКТ

Сегодня одной из наиболее развивающихся цифровых продуктов выступают компьютерные игры, создание которых превратилось в крупную индустрию с одноименным названием. Капиталовложения одного из цифровых «гигантов» «Electronic Arts» и соответствует валовому внутреннему продукту

[1] Научный руководитель — ТЕРТЫЧНАЯ Илона Викторовна, доцент кафедры криминалистики Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент.

(ВВП) некоторых государств, например: «market cap» «Electronic Arts» составляет более 36 млрд долларов США[1], когда как подобная сумма составляется из сложения данного показателя Лесото (2,37 млрд долларов США), Зимбабве (32,42 млрд долларов США), Либерии (0,8 млрд долларов США)[2]. И подобных компаний на современном рынке достаточно большое количество.

Помимо исключительно цифровых показателей данные компании создают и совершенствуют современные технологии и формируют основу для внедрения собственных разработок в иные сферы деятельности, например, как 3D – моделирование, которое долгое время широко применяется в кинематографе, медицине, строительстве и т. п.

Однако существующая тенденция практически всегда позволяет сделать прогнозирующий вывод: сфера, в которой в обороте находятся весьма большие суммы, привлекает криминально ориентированный контингент, который ставит для себя задачей максимальный заработок в данной сфере, в том числе в обход законодательства. А «способствовать» данной категории может отсутствие нормативного закрепления отдельных вопросов, связанных с указанной сферой.

На сегодняшний день наибольшее распространение среди «геймеров» получили «онлайн-игры», отличительной особенностью которых является не прекращающийся процесс функционирования игры, постоянно совершенствующийся и создающий условия для постоянного привлечения внимания пользователя.

Отдельно стоит остановиться на практически повсеместно встречающихся игровых предметах, являющимися созданными разработчиками игры моделей персонажа, предмета, используемого им в ходе игрового процесса, обладающему стоимостью, выраженную во внутриигровой валюте либо реальных денежных средствах.

[1] Market capitalization of Electronic Arts (EA) // Global ranking : сайт. URL: https://companiesmarketcap.com/electronic-arts/marketcap/ (дата обращения: 25.11.2023).

[2] Statista : сайт. URL: https://www.statista.com/ (дата обращения: 25.11.2023).

Игровые компании получают прибыль за счет приобретения пользователями лицензионных копий своего продукта, а также продажи дополнительного материала, которыми могут выступать как раз указанные предметы. В условиях вложения настоящих денежных средств для приобретения игровых предметов можно выдвинуть тезис относительно включения их в категорию имущества в привычном его понимании.

В настоящий момент однозначный подход к понятию «виртуального имущества» не сформирован, однако, по мнению Рожковой М.А., «чаще всего к таковому относят нематериальные объекты, которые имеют экономическую ценность, полезны и могут быть использованы исключительно в виртуальном пространстве (игровое имущество, криптовалюта, виртуальные токены, доменные имена, виртуальное имущество в социальных сетях и др.)»[1].

Но в тоже время отнести указанные «цифровые предметы» к имуществу не представляется возможным. Дефиниция ст. 128 ГК РФ, устанавливающая перечень объектов гражданских прав, не включает рассматриваемые предметы в качестве таковых. Однако формально судом может быть осуществлена оценка в зависимости от представленных доказательств и материалов уголовного дела в целях последующего отнесения данных объектов к иному имуществу. К сожалению, в настоящий момент подобной практики не сформировано, и тезис является лишь предложением для правоприменителей.

Очередную сложность для однозначного отнесения игровых предметов к имуществу можно считать статус их нахождения у пользователя. Созданные цифровые объекты формально являются интеллектуальной собственностью компании-разработчика и предоставляются пользователю на время существования игры. В случае отключения игровых серверов, запрещения распространения игры и т.п. действий, правообладатель не будет нести ответственность перед владельцем игрового имущества. Пользователь потеряет все, что ему принадлежало без возможности компенсации затраченных средств.

[1] Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // Закон.ру : сайт. URL: https://zakon.ru (дата обращения: 25.11.2023).

В доказательство отнесения рассматриваемых предметов к имуществу можно продемонстрировать стоимость некоторых из них. Так, на бирже игровых предметов «CS GO Market», предмет из компьютерной игры «Counter-Strike 2» под наименованием «AWP Гунгнир (немного поношенное)» продается за сумму, свыше 1 млн. 120 тыс. рублей, предмет «Штык-нож M9 Волны (прямо с завода)» — свыше 1 млн рублей и т. д.[1].

Помимо достаточно высокой стоимости отдельных игровых предметов интернет-площадки предоставляют возможность осуществления операций с ними, таких как продажа, обмен, дарение. Торговая площадка онлайн-сервиса «Steam», предоставляет пользователю возможность владеть, пользоваться «игровым имуществом», находящимся в «инвентаре» у владельца аккаунта. Однако оплата товара и получение денежных средств происходит за счет внутреннего кошелька «Steam», откуда вывод денежных средств невозможен. В таком случае «на помощь» приходят сторонние сервисы, к примеру, как вышеуказанная площадка, «CS GO Market». В настоящее время подобных сервисов в сети «Интернет» находится огромное множество

Исходя из вышеперечисленного, возникают некоторые вопросы, касающиеся возможного использования указанных игровых предметов в преступных целях, и совершения преступных посягательств с целью неправомерного завладения последних. Согласно данному тезису, можно определить две основные группы преступлений, связанных с игровыми предметами: преступления, в которых цифровое имущество выступает в качестве предмета преступного посягательства, и преступления, в которых игровые предметы являются средством совершения уголовно-наказуемого деяния.

К первой можно отнести преступления, предусмотренные гл. 21 УК РФ, против собственности. Кража (ст. 158 УК РФ) применима в отношении игровых предметов исключительно в случае неправомерного доступа лица к аккаунту владельца имущества, и как следствие будет применяться в совокупности со ст. 272 УК РФ («неправомерный доступ к компьютерной информации»).

[1] Ыфегкшф Дшьшеув Ж сайтю ГКДЖ реезыЖ..ьфклуеюсыпщюсщь.кг. (дата обращенияЖ 25ю11ю2023)

Хищение рассматриваемых предметов возможно мошенническим путем (ст. 159 УК РФ). В представленной ситуации наиболее верно применять специальную норму ст. 159.6 УК РФ («мошенничество в сфере компьютерной информации»). В том числе игровые предметы могут выступать предметом преступного посягательства при квалификации вымогательства (ст. 163 УК РФ).

Вторая группа преступлений, характеризующаяся использованием игровых предметов в качестве средства совершения преступления, включает в себя преимущественно ряд преступлений коррупционной направленности. Являясь относительно не контролируемым и не отслеживаемым предметом, обладающим ценностью, причем, как было рассмотрено выше, весьма значительной, рассматриваемое имущество выступает «идеальным» предметом взятки. Указанные качества также способствуют использованию в целях легализации (отмывания) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ).

Относительная анонимность операций, их транснациональный и трансграничный характер позволяет использовать игровые предметы в целях финансирования террористической деятельности (ст. 205.1 УК РФ).

Подводя итог, необходимо сформулировать определенные выводы:

уголовно-правовая охрана игровых предметов возможно лишь в том случае, если последние будут признаны в качестве конкретного вида имущества. В том числе иного, согласно ст. 128 ГК РФ. В противном случае, можно утверждать об абсолютной «беззащитности» общественных отношений, связанных с оборотом игровых предметов в отечественном законодательстве;

использование игровых предметов возможно в качестве средства совершения преступления, создавая тем самым целую нишу, не регулируемую законодательством, для осуществления преступной деятельности.

ИНФОРМАЦИЯ ДЛЯ РОССИЙСКОГО ИНДЕКСА НАУЧНОГО ЦИТИРОВАНИЯ

АЙВАЗЯН Асмик Грандовна, помощник Волго-Донского транспортного прокурора Южной транспортной прокуратуры	**AYVAZYAN Hasmik G.** Assistant to the Volga-Don Transport Prosecutor of the Southern Transport Prosecutor's Office
УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ ЖИЗНИ, СВЯЗАННЫХ С САМОУБИЙСТВОМ ПОТЕРПЕВШЕГО, СОВЕРШЕННЫХ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ	**GENERAL CHARACTERISTICS OF CRIMES AGAINST LIFE RELATED TO THE SUICIDE OF THE VICTIM COMMITTED WITH THE HELP OF INFORMATION TECHNOLOGY**
В статье рассматривается уголовно-правовая и криминологическая характеристика преступлений против жизни, связанных с самоубийством потерпевшего, совершенных с помощью информационных технологий. Исследованы возможные причины такого социального явления, как суицид. Путем изучения судебной практики, сведений, опубликованных на официальных сайтах надзорных ведомств, а также информации, полученной из средств массовой информации, выделены наиболее популярные способы совершения анализируемых преступных деяний	The article examines the criminal law and criminological characteristics of crimes against life related to the suicide of the deceased, committed with the help of information technology. The possible causes of such a social phenomenon as suicide are investigated. By studying judicial practice, information published on the official websites of supervisory agencies, as well as information obtained from the mass media, the most popular ways of committing the analyzed criminal acts are highlighted.
Ключевые слова: преступления против жизни, доведение до самоубийства, склонение к самоубийству, содействие самоубийству, побуждение к совершению самоубийства, суицид	**Keywords:** crimes against life, incitement to suicide, inducement to suicide, assistance to suicide, inducement to commit suicide, suicide
АНТОНОВА Елена Юрьевна, декан юридического факультета Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, профессор	**ANTONOVA Elena Yurievna,** Dean of the Faculty of Law of the Far Eastern Law Institute (branch) of the University of prosecutor's office of the Russian Federation, Doctor of Science (Law), Professor
ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ЦИФРОВОМ ПРОСТРАНСТВЕ: ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ	**RESPONSIBILITY FOR CRIMES COMMITTED IN THE DIGITAL SPACE OR USING DIGITAL TECHNOLOGIES: ISSUES OF CRIMINAL LEGAL POLICY**
В статье рассматриваются отдельные вопросы уголовно-правовой политики в сфере противодействия преступлениям, совершаемым в цифровом пространстве или с	The article discusses certain issues of criminal law policy in the field of combating crimes committed in the digital space or using digital technologies. The need to comply with all the

использованием цифровых технологий. Отмечается необходимость соблюдения всех оснований криминализации деяний (изменения интенсивности пенализации) при принятии уголовно-политических решений в названной сфере. Обозначается, что не всегда при использовании цифровых технологий и площадок в процессе совершения преступлений увеличивается их степень общественной опасности. Поднимается вопрос о выработке единого понятийно-категориального аппарата.	grounds for the criminalization of acts (changes in the intensity of penalization) when making criminal and political decisions in the designated area is noted. It is indicated that the use of digital technologies and platforms in the process of committing crimes does not always increase their degree of public danger. The question is raised about the development of a unified conceptual-categorical apparatus.
Ключевые слова: уголовно-правовая политика, цифровое пространство, цифровые технологии, криминализация, общественная опасность деяний	**Keywords:** criminal law policy, digital space, digital technologies, criminalization, public danger of acts
АРТЕМЬЕВА Алёна Сергеевна, эксперт Экспертно-криминалистического центра ГУ МВД России по г. Санкт-Петербургу и Ленинградской области	**ARTEMYEVA Alyona Sergeevna,** expert of the Forensic Center of the Main Directorate of the Ministry of Internal Affairs of Russia for St. Petersburg and the Leningrad region
ВОПРОСЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПРЕДОСТАВЛЯЕМЫХ ПОЛЬЗОВАТЕЛЯМИ СЕТИ «ИНТЕРНЕТ»	**ISSUES OF PROTECTION OF BIOMETRIC PERSONAL DATA PROVIDED BY INTERNET USERS**
В статье рассматривается вопрос о необходимости комплексного подхода к обеспечению безопасности биометрических персональных данных на государственном уровне. Автором предлагается комплекс мер, затрагивающих не только техническую, но правовую и этическую стороны проблемы. Кроме того, в рамках выявления возможных направлений угроз при предоставлении, обработке, использовании и хранении биометрических персональных данных приводится прямо пропорциональная зависимость уровня национальной безопасности от степени защищенности таких данных.	The article discusses the need for an integrated approach to ensuring the security of biometric personal data at the state level. The author proposes a set of measures affecting not only the technical, but also the legal and ethical aspects of the problem. In addition, as part of the identification of possible threat areas in the provision, processing, use and storage of biometric personal data, a directly proportional dependence of the level of national security on the degree of protection of such data is provided.
Ключевые слова: биометрические персональные данные, идентификация, информационно-телекоммуникационные технологии, информационное общество, национальная безопасность	**Keywords:** biometric personal data, identification, information and telecommunication technologies, information society, national security
БАРАНЧИКОВА Марина Вячеславовна, заместитель начальника кафедры уголовного права, криминологии и психологии	**BARANCHIKOVA Marina Viacheslavovna,** Deputy Head of the Department of Criminal Law, Criminology and Psychology

Орловского юридического института Министерства внутренних дел Российской Федерации имени В. В. Лукьянова, кандидат юридических наук, доцент	of the Orel Law Institute of the Ministry of Internal Affairs of the Russian Federation named after V.V. Lukyanova, Candidate of Science (Law), Associate Professor
ТРАНСПОРТНЫЕ СРЕДСТВА КАК ПРЕДМЕТ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	**VEHICLES AS A SUBJECT OF FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS**
В статье раскрываются особенности мошенничества, совершаемого в отношении транспортных средств, анализируются способы, связанные с использованием информационно-телекоммуникационных сетей. С развитием современных технологий возникает необходимость оценки новых видов мошенничества, в числе которых совершение сделок купли-продажи через сеть «Интернет», безналичная оплата услуг, связанных с эксплуатацией транспортных средств.	The article reveals the features of fraud committed against vehicles, analyzes the methods associated with the use of information and telecommunication networks. With the development of modern technologies, there is a need to assess new types of fraud, including making purchase and sale transactions via the Internet, non-cash payment for services related to the operation of vehicles.
Ключевые слова: транспортные средства, мошенничество, информационно-телекоммуникационная сеть, онлайн-продажи, безналичный расчет, обман, использование транспортных средств, водитель	**Keywords:** vehicles, fraud, information and telecommunication network, online sales, cashless payment, deception, use of vehicles, driver
БАЧО Ирина Игоревна, старший следователь отдела по расследованию бандитизма, организованной преступной деятельности в сфере экономики и противодействия коррупции следственной части по расследованию организованной преступной деятельности следственного управления УМВД России по Псковской области	**BACHO Irina Igorevna,** Senior investigator of the Department for the investigation of banditry, organized criminal activity in the field of economics and anti-corruption of the investigative unit for the investigation of organized criminal activity of the Investigative Department of the Ministry of Internal Affairs of Russia in the Pskov region
ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБНАЛИЧИВАНИЕМ И ТРАНЗИТИРОВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	**SPECIAL ASPECTS OF INVESTIGATION OF CRIMES RELATED TO ILLEGAL CASHING AND TRANSIT OF FUNDS, COMMITTED WITH THE USE OF INFORMATION AND TELECOMMUNICATION NETWORKS**
В статье рассматриваются способы и схемы совершения незаконного обналичивания и транзитирования денежных средств, в основе которых лежит использование информационно-телекоммуникационных сетей.	The article considers ways and schemes of committing illegal cashing and transit of funds, which are based on the use of information and telecommunication networks. The article studied investigation of trace formation when using

Исследуется следообразование при использовании сети «Интернет» в данной преступной деятельности, а также особенности расследования обналичивания денежных средств через криптовалюту. **Ключевые слова:** блокчейн, криптовалюта, транзитные операции, обналичивание, сеть «Интернет»	the Internet in this criminal activity, as well as the special aspects of investigation of cashing funds through cryptocurrency. **Keywords:** blockchain, cryptocurrency, transit operations, cashing, the Internet
БЕЗБОРОДОВ Дмитрий Анатольевич, профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **СОМКО Виктория Владимировна,** студентка Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации **СОЦИАЛЬНО-ПРАВОВАЯ ОБУСЛОВЛЕННОСТЬ КРИМИНАЛИЗАЦИИ РАСПРОСТРАНЕНИЯ МАТЕРИАЛОВ, ПРОПАГАНДИРУЮЩИХ КУЛЬТ НАСИЛИЯ И ЖЕСТОКОСТИ, В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»** В статье рассматриваются последствия демонстрации, распространения и пропаганды в информационно-телекоммуникационной сети «Интернет» культа насилия и жестокости, дается оценка общественной опасности вышеуказанных материалов, предлагается криминализировать пропаганду материалов, содержащих культ насилия и жестокости, в том числе разработана редакция потенциальной нормы уголовного права **Ключевые слова:** культ жестокости, насилие, информационно-телекоммуникационная сеть «Интернет», пропаганда, треш-стриминг	**BEZBORODOV Dmitry Anatolyevich,** professor of the Department of Criminal Law, Criminology and Penal Enforcement Law of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation, Candidate of Law, Associate Professor **SOMKO Viktoria Vladimirovna,** student of St. Petersburg Law Institute (branch) of the University of Prosecutor's Office of the Russian Federation **SOCIO-LEGAL ASSESSMENT OF THE CRIMINALIZATION OF THE DISSEMINATION OF MATERIALS PROMOTING THE CULT OF CRUELTY AND VIOLENCE ON THE INTERNET INFORMATION AND TELECOMMUNICATIONS NETWORK** The article examines the consequences of the demonstration, dissemination and propaganda of the cult of cruelty and violence in the information and telecommunications network «Internet». An assessment of the public danger of the above-mentioned materials is given. The article also proposes to criminalize the propaganda of materials containing the cult of cruelty and violence, including the drafting of a potential rule of criminal law. **Keywords:** cult of cruelty, violence, information and telecommunication network «Internet», propaganda, trash streaming
БОГОВАЯ Ольга Фёдоровна, старший преподаватель кафедры русского языка Донецкого государственного университета	**BOGOVAYA Olga Fedorovna,** Senior Lecturer at the Department of Russian at Donetsk State University

КОСЯК Евгений Леонидович, доцент кафедры права и национальной безопасности Донецкого государственного университета, кандидат юридических наук	**KOSYAK Evgeny Leonidovich,** Associate Professor of the Department of Law and National Security of Donetsk State University, Candidate of Science (Law)
ПРОБЛЕМНЫЕ ВОПРОСЫ РАЗГРАНИЧЕНИЯ ПУБЛИЧНЫХ ПРИЗЫВОВ К ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ	**PROBLEMATIC ISSUES OF DISTINGUISHING PUBLIC CALLS FOR EXTREMIST AND TERRORIST ACTIVITIES**
В статье рассматриваются вопросы разграничения призывов к осуществлению экстремистской деятельности и террористической деятельности. В современных условиях роста политического экстремизма необходимо выработать эффективные меры противодействия подобным проявлениям. Авторы отмечают необходимость усовершенствования уголовно-правового противодействия призывам к экстремистской и террористической деятельности в информационной среде посредством внесения изменений в руководящие разъяснения Верховного Суда Российской Федерации с целью повышения эффективности применения соответствующих норм Уголовного кодекса Российской Федерации.	The article deals with the differentiation of appeals for extremist activity from appeals for terrorist activity. In conditions of the rise of political extremism the effective measures to counter appeals are necessary. Authors remark that the improvement of criminal law counteraction to appeals for extremism and terrorism by changing of Supreme Court's of Russian Federation guidance clarifications is necessary.
Ключевые слова: противодействие призывам к экстремистской и террористической деятельности, интернет, экстремистские проявления	**Keywords:** counteraction to appeals for extremism and terrorism, Internet, extremist manifestations
БОРИСОВ Игорь Дмитриевич, аспирант Санкт-Петербургского юридического института (филиал) Университета прокуратуры Российской Федерации	**BORISOV Igor Dmitrievich,** Postgraduate student of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation
К ВОПРОСУ О СООТНОШЕНИИ СОСТАВОВ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЯМИ 165 И 272 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ	**ON THE QUESTION OF THE RATIO OF THE ELEMENTS OF CRIMES PROVIDED FOR IN ARTICLES 165 AND 272 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
Несмотря на различную природу рассматриваемых уголовно- правовых норм, состав преступления, предусмотренный статьей 272 УК РФ, при определенных обстоятельствах может обладать специальным характером по отношению к статье 165	Despite the different nature of the criminal law norms under consideration, the corpus delicti provided for in Article 272 of the Criminal Code of the Russian Federation, under certain circumstances, may have a special character in relation to Article 165 of the Criminal Code of

УК РФ. При этом указанные составы преступления зачастую могут также порождать совокупность. **Ключевые слова:** причинение имущественного ущерба, неправомерный доступ, компьютерная информация, специальная норма, конкуренция норм, обман	the Russian Federation. At the same time, these elements of the crime can often also generate a set of crimes. **Keywords:** causing property damage, illegal access, computer information, special norm, competition of norms, deception
ГОЛОВКО Ирина Ивановна, декан факультета профессиональной переподготовки и повышения квалификации Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **УЧАСТИЕ ПРОКУРОРА В СУДАХ ОБЩЕЙ ЮРИСДИКЦИИ ПО ДЕЛАМ О ДИФФАМАЦИИ** В статье рассматриваются особенности правового регулирования и реализации полномочий прокурора в связи с распространением недостоверной информации, порочащей честь, достоинство или деловую репутацию гражданина. На основании результатов исследования сделан вывод, что прокурор вправе участвовать в рассмотрении судами споров о диффамации путем обращения с заявлением, в качестве третьего лица без самостоятельных требований, ответчика. **Ключевые слова:** прокурор, диффамация, порочащие недостоверные сведения, защита прав, судопроизводство	**GOLOVKO Irina Ivanovna,** Dean of the faculty of professional retraining and advanced training of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate professor **PARTICIPATION OF THE PROSECUTOR IN COURTS OF GENERAL JURISDICTION IN DEFAMATION CASES** The article discusses the features of legal regulation and implementation of the powers of the prosecutor in connection with the dissemination of false information discrediting the honor, dignity or business reputation of a citizen. Based on the results of the study, it was concluded that the prosecutor has the right to participate in the consideration of defamation disputes by the courts by filing a statement as a third party without independent demands and a defendant. **Keywords:** prosecutor, defamation, defamatory false information, protection of rights, legal proceeding
ГОЛУБЕВ Георгий Андреевич, прокурор отдела государственных обвинителей уголовно-судебного управления прокуратуры г. Санкт-Петербурга **ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ СБЫТОМ НАРКОТИКОВ И СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»** В статье на основе анализа уголовного законодательства и правоприменительной практики отмечены некоторые проблемы квалификации преступлений, связанных с	**GOLUBEV Georgy Andreevich,** Prosecutor of the Department of State Prosecutors of the Criminal Judicial Department of the Prosecutor's Office St. Petersburg **SOME PROBLEMS OF QUALIFICATION CRIMES RELATED TO THE ILLEGAL SALE DRUGS COMMITTED USING THE INTERNET** Based on the analysis of criminal legislation and law enforcement practice, the article highlights some problems in the qualification of crimes related to the illegal sale of

незаконным сбытом наркотиков, совершаемых с использованием сети «Интернет». Разработаны предложения по совершенствованию практики применения уголовного законодательства, предусматривающего ответственность за преступления, связанные с незаконным сбытом наркотиков, совершаемые с использованием сети «Интернет». **Ключевые слова:** сбыт наркотических средств через сеть «Интернет», проблемы квалификации преступлений	drugs committed using the Internet. Proposals have been developed to improve the practice of applying criminal legislation on liability for crimes related to the illegal sale of drugs committed using the Internet. **Keywords:** drugs sales via the Internet, problems of crime qualification
ЗАРУБИН Андрей Викторович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **НЕКОТОРЫЕ ВОПРОСЫ ОТВЕТСТВЕННОСТИ ЗА ОРГАНИЗАЦИЮ И ПРОВЕДЕНИЕ АЗАРТНЫХ ИГР, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ»** В статье рассматриваются некоторые проблемы уголовной ответственности за организацию и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны либо с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Разработаны предложения по совершенствованию практики применения уголовного законодательства, предусматривающего ответственность за организацию и (или) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, сеть «Интернет», организация и проведение азартных игр с использованием игрового оборудования вне игорной зоны	**ZARUBIN Andrey Viktorovich,** Associate Professor at the Department of criminal law, criminology and penal executive law, St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor **SOME ISSUES OF RESPONSIBILITY FOR THE ORGANIZATION AND CONDUCT OF GAMBLING COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET** The article discusses some problems of criminal liability for organizing and (or) conducting gambling games using gaming equipment outside the gambling zone, or using information and telecommunications networks, including the Internet. Proposals have been developed to improve the practice of applying criminal legislation on liability for organizing and (or) conducting gambling using information and telecommunications networks, including the Internet. **Keywords:** the qualification of crimes, the use of information and telecommunication networks, including the Internet, the organization and conduct of gambling using gaming equipment outside the gambling zone

КАДЫРОВА Надежда Николаевна, доцент кафедры уголовного права и криминологии Челябинского государственного университета, кандидат юридических наук, доцент	**KADYROVA Nadezhda Nikolaevna,** Associate Professor of the Department of criminal law and criminology of Chelyabinsk State University, Candidate of Sciences (Law), Associate Professor
К ВОПРОСУ О ЗНАЧЕНИИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ	**ON THE QUESTION OF THE IMPORTANCE OF USING ELECTRONIC OR INFORMATION AND TELECOMMUNICATION NETWORKS IN THE COMMISSION OF CRIMES**
В данной статье рассматриваются уголовно-правовое и криминологическое значение использования электронных и информационно-телекоммуникационных сетей при совершении преступлений, отмечается необходимость совершенствования отечественного уголовного законодательства и норм иных отраслей права в части установления соответствующих ограничений при использовании информационно-телекоммуникационной сети.	This article examines the criminal law discipline and criminological significance of the use of electronic and information and telecommunication networks in the commission of crimes, and notes the need to improve domestic criminal legislation and the norms of different branches of law in terms of establishing appropriate restrictions on the use of information and telecommunication networks.
Ключевые слова: преступления в информационно-телекоммуникационной сети, детерминанты преступности, квалификация преступлений	**Keywords:** crimes in information and telecommunication network, determinants of crime, qualification of crimes
КАЛАШНИКОВ Виктор Сергеевич, доцент кафедры уголовного процесса и криминалистики Кемеровского государственного университета, кандидат юридических наук	**KALASHNIKOV Viktor Sergeevich,** ASSOCIATE Professor of the Department of criminal procedure and criminalistics of Kemerovo State University, Candidate of Science (Law)
РОЛЬ ПРОКУРОРА В ОПРЕДЕЛЕНИИ ТЕРРИТОРИАЛЬНОЙ ПОДСЛЕДСТВЕННОСТИ УГОЛОВНЫХ ДЕЛ О ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ	**THE ROLE OF THE PROSECUTOR IN DETERMINING THE TERRITORIAL JURISDICTION OF CRIMINAL CASES OF CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES**
Статья посвящена вопросу определения места совершения преступления, совершенного с использованием информационно-коммуникационных технологий, и роли прокурора в противодействии необоснованному перенаправлению сообщений о преступлениях между территориальными правоохранительными органами. Рассмот-	The article is devoted to the issue of determining the place of commission of a crime committed using information and communication technologies and the role of the prosecutor in countering the unjustified redirection of crime reports between territorial law enforcement agencies. The correlation of information and physical space is considered in order to determine the place of investigation of a crime.

рено соотношение информационного и физического пространства в целях определения места расследования преступления. Предложено применять положения ст. 151 УПК РФ к спорам о территориальной подследственности и разрешать их прокурору, а в необходимых случаях и самостоятельно инициировать процесс передачи материалов процессуальной проверки или уголовного дела уполномоченному территориальному органу расследования. **Ключевые слова:** территориальная подследственность, киберпреступления, информационное пространство, информационно коммуникационные технологии, место совершения преступления, прокурор	It is proposed to apply the provisions of Article 151 of the Criminal Procedure Code of the Russian Federation to disputes on territorial jurisdiction and resolve them to the prosecutor, and, if necessary, independently initiate the process of transferring the materials of a procedural check or a criminal case to the authorized territorial investigation body. **Keywords:** territorial jurisdiction, cybercrimes, information space, information and communication technologies, crime scene, prosecutor
КАФИАТУЛИНА Алла Владимировна, доцент кафедры уголовно-правовых дисциплин Ивановского филиала Российской академии народного хозяйства и государственной службы при Президента Российской Федерации, кандидат юридических наук **ПОРЯДОК И ПРАКТИКА НАЗНАЧЕНИЯ ЛИШЕНИЯ ПРАВА ЗАНИМАТЬ ОПРЕДЕЛЕННЫЕ ДОЛЖНОСТИ ИЛИ ЗАНИМАТЬСЯ ОПРЕДЕЛЕННОЙ ДЕЯТЕЛЬНОСТЬЮ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** Наказание в виде лишения права занимать определенные должности или заниматься определенной деятельностью имеет ярко выраженный превентивный характер, лишая осужденного перспективы злоупотребления возможностями, вытекающими из занятия той или иной деятельностью, в целях предупреждения повторного совершения им аналогичного преступления, что предопределяет необходимость разумной конкретизации в приговоре — при условии его исполнимости — запрещаемой профессиональной или другой деятельности. Автором проведен выборочный анализ порядка и практики назначения этого вида наказания в сфере компьютерной информации, предложены формулировки уголовно-правового запрета.	**KAFIATULINA Alla Vladimirovna,** Associate Professor of the Department of criminal law disciplines of the Ivanovo branch of the Russian academy of national economy and public administration under the President of the Russian Federation, Candidate of Science (Law) **THE PROCEDURE AND PRACTICE OF APPOINTMENT AND DEPRIVATION OF THE RIGHT TO HOLD CERTAIN POSITIONS OR ENGAGE IN CERTAIN ACTIVITIES IN THE FIELD OF COMPUTER INFORMATION** The relevance of the study lies in the fact that the punishment in the form of deprivation of the right to hold certain positions or engage in certain activities has a pronounced preventive character, depriving the convicted person of the prospect of abusing the opportunities arising from engaging in a particular activity in order to prevent him from re-committing a similar crime, which determines the need for reasonable specification in the sentence — provided it enforceability — prohibited professional or other activity. The author conducted a selective analysis of the procedure and practice of assigning this type of punishment in the field of computer information, and proposed formulations of a criminal law prohibition.

Ключевые слова: наказание, лишение права заниматься определенной деятельностью, администрирование сайтов, компьютерная информация	**Keywords:** punishment, deprivation of the right to engage in certain activities, website administration, computer information
КИРИЛЛОВА Яна Максимовна, доцент кафедры уголовного права и процесса Санкт-Петербургского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук **ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)** В статье рассматриваются некоторые проблемы преступлений против собственности, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). Исследуемые проблемы связаны с неопределенностью предмета и способа совершения преступлений. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за преступления против собственности, совершаемые с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). **Ключевые слова:** киберпреступления, хищение, мошенничество, кража, преступления против собственности	**KIRILLOVA Yana Maksimovna,** Associate Professor of the Department of criminal law and procedure at the St. Petersburg Institute (branch) All-Russian state university of law (RPA of the Ministry of justice of the Russian Federation), Candidate of Science (Law) **PROBLEMS OF QUALIFICATION OF CRIMES AGAINST PROPERTY COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)** The article discusses some problems of crimes against property committed using information and telecommunication networks (including the Internet). The problems under study are related to the uncertainty of the subject and method of committing crimes. Proposals have been developed to improve the practice of applying criminal legislation on liability for crimes against property committed using information and telecommunications networks (including the Internet). **Keywords:** cybercrime, theft, fraud, theft, crimes against property
КОСТРОВА Марина Борисовна, профессор кафедры уголовного права и процесса Института права Уфимского университета науки и технологий, кандидат юридических наук, доцент **ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»), В РОССИЙСКОМ УГОЛОВНОМ ПРАВЕ: ЯЗЫКОВОЙ АСПЕКТ**	**KOSTROVA Marina Borisovna,** Professor of the Chair of Criminal Law and Procedure of the Institute of Law of the Ufa University of Science and Technologies, Candidate of Sciences (Law), Associate Professor, **CRIMES COMMITTED WITH THE USE OF MASS MEDIA OR ELECTRONIC OR INFORMATION-TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET), IN RUSSIAN CRIMINAL LAW: LINGUISTIC ASPECT**

В статье на основе анализа норм уголовного и информационного права критически оценивается несистемный подход законодателя к употреблению языковых средств в российском уголовном законе при формулировании признака «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть “Интернет”)» в его различных вариациях в разных составах преступлений.	Based on the analysis of the norms of criminal and information law, the article critically assesses the non-systematic approach of the legislator to the use of language means in Russian criminal law in the formulation of the feature «with the use of mass media or electronic or information and telecommunication networks (including the Internet)» in its various variations in different crimes**.**
Ключевые слова: уголовный закон, язык уголовного закона, преступление, признак состава преступления, средства массовой информации, электронные сети, информационно-телекоммуникационные сети, сеть «Интернет»	**Keywords:** criminal law, language of criminal law, crime, sign of corpus delicti, mass media, electronic networks, information-telecommunication networks, the Internet network
КРАВЧЕНКО Роман Михайлович, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации», кандидат юридических наук	**KRAVCHENKO Roman Mikhailovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (Branch) University of the prosecutor's office of the Russian Federation, Candidate of Sciences (Law)
ВОПРОСЫ КВАЛИФИКАЦИИ ОБОРОТА ПОДДЕЛЬНЫХ ЭЛЕКТРОННЫХ ОФИЦИАЛЬНЫХ ДОКУМЕНТОВ	**ISSUES OF QUALIFICATION OF THE TURNOVER OF FORGED ELECTRONIC OFFICIAL DOCUMENTS**
Работа посвящена рассмотрению вопросов подделки и использования электронных официальных документов, соотношению составов преступлений, предусмотренных ст.ст. 327 и 272 УК РФ. В работе проанализированы положения уголовного законодательства, разъяснения Пленума Верховного Суда Российской Федерации, материалы судебной практики и положения научных трудов по заявленной теме. Разработаны и сформулированы предложения по совершенствованию применения норм об ответственности за незаконный оборот электронных официальных документов.	The work is devoted to the consideration of issues of forgery and use of electronic official documents, the ratio of the elements of crimes provided for in Articles 327 and 272 of the Criminal Code of the Russian Federation. The article analyzes the provisions of criminal legislation, explanations of the Plenum of the Supreme Court of the Russian Federation, materials of judicial practice and the provisions of scientific papers on the stated topic. Proposals have been developed and formulated to improve the application of the rules on liability for illegal trafficking in electronic official documents.
Ключевые слова: официальный документ, электронный документ, статья 327 УК РФ, статья 272 УК РФ	**Keywords:** official document, electronic document, Article 327 of the Criminal Code of the Russian Federation, Article 272 of the Criminal Code of the Russian Federation

КРАЕВ Денис Юрьевич, профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**KRAYEV Denis Yurievich**, Professor of the Department of criminal law, criminology and penal executive law, St. Petersburg Law Institute (branch) of the University of the prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate professor
КВАЛИФИКАЦИЯ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ, НАПРАВЛЕННОЙ НА ПОБУЖДЕНИЕ К СОВЕРШЕНИЮ САМОУБИЙСТВА, СОПРЯЖЕННОЕ С ПУБЛИЧНЫМ ВЫСТУПЛЕНИЕМ, ИСПОЛЬЗОВАНИЕМ ПУБЛИЧНО ДЕМОНСТРИРУЮЩЕГОСЯ ПРОИЗВЕДЕНИЯ, СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ») (ч. 2 ст. 110.2 УК РФ)	**QUALIFICATION OF ORGANIZING ACTIVITIES AIMED AT INDUCING SUICIDE BY DISSEMINATING INFORMATION ABOUT METHODS OF COMMITTING SUICIDE OR CALLS TO COMMIT SUICIDE, ASSOCIATED WITH PUBLIC SPEAKING, THE USE OF A PUBLICLY DISPLAYED WORK, THE MEDIA OR INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET) (PART 2 OF ARTICLE 110.2 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)**
В статье рассматриваются некоторые вопросы уголовно-правовой оценки организации деятельности, направленной на побуждение к совершению самоубийства, совершенное путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства, сопряженных с публичным выступлением, использованием публично демонстрирующегося произведения, средств массовой информации или информационно-телекоммуникационных сетей (включая сеть «Интернет»).	The article discusses some issues of the criminal legal assessment of the organization of activities aimed at inducing suicide by disseminating information about methods of committing suicide or calls to commit suicide associated with public speaking, the use of a publicly displayed work, the media or information and telecommunication networks (including the Internet).
Ключевые слова: организация деятельности, направленной на побуждение к совершению самоубийства, распространение информации о способах совершения самоубийства, призывы к совершению самоубийства, публичное выступление, публично демонстрирующееся произведение, средства массовой информации, информационно-телекоммуникационные сети, сеть «Интернет», статья 110.2 Уголовного кодекса Российской Федерации	**Keywords:** organizing activities aimed at inducing suicide; dissemination of information about methods of committing suicide; calls to commit suicide; public speaking; publicly displayed work; mass media; information and telecommunication networks; Internet»; Article 110.2 of the Criminal Code of the Russian Federation
КУРСАЕВ Александр Викторович, главный эксперт-специалист Договорно-правового департамента МВД России, кандидат юридических наук	**KURSAEV Alexander Viktorovich,** chief Expert-Specialist of the Contract and Legal Department of the Ministry of Internal Affairs of Russia, Candidate of Legal Sciences

НЕЗАКОННОЕ РАСПРОСТРАНЕНИЕ ПОРНОГРАФИЧЕСКИХ МАТЕРИАЛОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»	**ILLEGAL DISTRIBUTION OF PORNOGRAPHIC MATERIALS USING INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET**
Статья посвящена проблемам уголовно-правовой квалификации распространения порнографических материалов с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет». Обращается внимание на особенности субъективной стороны такого деяния. Исследуется вопрос соотношения рассматриваемого преступления с иными уголовно-правовыми нормами и случаи, при которых они образуют идеальную совокупность преступлений.	The article is devoted to the problems of criminal legal qualification of the distribution of pornographic materials using information and telecommunication networks, including the Internet. Attention is drawn to the peculiarities of the subjective side of such an act. The issues of correlation of the considered crime with other criminal law norms and the cases in which they form an ideal set of crimes are investigated.
Ключевые слова: порнография, распространение порнографических материалов, квалификация преступлений, субъективное вменение	**Keywords:** pornography, distribution of pornographic materials, qualification of crimes, subjective imputation
МЕДУНЦОВА Сабина Мурсаловна, научный сотрудник отдела НИИ Университета прокуратуры Российской Федерации	**MEDUNTSOVA Sabina Mursalovna**, Researcher of the Department at the Research Institute of the University of the prosecutor's office of the Russian Federation
ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, СВЯЗАННЫЕ С БЛАНКЕТНЫМИ ПРИЗНАКАМИ СОСТАВОВ ЭТИХ ПРЕСТУПЛЕНИЙ	**PROBLEMS OF QUALIFICATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION, BLANKET SIGNS RELATED COMPONENTS OF THESE CRIMES**
Настоящая статья посвящена рассмотрению проблем квалификации преступлений в сфере компьютерной информации, которые связаны с бланкетным характером диспозиций норм этих преступлений. В ходе исследования проанализирована судебная практика, а также правоприменительные проблемы, связанные с привлечением к уголовной ответственности за совершение преступлений в сфере компьютерной информации.	This article is devoted to the consideration of problems of qualification of crimes in the field of computer information, which are associated with the blanket nature of the dispositions of the norms of these crimes. The study analyzed judicial practice, as well as law enforcement problems related to criminal prosecution for crimes in the field of computer information.
Ключевые слова: квалификация преступлений, преступления в сфере компьютерной информации, бланкетная норма права, уголовная ответственность	**Keywords:** qualification of crimes, computer crimes, blanket norm of law, criminal liability

МОРОЗОВА Юлия Владимировна, доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук

НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В статье рассматриваются некоторые проблемы квалификации преступления, предусмотренного п. «г» ч. 2 ст. 242.1 УК РФ. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних с использованием информационно-телекоммуникационных сетей.

Ключевые слова: несовершеннолетние, порнография, детская порнография, развратные действия, сексуальная эксплуатация

MOROZOVA Yulia Vladimirovna, Associate Professor of the Department of criminal law, criminology and criminal executive law of the St. Petersburg Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Candidate of Sciences (Law)

SOME ISSUES OF CLASSIFICATION OF CRIMES AGAINST MINORS, COMPLETED USING INFORMATION AND TELECOMMUNICATION NETWORKS

The article discusses some problems of qualification of the offense provided for in paragraph "d" of Part 2 of Article 242.1 of the Criminal Code of the Russian Federation. Proposals have been developed to improve the practice of applying criminal legislation on liability for the manufacture and trafficking of materials or objects with pornographic images imperfectly using information and telecommunication networks.

Keywords: minors, pornography, child pornography, indecent acts, sexual exploitation

НЕПЕИН Григорий Григорьевич, научный сотрудник криминалистической лаборатории Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации

ОСОБЕННОСТИ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ ПРИ ПРОИЗВОДСТВЕ ОБЫСКА (ВЫЕМКИ)

В статье рассматриваются вопросы расследования преступлений, совершенных с использованием информационно-телекоммуникационных (компьютерных) технологий, а также тактические приемы обыска помещений и жилища с целью поиска и последующего изъятия электронных носителей информации, а также иных объектов информационно-телекоммуникационных (компьютерных) технологий.

NEPEIN Grigory Grigorievich, Researcher at the forensic laboratory of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation

FEATURES OF THE SEIZURE OF ELECTRONIC MEDIA DURING A SEARCH (SEIZURE)

The article deals with the investigation of crimes committed using information and telecommunication (computer) technologies, as well as tactical techniques for conducting a search of premises and dwellings in order to search and subsequently seize electronic media, as well as other objects of information and telecommunication (computer) technologies.

Ключевые слова: преступление, следователь, криминалистика, уголовное дело, обыск, выемка, компьютер, электронный носитель информации	**Keywords:** crime, investigation, criminalistics, criminal case, search, seizure, computer, electronic storage device
ПЕТРОВА Татьяна Михайловна, аспирант Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации **НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ И ЗАКОНОДАТЕЛЬНОЙ РЕГЛАМЕНТАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ», ПРОТИВ ОСОБО ОХРАНЯЕМЫХ БИОРЕСУРСОВ** Актуальность темы исследования обусловлена развитием цифровых технологий, оказывающих огромное влияние на все сферы человеческой жизнедеятельности. В области обеспечения экологической безопасности наиболее глобальной задачей является защита редких и исчезающих видов животных и растений. В статье рассматриваются некоторые проблемы квалификации и законодательной регламентации преступлений против особо охраняемых биоресурсов, совершаемых с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»). **Ключевые слов:** цифровые технологии, интернет, ценные виды животного и растительного мира, экологические преступления	**PETROVA Tatyana Mikhailovna,** Graduate student St. Petersburg Law Institute (branch) of the University of the prosecutor's office of the Russian Federation, Candidate of Legal Sciences **SOME ISSUES OF QUALIFICATION AND LEGISLATIVE REGULATION OF CRIMES COMMITTED USING THE INTERNET AGAINST SPECIALLY PROTECTED BIOLOGICAL RESOURCES** The relevance of the research topic is due to the development of digital technologies, which have a huge impact on all spheres of human life. In the field of ensuring environmental safety, the protection of rare and endangered species of animals and plants is the most global task. The article discusses some problems of qualification and legislative regulation of crimes against specially protected biological resources committed using the media or electronic or information and telecommunication networks (including the Internet). **Key words:** digital technologies, Internet, valuable species of flora and fauna, environmental crimes
ПИСКУН Лидия Павловна, помощник прокурора Кронштадтского района г. Санкт-Петербурга **АЛГОРИТМ ПОДГОТОВКИ ИСКОВОГО ЗАЯВЛЕНИЯ О ВЗЫСКАНИИ НЕОСНОВАТЕЛЬНОГО ОБОГАЩЕНИЯ ПО УГОЛОВНЫМ ДЕЛАМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ** В настоящей статье автором представлен краткий алгоритм подготовки в порядке	**PISKUN Lidia Pavlovna,** Assistant of the prosecutor of the Kronstadt district of St. Petersburg **THE ALGORITHM FOR PREPARING A STATEMENT OF CLAIM FOR RECOVERY OF UNJUSTIFIED ENRICHMENT IN CRIMINAL CASES IN THE FIELD OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES** In this article, the author presents a brief algorithm for preparing, in accordance with Arti-

ст. 45 ГПК РФ искового заявления о взыскании неосновательного обогащения. Алгоритм может использоваться прокурорскими работниками при осуществлении надзорной деятельности за органами предварительного расследования по уголовным делам в сфере информационных технологий. **Ключевые слова:** информационные технологии, исковое заявление, мошенничество, неосновательное обогащение	cle 45 of the Civil Procedure Code of the Russian Federation, a statement of claim for recovery of unjustified enrichment. The algorithm can be used by prosecutors in the implementation of supervisory activities for the bodies of preliminary investigation of criminal cases in the field of information technology. **Keywords:** information technology, claims, fraud, unjust enrichment
ПИКАЛОВ Станислав Владимирович, аспирант Санкт-Петербургского государственного университета **ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ИСПОЛЬЗОВАНИЯ СЛУЖЕБНОГО ПОЛОЖЕНИЯ ПРИ КВАЛИФИКАЦИИ ОТДЕЛЬНЫХ ВИДОВ ПРЕСТУПЛЕНИЙ** В статье анализируются проблемы практики применения квалифицирующего признака «с использованием служебного положения», содержащегося в ст.ст. 272, 273 УК РФ. В качестве одной из проблем автор выделяет неверное понимание судами признаков субъекта преступлений. Вместо лиц, которые обладают организационно-распорядительными или административно-хозяйственными полномочиями или признаками должностного лица, к уголовной ответственности привлекаются рядовые сотрудники частных организаций за нарушение профессиональных функций. **Ключевые слова:** компьютерная информация, использование служебного положения, должностные преступления, квалификация, расследование	**PIKALOV Stanislav Vladimirovich**, Postgraduate student, St. Petersburg University **PROBLEMS OF DETERMINING THE USE OF OFFICIAL POSITION IN THE QUALIFICATION OF CERTAIN TYPES OF CRIMES** The article analyzes the problems of the practice of applying the qualifying attribute "using official position" according to Articles 272, 273 of the Criminal Code of the Russian Federation. As one of the problems, the author highlights the incorrect understanding by the courts of the signs of the subject of crimes. Instead of persons who have organizational and administrative or administrative-economic powers, or signs of an official, ordinary employees of private organizations are brought to criminal responsibility for violations of professional functions. **Keywords:** computer information, use of official position, official crimes, qualifications, investigation
ПОБЕГАЙЛО Анастасия Эдуардовна, доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, кандидат юридических наук **УГОЛОВНО-ПРАВОВАЯ И КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, РАСПРОСТРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ**	**POBEGAILO Anastasia Eduardovna,** associate Professor of the Department of Criminal Law Disciplines of the University of the Prosecutor's Office of the Russian Federation, Candidate of Legal Sciences **CRIMINAL LAW AND CRIMINOLOGICAL CHARACTERISTICS OF THE CREATION, DISTRIBUTION AND USE OF MALICIOUS COMPUTER PROGRAMS**

Статья 273 УК РФ, хотя и присутствует в УК РФ с момента его принятия, имеет ряд проблем, которые не были решены ни изменениями, внесенными Федеральным законом от 07.12.2011 № 420-ФЗ, ни Постановлением Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37; помимо проблемных уголовно-правовых аспектов, деяния, предусмотренные ст. 273 УК РФ, являются высоколатентными и требуют специальных мер общесоциальной и специальной криминологической профилактики.	Creation, distribution and use of malicious computer programs, although present in the Criminal Code of the Russian Federation since its adoption, has a number of problems that have not been solved either by the changes introduced by the Federal Law of 07.12.2011 № 420-FZ, or by the Resolution of the Plenum of the Supreme Court of the Russian Federation of 15.12.2022 № 37; in addition to the problematic criminal-legal aspects, the acts envisaged by Art. 273 of the Criminal Code of the Russian Federation are highly latent, and require special measures of general social and special criminological prevention.
Ключевые слова: создание, использование, распространение вредоносных компьютерных программ, ст. 273 УК РФ, киберпреступность, киберпреступления	**Keywords:** creation, use, distribution of malicious computer programs, article 273 of the Criminal Code of the Russian Federation, cybercrime, cybercrime
РАДЧЕНКО Алексей Андреевич, доцент Иркутского института (филиала) Всероссийского государственного университета юстиции, кандидат юридических наук	**RADCHENKO Alexei Andreevich**, Associate professor of Irkutsk Institute (branch) All-Russian State University of Justice, Candidate of Science (Law)
НЕКОТОРЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ ПРОТИВ ОСНОВ КОНСТИТУЦИОННОГО СТРОЯ И БЕЗОПАСНОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	**SOME ISSUES OF QUALIFICATION OF CRIMES AGAINST THE FOUNDATIONS OF THE CONSTITUTIONAL ORDER AND SECURITY OPERATIONS CARRIED OUT USING INFORMATION AND TELECOMMUNICATION NETWORKS**
В статье рассматриваются вопросы уголовно-правовой оценки совершения действий, образующих состав преступления, предусмотренного статьей 275.1 УК РФ, с использованием информационно-телекоммуникационных сетей. Анализируются различные вариантах возможного применения уголовного закона в случае оконченного и неоконченного установления и поддержания конфиденциального сотрудничества российских граждан с иностранными специальными службами. Рассматривается соотношение государственной измены и «сотрудничества на конфиденциальной основе с иностранной стороной».	The article discusses the issues of criminal legal assessment of the commission of actions that constitute a crime under Article 275.1 of the Criminal Code of the Russian Federation, using information and telecommunication networks. Various options for the possible application of the criminal law in the case of completed and unfinished establishment and maintenance of confidential cooperation of Russian citizens with foreign special services are analyzed. The relationship between high treason and “cooperation on a confidential basis with a foreign party” is considered.
Ключевые слова: государственная измена, шпионаж, конфиденциальное сотрудничество, приготовление, покушение, соучастие	**Keywords:** treason, spying confidential cooperation, preparation, attempt, complicity

РЕЗЦОВ Андрей Викторович, прокурор отдела управления Генеральной прокуратуры Российской Федерации по Северо-Западному федеральному округу	**REZTSOV Andrey Viktorovich,** Prosecutor, Department of the Prosecutor General's Office of the Russian Federation in the North-Western Federal District
ПРОТИВОДЕЙСТВИЕ ДИСТАНЦИОННОМУ ХИЩЕНИЮ ДЕНЕЖНЫХ СРЕДСТВ: ОБМЕН ОПЫТОМ, ОЦЕНКИ И ТЕНДЕНЦИИ	**COUNTERING REMOTE THEFT OF FUNDS: EXCHANGE OF EXPERIENCE, ASSESSMENTS AND TRENDS**
В статье анализируются результаты проведенного 08.11.2023 в Санкт-Петербурге форума «Противодействие и профилактика несанкционированных операций по переводу денежных средств с банковских счетов, совершенных с использованием электронных средств платежа». Оцениваются предлагаемые способы повышения эффективности противодействия дистанционным хищениям денежных средств. Рассматриваются вопросы преодоления латентности преступлений экономической направленности.	The article analyzes the results of the forum held on 11/28/2023 in St. Petersburg "Prevention and prevention of unauthorized money transfer operations from bank accounts performed using electronic means of payment". The proposed ways to increase the effectiveness of countering remote theft of funds are evaluated. The issues of overcoming the latency of economic crimes are considered.
Ключевые слова: цифровые технологии, интернет, операции без согласия, координация, социальная инженерия, латентные преступления	**Keywords:** digital technologies, Internet, transactions without the consent, coordination, social engineering, latent crimes
САФАРОВ Эмиль Алмасович, аспирант Санкт-Петербургской юридической академии	**SAFAROV Emil Almasovich,** Postgraduate student at the St. Petersburg Law Academy
НЕЙРОСЕТЬ КАК ОРУДИЕ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ: НОВЫЕ ВЫЗОВЫ ДЛЯ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ	**ARTIFICIAL INTELLIGENCE AS AN INSTRUMENT FOR COMMITTING CRIMES: NEW CHALLENGES FOR THE LAW ENFORCEMENT SYSTEM**
В настоящей научной статье рассматриваются вопросы использования нейросети как орудия совершения преступления. Дано определение технологий нейронных сетей, проанализированы способы использования нейросетей в преступной деятельности. Предложено решение проблем, выявленный в процессе исследования темы, и даны перспективные предложения для их решения.	In the present scientific article, issues regarding the use of neural networks as a tool for committing crimes are examined. A definition of neural network technologies is provided, and methods of using neural networks in criminal activities are analyzed. The problems of the research topic are identified, and prospective suggestions for their resolution are presented.
Ключевые слова: уголовный кодекс, информационные технологии, нейросети, искусственный интеллект, преступления, IT, киберпреступления	**Keywords:** criminal code, information technologies, neural networks, artificial intelligence, crimes, IT, cybercrimes

САФОНОВ Владимир Николаевич, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**SAFONOV Vladimir Nikolaevich,** Associate Professor of the Department of criminal law of the Northwestern Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor
ПРАВОВАЯ ОЦЕНКА ХИЩЕНИЯ В МЕЛКИХ РАЗМЕРАХ ПРИ КВАЛИФИЦИРУЮЩИХ ПРИЗНАКАХ (НА ПРИМЕРЕ КРАЖИ С БАНКОВСКОГО СЧЕТА, А РАВНО В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ)	**LEGAL ASSESSMENT OF THEFT IN SMALL AMOUNTS WITH QUALIFYING SIGNS (FOR EXAMPLE, THEFT FROM A BANK ACCOUNT, AS WELL AS IN RELATION TO ELECTRONIC MONEY)**
В статье рассматривается дискуссионная в доктрине уголовного права правовая оценка мелкого хищения в целом и кражи с банковского счета, а равно в отношении электронных денежных средств в частности, когда деяние совершено при квалифицирующих признаках. Указывается на противоположные подходы в доктрине и в судебной практике. На основе принципов уголовного права предлагается установить нижний предел мелкого хищения, совершенного при квалифицирующих признаках, для его законодательного закрепления в качестве преступления.	The article discusses the controversial legal assessment in the doctrine of criminal law of petty theft in general and theft from a bank account, as well as in relation to electronic money, in particular, when the act was committed with qualifying signs. The opposite approaches in the doctrine and in judicial practice are pointed out. Based on the principles of criminal law, it is proposed to establish the lower limit of petty theft committed with qualifying signs for its legislative consolidation as a crime.
Ключевые слова: хищение, кража, кража с банковского счета, кража электронных денежных средств, малозначительное деяние, мелкое хищение, принципы уголовного права	**Keywords:** embezzlement; theft; theft from a bank account, as well as in relation to electronic money; insignificant act; petty crime; principles of criminal law
СЕРДЮК Александра Юрьевна, старший преподаватель кафедры прокурорского надзора и участия прокурора в гражданском, арбитражном и административном процессе Крымского юридического института (филиала) Университета прокуратуры Российской Федерации	**SERDYUK Aleksandra Yuryevna,** Senior Lecturer, Department of prosecutorial supervision and participation of the prosecutor in civil, arbitration and administrative procedure, crimean law institute (branch) of the University of prosecutor's office of the Russian Federation
К ВОПРОСУ О СУБЪЕКТЕ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 172.2 УК РФ	**TO THE QUESTION OF THE SUBJECT OF THE CRIME PROVIDED FOR IN ARTICLE 172.2 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
В статье дана характеристика субъекта преступления, предусмотренного ст. 172.2 УК РФ. В действующей редакции данной нормы субъект преступления определен как общий. При этом существует неопре-	The article provides a description of the subject of the crime provided for in Art. 172.2 of the Criminal Code of the Russian Federation. In the current version of this norm, the subject of the crime is defined as general. At the same

деленность в части возможности привлечения к уголовной ответственности сотрудников и активных вкладчиков финансовой пирамиды и коллизии с институтом соучастия в преступлении. Рассмотрены отдельные аспекты субъекта организации деятельности по привлечению имущества как преступления в сфере экономической деятельности. Проведено сравнение субъектов административной и уголовной ответственности. **Ключевые слова:** финансовая пирамида, субъект преступления, привлечение денежных средств, преступления в сфере экономики, статья 172.2 УК РФ, статья 14.62 КоАП РФ	time, there is uncertainty regarding the possibility of bringing to criminal liability employees and active investors of a financial pyramid and conflicts with the institution of complicity in a crime. Certain aspects of the subject of the organization in the activity of attracting property as a crime in the field of economic activity are considered. A comparison is made between subjects of administrative and criminal liability. **Keywords:** financial pyramid, subject of the crime, entrepreneurial activity, raising funds, economic crimes, Art. 172.2 of the Criminal Code of the Russian Federation, Art. 14.62 Code of Administrative Offenses of the Russian Federation
СУМАЧЕВ Алексей Витальевич, профессор кафедры уголовно-правовых дисциплин Института государства и права Тюменского государственного университета, доктор юридических наук, профессор **ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»): УГОЛОВНО-ПРАВОВЫЕ «МИНУСЫ»** В статье рассматриваются вопросы использования информационно-телекоммуникационных сетей (включая сеть «Интернет») в процессе совершения преступлений. Констатируется, что такие действия (использование компьютеров) порой существенно влияют на ужесточение уголовной ответственности, причем иногда ужесточение наказания за совершение соответствующих видов квалифицированных (особо квалифицированных) составов преступлений чрезмерно, даже необоснованно велико. Отмечается, что имеются и достоинства в сфере использования компьютеров (компьютерной информации), когда речь идет об уголовно-правовой охране добросовестных пользователей информационно-телекоммуникационных сетей (включая сеть «Интернет»).	**SUMACHEV Alexey Vitalievich,** Professor of the Department of criminal law disciplines of the Institute of State and Law of Tyumen State University, Doctor of Science (Law), Professor **USE OF INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET): CRIMINAL LAW "DISADVANTAGES"** The article discusses the use of information and telecommunication networks (including the Internet) in the process of committing crimes. It is stated that such actions (the use of computers) sometimes significantly affect the tightening of criminal liability, and sometimes the tightening of penalties for the commission of appropriate types of qualified (especially qualified) crimes is excessive and even unreasonably large. It is noted that there are advantages in the use of computers (computer information) when it comes to the criminal protection of bona fide users of information and telecommunications networks (including the Internet).

Ключевые слова: информационно-телекоммуникационные сети, интернет, квалифицирующие признаки, конструктивные признаки, ужесточение наказания	**Keywords:** information and telecommunication networks, the Internet, qualifying signs, constructive signs, tougher penalties
ТИМОЩУК Кирилл Игоревич, старший преподаватель кафедры общегуманитарных и социально-экономических дисциплин Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат физико-математических наук	**TIMOSHCHUK Kirill Igorevich,** Senior lecturer at the Department of general humanitarian and socio-economic disciplines of the St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation, Candidate of Science (Physical and Mathematical)
ПРЕСТУПЛЕНИЯ ПРОТИВ РЕЛИГИОЗНЫХ ПРАВ ГРАЖДАН, СОВЕРШАЕМЫЕ В СЕТИ «ИНТЕРНЕТ», В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ СТРАН	**CRIMES AGAINST THE RELIGIOUS RIGHTS OF CITIZENS COMMITTED ON THE INTERNET AND IN THE CRIMINAL LEGISLATION OF FOREIGN COUNTRIES**
В статье приводятся результаты сравнительного анализа позиций законодателей в подходах к формулированию диспозиций и санкций соответствующих статей уголовных кодексов и других нормативных правовых актов Российской Федерации и ряда зарубежных государств, обеспечивающих защиту уголовно-правовыми средствами религиозных прав граждан, в том числе в сети «Интернет». Результаты проведенного анализа позволили не только сформулировать существующие проблемы, связанные с применением указанных статей Уголовного кодекса Российской Федерации, но и предложить некоторые варианты их решения для повышения эффективности противодействия нарушениям конституционного права на свободу совести и вероисповедания.	The article presents the results of a comparative analysis of the positions of legislators in approaches to the formulation of dispositions and sanctions of the relevant articles of the criminal codes and other normative legal acts of the Russian Federation and a number of foreign states that ensure the protection of religious rights of citizens by criminal legal means, including on the Internet. The results of the analysis made it possible not only to formulate existing problems related to the application of these articles of the Criminal Code of the Russian Federation, but also to propose some solutions to improve the effectiveness of the practice of countering violations of the constitutional right to freedom of conscience and religion.
Ключевые слова: уголовное право, уголовная ответственность, преступление, религиозные права, права граждан, зарубежные государства	**Keywords:** criminal law, criminal liability, crime, religious rights, citizens' rights, foreign states
ТИТОВ Сергей Николаевич, проректор по учебно-методической работе, доцент кафедры права Ульяновского государственного педагогического университета имени И.Н. Ульянова, кандидат юридических наук, доцент	**TITOV Sergey Nikolaevich,** Vice-Rector for educational and methodological work, Associate professor of the Department of law of the Ulyanovsk State Pedagogical University named after I.N. Ulyanov, Candidate of Law, Associate Professor

ПРИЗНАК ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СОСТАВАХ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ	**SIGN OF THE USE OF INFORMATION TECHNOLOGY IN CRIMES AGAINST INTELLECTUAL PROPERTY**
Статья посвящена проблеме учета использования информационных технологий при совершении преступлений против интеллектуальной собственности. Автор рассматривает эту проблему в трех аспектах: использование при совершении преступлений компьютерной информации, информационно-телекоммуникационных сетей, включая сеть «Интернет», и использование при совершении преступлений технологий искусственного интеллекта. Предлагается включение в отдельные статьи о преступлениях против интеллектуальной собственности квалифицирующего признака «деяние, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть “Интернет”, либо с использованием систем искусственного интеллекта».	The article is devoted to the problem of accounting for the use of information technology in the commission of crimes against intellectual property. The author considers this problem in three aspects: the use of computer information in the commission of crimes, information and telecommunication networks, including the Internet, and the use of artificial intelligence technologies in the commission of crimes. It is proposed that the qualifying feature "an act committed using information and telecommunications networks, including the Internet, or using artificial intelligence systems" be included in separate articles on crimes against intellectual property.
Ключевые слова: уголовная ответственность, интеллектуальная собственность, искусственный интеллект, интеллектуальные права, посягательства на интеллектуальную собственность	**Keywords:** criminal liability; intellectual property; artificial intelligence; intellectual rights; infringement of intellectual property
ТЫДЫКОВА Надежда Владимировна, доцент кафедры уголовного права и криминологии Алтайского государственного университета, кандидат юридических наук, доцент	**TYDYKOVA Nadezhda Vladimirovna,** Associate Professor of the Department of criminal law and criminology of Altai State University, Candidate of Law, Associate Professor
ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПОЛОВЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ДИСТАНЦИОННЫМ СПОСОБОМ	**FEATURES OF THE QUALIFICATION OF SEXUAL CRIMES COMMITTED REMOTELY**
Статья посвящена исследованию особенностей квалификации половых преступлений, совершаемых с использованием информационно-телекоммуникационных сетей. Отмечается, что такой способ не является фактором, существенно повышающем общественную опасность этих преступлений, соответственно, не требует выделения в отдельный квалифицирующий признака. Называются правила установления знания	The article is devoted to the study of the characteristics of the qualification of sexual crimes committed using information and telecommunication networks. It is noted that such a method is not a factor that significantly increases the public danger of these crimes, accordingly, it does not require identification in qualifying signs. The rules for establishing the knowledge of the age of the victim by the perpetrator are called, the spe-

виновным возраста потерпевшего, рассмотрена специфика проявления признаков соучастия в таких преступлениях, отмечена необходимость в ряде случаев квалификации таких деяний по совокупности с другими преступлениями. **Ключевые слова:** развратные действия, действия сексуального характера, понуждение к действиям сексуального характера, информационно-телекоммуникационные сети, интернет	cifics of the manifestation of signs of complicity in such crimes are considered, the need in some cases for the qualification of such acts in combination with other crimes is noted. **Keywords:** indecent acts, acts of a sexual nature, compulsion to act of a sexual nature, information and telecommunication networks, the Internet
ФЕДОТОВА Кристина Александровна, помощник прокурора Катайского района прокуратуры Курганской области **ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ДЛЯ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ** В статье рассматриваются некоторые проблемы уголовной ответственности за совершение преступлений с использованием информационно-телекоммуникационных сетей. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за совершение преступлений с использованием информационно-телекоммуникационных сетей. **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», преступления против личности, стриминговые площадки	**FEDOTOVA Kristina Alexandrovna,** Assistant prosecutor of the Kataysky district of the prosecutor's office of the Kurgan region **THE USE OF INFORMATION AND TELECOMMUNICATION NETWORKS FOR THE COMMISSION OF CRIMES** The article discusses some problems of criminal liability for the commission of crimes using information and telecommunication networks to commit crimes. Proposals have been developed to improve the practice of applying criminal legislation on liability for the commission of crimes using information and telecommunication networks to commit crimes. **Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet, crimes against the person, streaming platforms
ФИРСОВ Виталий Викторович, доцент кафедры государственно-правовых дисциплин Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **УГОЛОВНО-ПРАВОВАЯ ЗАЩИТА КОНСТИТУЦИОННЫХ ПРАВ ГРАЖДАН В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ**	**FIRSOV Vitaly Viktorovich,** Associate Professor of the Department of state and legal disciplines of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor **CRIMINAL LAW PROTECTION OF THE CONSTITUTIONAL RIGHTS OF CITIZENS IN THE FIELD OF HIGH TECHNOLOGY**

В статье рассматриваются некоторые проблемы уголовно-правовой защиты конституционных прав граждан в сфере высоких технологий. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за преступления, совершаемые против конституционных прав граждан в сфере высоких технологий. **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	The article discusses some problems of criminal law protection of constitutional rights of citizens in the field of high technology. Proposals have been developed to improve the practice of applying criminal legislation on liability for crimes in the field of constitutional rights of citizens in the field of high technology. **Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet
ХОВАНОВ Илья Сергеевич, аспирант Орловского государственного университета имени И.С. Тургенева **РОЛЬ ПРОКУРАТУРЫ В ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИЗМУ В СЕТИ «ИНТЕРНЕТ»** В статье рассмотрена роль прокуратуры Российской Федерации в противодействии экстремизму в сети «Интернет». Представлен анализ основных полномочий и направлений деятельности прокуратуры по профилактике, выявлению и пресечению экстремистской деятельности. Отмечены проблемы, возникающие в ходе мониторинга сети «Интернет» на предмет выявления экстремистских материалов. Предложены пути совершенствования мониторинга запрещенных материалов в сети. **Ключевые слова:** прокуратура, экстремизм, противодействие, субъект, полномочия, интернет	**KHOVANOV Ilya Sergeevich,** Postgraduate student of I.S. Turgenev Oryol State University **THE ROLE OF THE PROSECUTOR'S OFFICE IN COUNTERING EXTREMISM ON THE INTERNET** The article considers the role of the Prosecutor's Office of the Russian Federation in countering extremism on the Internet. The analysis of the main powers and directions of activity of the prosecutor's office on prevention detection and suppression of extremist activity is presented. The problems arising in the course of monitoring the Internet for detection of extremist materials are noted. Ways to improve the monitoring of prohibited materials on the Internet are proposed. **Keywords:** prosecutor's office, extremism, counteraction, subject, powers, internet
ХОЛОПОВ Алексей Васильевич, заведующий криминалистической лабораторией Санкт-Петербургского юридического института (филиал) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ВИЗУАЛИЗАЦИИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО**	**KHOLOPOV Alexey Vasilyevich,** Head of the Forensic Laboratory of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation, Candidate of Law, Associate Professor **MODERN POSSIBILITIES FOR VISUALIZING CRIMINAL ACTIVITIES COMMITTED USING MASS MEDIA OR ELECTRONIC OR INFORMATION AND TELECOMMUNICATION NETWORKS**

ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ Статья посвящена применяемым, как на досудебных, так и судебных стадиях уголовного судопроизводства, современным технологиям визуализации преступной деятельности, осуществляемой с использованием электронных или информационно-телекоммуникационных сетей. Автор рассматривает возможности отечественного специального программного обеспечения «Следопыт» и «Октопус», используемого в рамках информационно-аналитической экспертизы по визуализации результатов анализа больших массивов данных, например, компьютерной (цифровой) информации о деятельности преступника (преступников), как на отдельном цифровом устройстве (компьютер, планшет, смартфон, роутер и т. д.), так и на сетевых ресурсах. **Ключевые слова:** визуализация, наглядность, систематизация, информационно-аналитическая экспертиза, событие преступления, познание преступления	The article is devoted to modern technologies used both at the pre-trial and judicial stages of criminal proceedings for visualizing criminal activities committed using electronic or information and telecommunication networks. The author considers the capabilities of domestic special software “Pathfinder”, “Octopus”, used as part of information and analytical expertise to visualize the results of the analysis of large amounts of data, for example, computer (digital) information about the activities of a criminal (criminals), as on a separate digital device (computer, tablet, smartphone, router, etc.) and on network resources. **Keywords:** visualization, visibility, systematization, information and analytical expertise, crime event, knowledge of crime
ЦВЕТКОВ Павел Валерьевич, старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия **ДРУК Ирина Дмитриевна,** студент Северо-Западного филиала Российского государственного университета правосудия **КИБЕРПРЕСТУПЛЕНИЯ: ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ И КВАЛИФИКАЦИИ** В статье рассматриваются некоторые проблемы, связанные с понятиями и квалификацией преступлений, совершаемых в компьютерной сфере, не являющихся преступлениями, предусмотренными главой 28 УК РФ. Разработаны предложения по совершенствованию уголовного законодательства по усилению ответственности за совершение преступлений, совершаемых в компьютерной сфере.	**TSVETKOV Pavel Valerievich,** Senior lecturer at the Department of criminal law of the North-Western Branch of the Russian State University of Justice **DRUK Irina Dmitrievna,** student of the North-Western Branch of the Russian State University of Justice **CYBERCRIMES: PROBLEMS OF DEFINITION AND QUALIFICATION** The article discusses some problems of definition and qualification of cybercrimes that are not provided for as crimes by the 28th Chapter of the Criminal Code of the Russian Federation. Proposals have been developed to improve the practice of applying criminal legislation to strengthen responsibility for cybercrimes as crimes committed in the computer sphere.

Ключевые слова: понятие киберпреступления, виртуальное пространство, квалификация преступления	**Keywords:** the concept of cybercrime, virtual space, crime qualification
ЧИХРАДЗЕ Анна Михайловна, доцент кафедры уголовного права и процесса Донецкого государственного университета, кандидат юридических наук **ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК СРЕДСТВА СОВЕРШЕНИЯ ПРОВОКАЦИОННЫХ ДЕЙСТВИЙ ПОТЕРПЕВШИМ В КОНТЕКСТЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА УБИЙСТВО, СОВЕРШЕННОЕ В СОСТОЯНИИ АФФЕКТА** В статье рассмотрены особенности уголовно-правовой характеристики использования электронных и информационно-телекоммуникационных сетей в механизме совершения преступления «убийство, совершенное в состоянии аффекта». Исследованы особенности квалификации действий субъекта преступления, предусмотренного ст. 107 УК РФ, в случаях использования потерпевшим электронных и информационно-телекоммуникационных сетей как средства совершения провокационных действий. Предложено определение термина «кибербуллинг» как формы поведения потерпевшего, выделены его основные юридически значимые признаки, имеющие значение для квалификации содеянного. **Ключевые слова:** потерпевший, насилие, издевательство, оскорбление, кибербуллинг	**CHIKHRADZE Anna Mikhailovna,** Associate professor of the Department of criminal law and procedure at Donetsk State University, Candidate of Science (Law) **THE USE OF ELECTRONIC AND INFORMATION AND TELECOMMUNICATION NETWORKS AS A MEANS OF COMMITTING PROVOCATIVE ACTIONS BY VICTIMS IN THE CONTEXT OF CRIMINAL LIABILITY FOR MURDER COMMITTED IN A STATE OF PASSION** The article considers the features of the criminal law characteristics of the use of electronic and information and telecommunication networks in the mechanism of committing the crime of "murder committed in a state of passion". The features of the qualification of the actions of the subject of the crime under Article 107 of the Criminal Code of the Russian Federation in cases of the use of electronic and information and telecommunication networks by the victim as a means of committing provocative actions are investigated. The definition of the term "cyberbullying" as a form of victim behavior is proposed, its main legally significant features that are important for the qualification of the deed are highlighted. **Keywords:** victim, violence, bullying, insult, cyberbullying
ШУТОВА Юлия Александровна, адъюнкт Санкт-Петербургского университета МВД России **К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА УГРОЗУ УБИЙСТВОМ ИЛИ ПРИЧИНЕНИЕМ ТЯЖКОГО ВРЕДА ЗДОРОВЬЮ, СОВЕРШЕННУЮ В СЕТИ «ИНТЕРНЕТ»** В статье рассматриваются отдельные вопросы практической реализации уголовно-	**SHUTOVA Yulia Alexandrovna,** Associate Professor at the St. Petersburg University of the Ministry of Internal Affairs of Russia **ON THE ISSUE OF CRIMINAL LIABILITY FOR THREATENING TO KILL OR CAUSE SERIOUS HARM TO HEALTH COMMITTED ON THE INTERNET** The article deals with certain issues of practical implementation of the criminal law norm

правовой нормы, предусмотренной ст. 119 УК РФ, в целях противодействия угрозам убийством, выраженным в сети «Интернет». Автор приводит положения уголовно-правовой доктрины в части оценки эффективной реализации уголовно-правовой нормы. Аргументируется позиция о необходимости своевременного и эффективного реагирования на новые формы выражения угрозы убийством с учетом имеющегося охранительного потенциала уголовно-правовой нормы.	provided for in Article 119 of the Criminal Code of the Russian Federation in order to counter death threats expressed on the Internet. The author cites the provisions of the criminal law doctrine regarding the assessment of the effective implementation of the criminal law norm. The position on the need for a timely and effective response to new forms of expression of the threat of murder, taking into account the existing protective potential of the criminal law norm, is argued.
Ключевые слова: угроза убийством или причинением тяжкого вреда здоровью, сеть «Интернет», психическое насилие, эффективная реализация уголовно-правовой нормы, психическое и социальное здоровье	**Keywords**: threat of murder or causing serious harm to health, the Internet, mental violence, effective implementation of criminal law norms, mental and social health
ЮРКОВ Сергей Александрович, доцент кафедры уголовного права, процесса и национальной безопасности Вятского государственного университета, кандидат юридических наук, доцент	**YURKOV Sergey Alexandrovich,** Associate professor of the Department of criminal law, procedure and national security of Vyatka State University, Candidate of Science (Law), Associate professor
НЕКОТОРЫЕ АСПЕКТЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА НАРУШЕНИЕ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ	**SOME ASPECTS OF CRIMINAL RESPONSIBILITY FOR VIOLATION OF PRIVACY**
Предметом исследования является практика применения ст. 137 УК РФ. В работе отражен анализ судебной практики по применению данной статьи УК РФ. В частности, показано, в чем чаще всего выражается собирание и распространение сведений о частной жизни лица. Установлено, что чаще всего предметом данного преступления являются сведения об интимной жизни. Местом совершения преступления является сеть «Интернет» и иные информационно-телекоммуникационные ресурсы. Отдельно рассмотрен вопрос о несовершенстве состава преступления, предусмотренного ч. 3 ст. 137 УК РФ.	The subject of the study is the practice of applying Article 137 of the Criminal Code of the Russian Federation. The paper reflects the analysis of judicial practice on the application of this article of the Criminal Code of the Russian Federation. In particular, it shows how the collection and dissemination of information about a person's private life is most often expressed. It is established that most often the subject of this crime is data about intimate life. The place of commission of the crime is the Internet and other information and telecommunication resources. The issue of the imperfection of the corpus delicti provided for in part 3 of article 137 of the Criminal Code of the Russian Federation is considered separately.
Ключевые слова: частная жизнь; тайна; неприкосновенность; распространение	**Keywords:** private life; secrecy; inviolability; distribution

АБДУЛКАДИРОВ Али Абдулкадирович, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель \ **АБДУЛАЗИЗОВА Патимат Гасановна,** доцент кафедры государственно-правовых дисциплин, Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России)**,** кандидат юридических наук	**ABDULKADIROV Ali Abdulkadirovich,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **ABDULAZIZOVA Patimat Hasanovna,** Associate Professor of the Department of state and legal disciplines, North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Candidate of Law
ТРЕШ-СТРИМИНГ КАК СОЦИАЛЬНО ОПАСНОЕ ЯВЛЕНИЕ В СЕТИ «ИНТЕРНЕТ» В статье рассмотрены наиболее актуальные вопросы, связанные с противодействием социально-деструктивному поведению в сети, прежде всего совершаемому в рамках треш-стримов. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за совершение преступлений против личности в сети «Интернет». **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», треш-стрим	**TRASH STREAMING AS A SOCIALLY DANGEROUS PHENOMENON ON THE INTERNET** The article discusses the most pressing issues related to countering socially destructive behavior on the web, primarily committed within the framework of trash streams. Proposals have been developed to improve the practice of applying criminal legislation on the responsibility of committing crimes against the person on the Internet. **Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet, trash stream
АГАРКОВА Анастасия Павловна, курсант Санкт-Петербургского университета МВД России научный руководитель **АЛЕШИНА-АЛЕКСЕЕВА Екатерина Николаевна,** старший преподаватель кафедры уголовного права Санкт-Петербургского университета МВД России	**AGARKOVA Anastasia Pavlovna,** cadet of the St. Petersburg University of the Ministry of Internal Affairs of Russia scientific supervisor **ALYOSHINA-ALEKSEEVA Ekaterina Nikolaevna,** Senior Lecturer at the Department of Criminal Law of the St. Petersburg University of the Ministry of Internal Affairs of Russia
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ СУБЪЕКТОВ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)	**CRIMINAL LIABILITY OF SUBJECTS OF CRIMES COMMITTED USING MASS MEDIA OR ELECTRONIC INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)**

В работе рассмотрены детерминанты и особенности преступлений, совершенных с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»). Авторами сделана попытка затронуть вопрос возраста субъекта преступлений, совершенных с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»). **Ключевые слова:** уголовная ответственность, субъект преступления, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	The paper considers the determinants and features of crimes committed using mass media or electronic information and telecommunication networks (including the Internet). The authors attempt to address the issue of the age of the subject of crimes committed using mass media or electronic information and telecommunication networks (including the Internet). **Keywords:** criminal liability, the subject of the crime, the use of information and telecommunication networks, including the Internet
АДАМОВИЧ Вячеслав Владимирович, слушатель Санкт-Петербургского университета МВД России научный руководитель **ОГАРЬ Татьяна Андреевна,** начальник кафедры уголовного права Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент **ВОПРОСЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ, ПРЕДУСМОТРЕННОЙ ЗА СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ** В статье рассматриваются актуальные проблемы применения нормы, предусмотренной ст. 273 УК РФ. Исследуется вопрос о необходимости включения в диспозицию ст. 273 УК РФ такого признака объективной стороны, как «приобретение» вредоносной компьютерной программы. Также анализируется вопрос относительно субъективной стороны состава преступления, предусмотренного ст. 273 УК РФ, в части формы вины. **Ключевые слова:** вредоносная программа, компьютерная информация, блокирование, уничтожение, модификация, копирование	**ADAMOVICH Vyacheslav Vladimirovich,** A student at the St. Petersburg University of the Ministry of Internal Affairs of Russia scientific supervisor **OGAR Tatyana Andreevna,** Head of the Department of Criminal Law of the St. Petersburg University of the Ministry of Internal Affairs of Russia, Candidate of Science (Law), Associate Professor **ISSUES OF CRIMINAL LIABILITY FOR THE CREATION OF, THE USE AND DISTRIBUTION OF MALWARE COMPUTER PROGRAMS** This article discusses current problems of applying the norm provided for in Art. 273 of the Criminal Code of the Russian Federation. The question is raised about the need to include in the disposition of Art. 273 of the Criminal Code of the Russian Federation such a sign of the objective side as the «acquisition» of a malicious computer program. The question regarding the subjective side of the crime under Art. 273 of the Criminal Code of the Russian Federation regarding the form of guilt. **Keywords:** malware, computer information, blocking, destruction, modification, copying

АДОВСКОВА Александра Дмитриевна, ГРИЦАЕВА Ольга Сергеевна, студенты Северо-Западного филиала Российского государственного университета правосудия научные руководители **ДВОРЖИЦКАЯ Марина Андреевна,** старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук; **ПИСАРЕВСКАЯ Елена Анатольевна,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**ADOVSKOVA Alexandra Dmitrievna, GRITSAEVA Olga Sergeevna,** students of the Northwestern Branch of the Russian State University of Justice scientific supervisors **DVORZHITSKAYA Marina Andreevna,** Senior Lecturer of the Department of Criminal Law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law); **PISAREVSKAYA Elena Anatolyevna,** Associate Professor of the Department of criminal law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor
МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ	**FRAUD IN THE FIELD OF COMPUTER INFORMATION: CRIMINOLOGICAL CHARACTERISTICS AND PROBLEMS OF COUNTERACTION**
В статье анализируются количественные и качественные показатели такого вида хищения, совершаемого в последние годы в Российской Федерации, как мошенничество с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. Авторами выявлены и обозначены негативные тенденции данного вида преступности. В статье указывается на колоссальный ущерб, причиняемый физическим лицам, особенно незащищенным категориям граждан, отмечается очевидная латентность анализируемых видов мошенничеств.	The article analyzes quantitative and qualitative indicators of such type of theft as fraud using information and communication technologies or in the field of computer information in recent years in the Russian Federation. The authors identify and identify negative trends in this type of crime. The article points to the enormous damage caused by their commission, which is caused to individuals, especially to unprotected categories of citizens, and the obvious latency of the analyzed types of fraud is noted.
Ключевые слова: мошенничество, показатели преступности, информационно-коммуникационные технологии, компьютерная информация, противодействие	**Keywords:** fraud, crime rates, information and communication technologies, computer information, counteraction
АЛФЕЕВА Виктория Сергеевна, студент Института права Челябинского государственного университета научный руководитель **КАДЫРОВА Надежда Николаевна,** доцент кафедры уголовно-правовых дисци-	**ALFEYEVA Victoria Sergeevna,** student of the Institute of Law of Chelyabinsk State University scientific supervisor **KADYROVA Nadezhda Nikolaevna,** Associate Professor of the Department of criminal

плин Челябинского государственного университета, кандидат юридических наук, доцент	law disciplines of Chelyabinsk State University, Candidate of Science (Law), Associate Professor
ДЕТЕРМИНАНТЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО ЧАСТЬЮ 2 СТАТЬИ 280 УК РФ	**DETERMINANTS OF THE COMMISSION OF A CRIME UNDER PART 2 OF ARTICLE 280 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
В статье рассматриваются детерминанты публичных призывов, осуществляемых с использованием сети «Интернет», к экстремистской деятельности. Выделены основные факторы, влияющие на совершение данного деяния, проанализированы основные средства совершения данного вида преступлений, а также предложена мера по предупреждению данных действий.	The article examines the determinants of public calls for extremist activity using the Internet. The main factors influencing the commission of this act are highlighted, the main means of committing this type of crimes are analyzed, as well as a measure to prevent these actions is proposed.
Ключевые слова: экстремистская деятельность, детерминанты, информационно-телекоммуникационная сеть «Интернет»	**Keywords:** extremist activity, determinants, the Internet
БАРСУКОВА Анастасия Вячеславовна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **БЕЗБОРОДОВ Дмитрий Анатольевич,** профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**BARSUKOVA Anastasia Viacheslavovna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **BEZBORODOV Dmitry Anatolyevich,** Professor of the Department of Criminal Law, criminology and penal enforcement law of the St. Petersburg Law Institute (Faculty) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor
ПРИЗНАКИ ОБЪЕКТИВНОЙ СТОРОНЫ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 159.6 УК РФ	**SIGNS OF THE OBJECTIVE SIDE OF THE CRIME UNDER ARTICLE 159.6 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
В статье рассматриваются признаки объективной стороны мошенничества в сфере компьютерной информации. Проанализировано уголовное законодательство России, в том числе в прошлых редакциях, и иные нормативные правовые акты в части указания на признаки объективной стороны преступления, предусмотренного ст. 159.6 УК РФ. Изучена также правоприменительная практика. Разработаны предложения по	The article discusses the signs of the objective side of fraud in the field of computer information. The article analyzes the criminal legislation of Russia, including in previous editions and other regulatory legal acts in terms of indicating the signs of the objective side of the crime provided for in Article 159.6 of the Criminal Code of the Russian Federation. The law enforcement practice has also been studied. Proposals have been developed to improve

совершенствованию статьи 159.6 УК РФ, предусматривающей ответственность за мошенничество в сфере компьютерной информации. **Ключевые слова:** мошенничество, объективная сторона, хищение, компьютерная информация, характер и степень общественной опасности	Article 159.6 of the Criminal Code of the Russian Federation, providing for liability for fraud in the field of computer information. **Keywords**: fraud, objective side, theft, computer information, nature and degree of public danger
БЕЗУГЛОВА Юлия Сергеевна, студент магистратуры Северо-Западного филиала Российского государственного университета правосудия научный руководитель **БЕРЕСТОВОЙ Андрей Николаевич,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент **ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ** В статье рассматриваются особенности преступлений в сфере компьютерной информации. Приводятся характеристики некоторых компьютерных преступлений, включенных в главу 28 УК РФ. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за преступления в сфере компьютерной информации. **Ключевые слова:** компьютерная информация, правовое регулирование, уголовная ответственность, уголовное законодательство, киберпреступление	**BEZUGLOVA Yulia Sergeevna,** Graduate student at the North-Western Branch of the Russian State University of Justice scientific supervisor **BERESTOVOI Andrey Nikolaevich,** Associate Professor of the Department of Criminal Law of the Northwestern Branch of the Russian State University of Justice, Candidate of Law, Associate Professor **CHARACTERISTICS OF CRIMES IN THE FIELD OF COMPUTER INFORMATION** The article examines the features of crimes in the field of computer information. The characteristics of some computer crimes included in Chapter 28 of the Criminal Code of the Russian Federation are given. Proposals have been developed to improve the practice of applying criminal legislation on liability for crimes in the field of computer information. **Keywords:** computer information, legal regulation, criminal liability, criminal legislation, cybercrime
БИСУЛТАНОВА Милана Ширваниевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института	**BISULTANOVA Milana Shirvanievna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian

(филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	Federation, Candidate of Science (Law), Associate Professor
СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ» КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ	**COMMITTING A CRIME USING THE INTERNET AS A WAY TO COMMIT A CRIME**
В статье рассматриваются некоторые проблемы уголовной ответственности, предусмотренной за совершение преступления с использованием сети «Интернет». Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за совершение преступления с использованием сети «Интернет».	The article discusses some problems of criminal liability for committing a crime using the Internet. Proposals have been developed to improve the practice of applying criminal legislation on liability for committing a crime using the Internet.
Ключевые слова: квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	**Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet
БОРОВИКОВ Владимир Витальевич, СТОЛЯРСКИЙ Егор Вадимович, студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ФЕДЫШИНА Полина Викторовна**, старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, советник юстиции	**BOROVIKOV Vladimir Vitalievich, STOLYARSKY Egor Vadimovich,** Students of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **FEDYSHINA Polina Viktorovna,** Senior Lecturer of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Adviser of Justice
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ», КАК СПОСОБ СОВЕРШЕНИЯ РАЗВРАТНЫХ ДЕЙСТВИЙ	**USE OF INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET, AS A WAY OF COMMITTING DEPRAVED ACTS**
В данной статье рассматриваются вопросы общественной опасности развратных действий, совершенных с помощью информационно-телекоммуникационных сетей, разграничение статьи 135 УК РФ и статьи 242 УК РФ, отграничение статьи 135 УК РФ от	This article discusses the issues of public danger of depraved acts committed using information and telecommunication networks, the differentiation of Article 135 of the Criminal Code and Article 242 of the Criminal Code, the delimitation of Article 135 of the

статьи 132 УК РФ, особенности квалификации развратных действий, совершенных посредством использования информационно-телекоммуникационных сетей. **Ключевые слова:** развратные действия, онлайн-груминг, информационно-телекоммуникационные системы	Criminal Code from Article 132 of the Criminal Code, the specifics of the qualification of depraved acts committed through the use of information and telecommunication networks. **Keywords:** depraved acts, online grooming, information and telecommunication systems
ВАЖЕНИНА Маргарита Витальевна, курсант Санкт-Петербургского университета Российской Федерации научный руководитель **АЛЕШИНА-АЛЕКСЕЕВА Екатерина Николаевна,** старший преподаватель кафедры уголовного права Санкт-Петербургского университета МВД России **КИБЕРПРЕСТУПЛЕНИЯ: ПОНЯТИЕ, ВИДЫ, ОСОБЕННОСТИ КВАЛИФИКАЦИИ** В статье обращается внимание на то, что динамическое развитие общества, цифровой сферы и технологий породило новый вид преступлений, а также способы их совершения. Разработаны предложения по совершенствованию противодействия киберпреступности **Ключевые слова:** киберпреступность, информация, информационно-телекоммуникационные средства, сетевая безопасность, кибервымогательство, кибермошенничество, фишинг	**VAZHENINA Margarita Vitalievna,** Cadet of St. Petersburg University of the Russian Federation scientific supervisor **ALYOSHINA-ALEKSEEVA Ekaterina Nikolaevna,** Senior Lecturer at the Department of criminal law of the St. Petersburg University of the Ministry of Internal Affairs of Russia **CYBERCRIMES: THE CONCEPT, TYPES, CHARACTERISTICS OF QUALIFICATIONS** The article draws attention to the fact that the dynamic development of society, the digital sphere and technology has given rise to a new type of crime, as well as ways of committing them. Proposals have been developed to improve counteraction to cybercrime. **Keywords:** cybercrime, information, information and telecommunication means, network security, cyber extortion, cyber fraud, phishing
ГАБИБОВА Эльвира Галибовна, **КОЛОШИНА Екатерина Викторовна,** студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**GABIBOVA Elvira Gotlibovna,** **KALOSHINA Ekaterina Viktorovna,** Students of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor

ПРОБЛЕМЫ КВАЛИФИКАЦИИ РАЗВРАТНЫХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»	**PROBLEMS OF QUALIFICATION OF DEPRAVED ACTS COMMITTED USING THE INTERNET**
В статье рассматриваются некоторые проблемы уголовной ответственности за развратные действия, совершаемые с использованием сети «Интернет». Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за развратные действия, совершаемые с использованием сети «Интернет».	The article discusses some problems of criminal liability for depraved acts committed using the Internet. Proposals have been developed to improve the practice of applying criminal legislation on liability for depraved acts committed using the Internet.
Ключевые слова: квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», развратные действия	**Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet, depraved actions
ГАДЖИЕВА Асият Гаджиевна, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель **РАМАЗАНОВА Пати Казихановна,** заведующий кафедрой гуманитарных и социально-экономических дисциплин Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции, кандидат филологических наук, доцент	**HAJIYEVA Asiyat Hajiyevna,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **RAMAZANOVA Pati Kazikhanovna,** Head of the Department of humanities and socio-economic disciplines of the North Caucasus Institute (branch) All-Russian State University of Justice, Candidate of Science (Philological), Associate Professor
ПАРТНЕРСТВО СБЕРБАНКА И УНИВЕРСИТЕТА МВД РОССИИ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ	**PARTNERSHIP BETWEEN SBERBANK AND THE UNIVERSITY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA IN THE FIGHT AGAINST CYBERCRIME**
В статье рассматриваются отдельные направления работы Департамента безопасности ПАО Сбербанк по совершенствованию подготовки сотрудников органов внутренних дел в области предотвращения, раскрытия и расследования киберпреступлений. Отдельное внимание уделено анализу позитивного опыта взаимодействия с Московским университетом МВД России имени В.Я. Кикотя.	The article discusses certain areas of work of the Security Department of Sberbank PJSC on improving the training of employees of internal affairs bodies in the field of prevention, disclosure and investigation of cybercrime are considered. Special attention is paid to the analysis of the positive experience of interaction with the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot.

Ключевые слова: киберпреступления, компьютерные преступления, расследование компьютерных преступлений, расследование киберпреступлений, взаимодействие государства и бизнеса, совершенствование подготовки полиции	**Keywords:** cybercrimes, computer crimes, investigation of computer crimes, investigation of cybercrimes, interaction between the state and business, improvement of police training
ГАРАЕВА Юлия Андреевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ФЕДЫШИНА Полина Викторовна,** старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации	**GARAEVA Yulia Andreevna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **FEDYSHINA Polina Viktorovna,** Senior Lecturer at the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (Faculty) University of prosecutor's office of the Russian Federation
ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 207.3 УК РФ, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ СМИ	**PROBLEMS OF QUALIFICATION OF A CRIME UNDER ARTICLE 207.3 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION COMMITTED USING THE MEDIA**
Статья посвящена актуальным вопросам применения статьи 207.3 УК РФ при квалификации деяний лиц в их тесной взаимосвязи с объективными признаками состава рассматриваемого преступления и особенностями субъекта, его совершающего. Автор акцентирует внимание на актуальности данной темы в рамках современной геополитической обстановки, анализирует основные положения, мнение отдельных представителей научного сообщества, судебную практику. Высказываются варианты разрешения проблем, возникающих при квалификации общественно опасных деяний.	The article is devoted to topical issues of the application of Article 207.3 of the Criminal Code of the Russian Federation in the qualification of acts of persons in their close relationship with objective signs of the composition of the crime in question and the characteristics of the subject committing it. The author focuses on the relevance of this topic in the context of the modern geopolitical situation, analyzes the main provisions, the opinion of individual representatives of the scientific community, and judicial practice. There are options for solving problems arising in the qualification of socially dangerous acts.
Ключевые слова: публичное распространение, заведомо ложная информация, Вооруженные Силы Российской Федерации, признаки объективной стороны преступления, блогер, военный корреспондент, средства массовой информации	**Keywords:** public dissemination, deliberately false information, the Armed Forces of the Russian Federation, signs of the objective side of the crime, blogger, war correspondent, mass media
МАТВЕЕВ Даниил Владимирович, студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации	**MATVEEV Daniil Vladimirovich,** Students of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation

научный руководитель **ШАРАПОВ Роман Дмитриевич,** профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, профессор	scientific supervisor **SHARAPOV Roman Dmitrievich,** Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Doctor of Science (Law), Professor
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ (СТАТЬЯ 274.2 УК РФ)	**CRIMINAL LIABILITY FOR VIOLATION OF THE RULES OF CENTRALIZED MANAGEMENT OF TECHNICAL MEANS OF COUNTERING THREATS (ARTICLE 274.2 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)**
В статье рассматриваются положения ст. 274.2 УК РФ. Авторы выявляют ряд проблем, которые могут возникнуть в процессе применения ст. 274.2 УК РФ, а также анализируют обоснованность криминализации рассматриваемого деяния. Отмечается необходимость отражения в диспозиции статьи конкретных последствий нарушения правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.	The paper discusses the provisions of Article 274.2 of the Criminal Code of the Russian Federation. The authors identify a number of problems that may arise during the application of Article 274.2 of the Criminal Code of the Russian Federation, and also analyze the validity of criminalization of the act under consideration. The necessity of reflecting in the disposition of the article the specific consequences of violations of the rules of centralized management of technical means of countering threats to the stability, security and integrity of functioning on the territory of the Russian Federation of the information and telecommunications network "Internet" and the public communication network is noted.
Ключевые слова: цифровой суверенитет, информационная безопасность, компьютерные преступления, технические средства противодействия угрозам, информационно-телекоммуникационные сети, статья 274.2 УК РФ	**Keywords:** digital sovereignty, information security, computer crimes, technical means of countering threats, information and telecommunication networks, article 274.2 of the Criminal Code of the Russian Federation
ГОРДИЕНКО Кира Николаевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ФЕДЫШИНА Полина Викторовна,** старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации	**GORDIENKO Kira Nikolaevna,** student of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation scientific supervisor **FEDYSHINA Polina Viktorovna,** Senior Lecturer at the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation

КВАЛИФИКАЦИЯ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ (НА ПРИМЕРЕ П. «Б» Ч. 2 СТ. 228.1 УК РФ)	**QUALIFICATION OF THE ILLEGAL SALE OF NARCOTIC DRUGS (USING THE EXAMPLE OF P. «B» PART 2 OF ART. 228.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)**
В статье анализируются вопросы, связанные с квалификацией незаконного сбыта наркотических средств и психотропных веществ с использованием сети «Интернет». Предлагается возможный вариант решения основных проблем, приводятся примеры ошибочного вменения данного квалифицирующего признака с учетом правоприменительной практики.	The article analyzes the issues related to the qualification of the illegal sale of narcotic drugs and psychotropic substances using the Internet. A possible solution to the main problems is proposed, and examples of erroneous imputation of this qualifying feature are given, taking into account law enforcement practice.
Ключевые слова: сбыт, сеть «Интернет», бесконтактный способ, сбыт из рук в руки, бесконтактный способ, наркополучатель, наркосбытчик	**Keywords:** sales, Internet network, contactless method, hand-to-hand sales, contactless method, drug recipient, drug collector
ГРИБАНОВА Юлия Евгеньевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**GRIBANOVA Yulia Evgenievna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor
ЭЛЕКТРОННЫЙ ДОКУМЕНТ КАК ПРЕДМЕТ ПОДЛОГА	**AN ELECTRONIC DOCUMENT AS THE SUBJECT OF FORGERY**
В статье раскрывается понятие официального электронного документа, анализируются возможности и пределы его правового регулирования, уголовно-правовой охраны. Автор обосновывает вывод о том, что официальный электронный документ является самостоятельным предметом преступлений о подлоге документа.	The article reveals the concept of an official electronic document, analyzes the possibilities and limits of its legal regulation, criminal law protection. The author substantiates the conclusion that the official electronic document is an independent subject of crimes of forgery of the document.
Ключевые слова: электронный документ, официальный документ, подлог	**Keywords:** electronic document, official document, forgery
ДАРШТ Яна Романовна, курсант Санкт-Петербургского университета МВД России	**DARSHT Yana Romanovna,** Cadet of the St. Petersburg University of the Ministry of Internal Affairs of Russia

научный руководитель **ВАСИЛЬЕВ Федор Юрьевич,** доцент кафедры уголовного процесса Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент	scientific supervisor **VASILIEV Fedor Yurievich,** Associate Professor of the Department of criminal procedure at the St. Petersburg University of the Ministry of Internal Affairs of Russia, Candidate of Science (Law), Associate Professor
ПРОБЛЕМЫ КВАЛИФИКАЦИИ СОВРЕМЕННОЙ КИБЕРПРЕСТУПНОСТИ: ДОКСИНГ	**PROBLEMS OF QUALIFICATION OF MODERN CYBERCRIME: DOXING**
Одним из современных разновидностей киберпреступности является доксинг. Статья посвящена проблеме квалификации данного деяния, направленного на незаконное распространение личных данных лица без его согласия в целях опорочить это лицо или получить прибыль. Исследованы вопросы содержания и характеристики доксинга, отграничения его от сходных обстоятельств, включения его в главу 19 УК РФ. Разработаны предложения по квалификации данного деяния и по совершенствованию уголовного законодательства.	One of the modern varieties of cybercrime is doxing. The article is devoted to the problem of the qualification of this act aimed at the illegal dissemination of personal data without the consent of a person in order to defame him or make a profit. The issues of the content and characteristics of doxing, delineation from similar circumstances, its inclusion in Chapter 19 of the Criminal Code of the Russian Federation are investigated. Proposals have been developed for the qualification of this act and the improvement of criminal legislation.
Ключевые слова: Интернет, доксинг, киберугроза, персональные данные, конфиденциальная информация, ответственность	**Keywords:** Internet, doxing, cyber threat, personal data, confidential information, responsibility
ДАУДОВА Ашура Рамазановна, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель **АБДУЛАЗИЗОВА Патимат Гасановна,** преподаватель кафедры государственно-правовых дисциплин Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук	**DAUDOVA Ashura Ramazanovna,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **ABDULAZIZOVA Patimat Hasanovna,** lecturer at the Department of state and legal disciplines of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Candidate of Science (Law)
МЕСТО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННОМ УГОЛОВНОМ ПРАВЕ	**THE PLACE OF ARTIFICIAL INTELLIGENCE IN MODERN CRIMINAL LAW**
Проблема определения места искусственного интеллекта в современном уголовном праве в настоящий момент приобретает особое значение в связи с появлением новых технологий, которые оказывают как	The problem of determining the place of artificial intelligence in modern criminal law is currently gaining special importance due to the emergence of new technologies that have both positive and negative effects on existing social

положительное, так и негативное влияние на существующие общественные отношения. В статье рассматриваются некоторые проблемы уголовной ответственности, предусмотренной за преступления, совершаемые с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».	relations. The article discusses some problems of criminal liability for crimes committed using information and telecommunication networks, including the Internet.
Ключевые слова: уголовная ответственность, искусственный интеллект, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	**Keywords:** criminal liability, artificial intelligence, use of information and telecommunication networks, including the Internet
ЗАЙЦЕВА Олеся Витальевна, студент магистратуры Северо-Западного филиала Российского государственного университета правосудия научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**ZAITSEVA Olesya Vitalievna,** Graduate student at the North-Western Branch of the Russian State University of Justice scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of Criminal Law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПУБЛИЧНЫЕ ПРИЗЫВЫ К ОСУЩЕСТВЛЕНИЮ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»	**CRIMINAL LIABILITY FOR PUBLIC CALLS TO CARRY OUT EXTREMIST ACTIVITIES COMMITTED USING THE INTERNET**
В статье рассматриваются некоторые проблемы уголовной ответственности, предусмотренной за публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием сети «Интернет». Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности за публичные призывы к осуществлению экстремистской деятельности, совершенные с использованием сети «Интернет».	The article discusses some problems of criminal liability for public calls for the implementation of extremist activities committed using the Internet. Proposals have been developed to improve the practice of applying criminal legislation on liability for public calls to carry out extremist activities committed using the Internet.
Ключевые слова: публичные призывы, средства массовой информации, информационно-телекоммуникационные сети, сеть «Интернет»	**Keywords:** public appeals, media, information and telecommunication networks, Internet

ЗАПЕВАЛОВА Варвара Александровна, ПУХОВА Милана Юрьевна, студенты Северо-Западного филиала Российского государственного университета правосудия научный руководитель **КРАСНОВА Кристина Александровна,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**ZAPEVALOVA Varvara Alexandrovna, PUKHOVA Milana Yuryevna,** Students of the North-Western Branch of the Russian State University of Justice scientific supervisor **KRASNOVA Kristina Alexandrovna,** Associate Professor of the Department of criminal law of the North-Western Branch of the Russian State University of Justice, Candidate of Legal Sciences, Associate Professor
ШАНТАЖ В СЕТИ «ИНТЕРНЕТ»: ПРОБЛЕМЫ РЕАЛИЗАЦИИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ	**BLACKMAIL ON THE INTERNET: PROBLEMS OF THE IMPLEMENTATION OF CRIMINAL RESPONSIBILITY**
В данной статье рассматриваются проблемы реализации уголовной ответственности за преступления, совершаемые посредством сети «Интернет». В частности, исследуется поведение преступников и жертв шантажа, осуществляемого посредством сети «Интернет». Приводится типичная модель развития событий при подготовке и реализации рассматриваемого преступления. Отдельное внимание в статье уделено законодательному регулированию рассматриваемой проблемы, предлагаются варианты ее решения.	This article discusses the problems of implementing criminal liability for crimes committed through the Internet. In particular, the behavior of criminals and victims of blackmail carried out through the Internet is being investigated. A typical model of the development of events in the preparation and implementation of the crime in question is given. Special attention is paid in the article to the legislative regulation of the problem under consideration, and options for its solution are proposed.
Ключевые слова: киберпреступность, сеть «Интернет», социальные сети, уголовная ответственность, шантаж	**Keywords:** cybercrime, the Internet, social networks, criminal liability, blackmail
ЗУЕВА Елизавета Андреевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **КРАЕВ Денис Юрьевич,** профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**ZUEVA Elizaveta Andreevna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **KRAEV Denis Yurievich,** Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor
НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ДОВЕДЕНИЕ ДО САМОУБИЙСТВА, СОВЕР-	**SOME PROBLEMS OF CRIMINAL LIABILITY FOR INCITEMENT TO SELF-MURDER COMMITTED IN A PUBLIC**

ШЕННОЕ В ПУБЛИЧНОМ ВЫСТУПЛЕНИИ, ПУБЛИЧНО ДЕМОНСТРИРУЮЩЕМСЯ ПРОИЗВЕДЕНИИ, СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)	**SPEECH, A PUBLICLY DEMONSTRATED WORK, THE MEDIA OR INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)**
В статье исследуются вопросы уголовно-правовой оценки доведения до самоубийства, совершенного в средствах массовой информации и информационно-телекоммуникационной сети «Интернет». Сравниваются статистические данные о совершенных актах суицида и обвинительных приговорах, вынесенных в отношении лиц, совершивших преступление, предусмотренное статьей 110 УК РФ. Дается квалификация доведения при помощи интернет-сайта, имеющего статус СМИ, до самоубийства. Отмечаются проблемы квалификации доведения до самоубийства в «группах смерти» и посредством кибербуллинга. Поднимается вопрос о привлечении руководителей «групп смерти» к уголовной ответственности по совокупности преступлений, в которую будет входить статья 239 УК РФ.	The article examines the issues of criminal legal assessment of incitement to suicide committed in the media or the information and telecommunications network «Internet». Statistical data on committed acts of suicide and convictions against persons who committed a crime under Article 110 of the Criminal Code of the Russian Federation are compared. A qualification is given for incitement to suicide using an Internet site that has mass media status. The problems of qualification of suicide in «death groups» and through cyberbullying are noted. The question is being raised about bringing the leaders of «death groups» to criminal liability for a set of crimes, which will include Article 239 of the Criminal Code of the Russian Federation.
Ключевые слова: суицид, доведение до самоубийства, средства массовой информации, «Интернет», группы смерти, кибербуллинг	**Keywords:** suicide, suicide, incitement to suicide, media, Internet, death groups, cyberbullying
ЗУЕНКО Дарья Михайловна, студент Крымского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **КРЮЧКОВ Роман Олегович,** доцент кафедры уголовно-правовых дисциплин Крымского юридического института (филиала) Университета прокуратуры Российской Федерации	**ZUENKO Daria Mikhailovna,** Student of the Crimean Law Institute (branch) University of the Prosecutor's Office of the Russian Federation scientific supervisor **KRYUCHKOV Roman Olegovich,** Associate Professor of the Department of criminal law disciplines of the Crimean Law Institute (branch) University of the Prosecutor's Office of the Russian Federation
НЕКОТОРЫЕ АСПЕКТЫ ВОВЛЕЧЕНИЯ НЕСОВЕРШЕННОЛЕТНИХ В НЕЗАКОННЫЙ ОБОРОТ НАРКОТИЧЕСКИХ И ПСИХОТРОПНЫХ ВЕЩЕСТВ С ИСПОЛЬЗОВАНИЕМ ИН-	**SOME ASPECTS OF THE INVOLVEMENT OF MINORS IN THE ILLICIT TRAFFICKING OF NARCOTIC AND PSYCHOTROPIC SUBSTANCES USING**

ФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ	**INFORMATION AND TELECOMMUNICATION TECHNOLOGIES IN THE RUSSIAN FEDERATION**
Статья посвящена актуальным вопросам вовлечения несовершеннолетних в незаконный оборот наркотических и психотропных веществ посредством использования информационно-телекоммуникационных технологий. Особое внимание уделено причинам роста данного вида преступления, среди которых присутствует полная конфиденциальность на скрытых площадках. Автор приходит к выводу о необходимости не только закрытия интернет-площадок, но и привлечения организаторов к уголовной ответственности.	The article is devoted to topical issues of involving minors in the illicit trafficking of narcotic and psychotropic substances through the use of information and telecommunication technologies. Special attention is paid to the reasons for the growth of this type of crime, among which there is complete confidentiality on hidden sites. The author comes to the conclusion that it is necessary not only to close Internet sites, but also to bring the organizers to criminal responsibility.
Ключевые слова: вовлечение несовершеннолетних, оборот наркотических веществ, Национальная антинаркотическая стратегия, информационно-телекоммуникационные технологии, социальные сети, латентность	**Key words:** involvement of minors, drug trafficking, National Anti-Drug Strategy, information and telecommunication technologies, social networks, latency
ИВАШИНА Инна Александровна, студент Института кибербезопасности и цифровых технологий Российского технологического университета — МИРЭА научный руководитель **ШЕВЕЛЕВА Ксения Владимировна,** старший преподаватель кафедры правового обеспечения национальной безопасности Института кибербезопасности и цифровых технологий Российского технологического университета — МИРЭА	**IVASHINA Inna Alexandrovna,** Student of the Institute of Cybersecurity and Digital Technologies of the Russian Technological University — MIREA scientific supervisor **SHEVELEVA Ksenia Vladimirovna,** Senior Lecturer at the Department of legal support of national security at the Institute of Cybersecurity and Digital Technologies of the Russian Technological University — MIREA
О НЕКОТОРЫХ КРИМИНАЛИСТИЧЕСКИХ АСПЕКТАХ РАССЛЕДОВАНИЯ НЕЗАКОННОГО ОБОРОТА ОРУЖИЯ, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»	**ON SOME CRIMINALISTIC ASPECTS OF THE INVESTIGATION OF ILLEGAL ARMS TRAFFICKING CARRIED OUT VIA THE INTERNET**
Статья посвящена роли сети «Интернет» в совершении преступлений в сфере незаконного оборота оружия, боеприпасов, взрывчатых веществ, взрывных устройств. Рассмотрена криминалистическая характеристика данной категории преступлений, проведен анализ статистических данных, криминалистической практики и научной литературы. Выявлены сложности в раскрытии преступлений, связанных с незаконным обо-	The article is devoted to the role of the Internet in the commission of crimes in the field of illicit trafficking in weapons, ammunition, explosives, and explosive devices. The criminalistic characteristics of this category of crimes are considered, statistical data, criminalistic practice and scientific literature are analyzed. Difficulties in solving crimes related to illegal trafficking of weapons, ammunition, explosives and

ротом оружия, боеприпасов, взрывчатых веществ и взрывных устройств и совершенных с использованием сети «Интернет». **Ключевые слова:** преступления, незаконный оборот оружия, Даркнет, методика расследования преступлений, преступность в сети «Интернет»	explosive devices using the Internet have been identified. **Keywords:** crimes, arms trafficking, Darknet, methods of crime investigation, crime on the Internet
КАРАБИН Иван Денисович, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **К ВОПРОСУ О ВОЗМОЖНОСТИ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЗА РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ** Статья посвящена проблеме возможности привлечения к уголовной ответственности средств массовой информации за распространение заведомо ложной информации. Разработаны предложения по совершенствованию уголовного законодательства об ответственности за распространение заведомо ложной информации. **Ключевые слова:** коллективная ответственность, субъект преступления, средства массовой информации	**KARABIN Ivan Denisovich,** Student of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor **ON THE ISSUE OF THE POSSIBILITY OF CRIMINAL LIABILITY OF THE MASS MEDIA FOR THE DISSEMINATION OF DELIBERATELY FALSE INFORMATION** The article is devoted to the problem of the possibility of bringing the mass media to criminal responsibility for the dissemination of deliberately false information. Proposals have been developed to improve the criminal legislation on liability for the dissemination of deliberately false information. **Keywords:** collective responsibility, the subject of the crime, law enforcement, mass media
КИРЕЕВА Анастасия Вадимовна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **МОРОЗОВА Юлия Владимировна,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук	**KIREEVA Anastasia Vadimovna,** Student of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation scientific supervisor **MOROZOVA Yulia Vladimirovna,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law)

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»	**INVOLVEMENT OF A MINOR IN THE COMMISSION OF A CRIME USING THE INTERNET**
В статье отмечается, что информация, содержащаяся в сети «Интернет», стала платформой для распространения определенного противоправного контента, привлекающего внимание, в том числе, несовершеннолетних. Отмечены тенденции роста угроз, включающие активизацию криминальных личностей в отношении детей. В этой связи особо опасны и, как правило, латентны преступления, связанные с вовлечением несовершеннолетнего в преступную деятельность. В работе также сделаны выводы о необходимости внесения изменений в часть 2 статьи 150 УК РФ.	The article notes that the information contained on the Internet has become a platform for the dissemination of certain illegal content that attracts the attention of, among others, minors. There are trends in the growth of threats, including the activation of criminal personalities against children. In this regard, crimes involving the involvement of a minor in criminal activity are particularly dangerous and, as a rule, latent. The paper also draws conclusions about the need to amend part 2 of Article 150 of the Criminal Code of the Russian Federation.
Ключевые слова: несовершеннолетний, сеть «Интернет», вовлечение несовершеннолетнего в совершение преступления	**Keywords:** minor, the Internet, involvement of a minor in the commission of a crime
КИРШИНА Эвелина Алексеевна, ЧУПАШОВА Аделина Радиковна, студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **МОРОЗОВА Юлия Владимировна,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук	**KIRSHINA Evelina Alekseevna, CHUPASHOVA Adelina Radikovna,** Students of the St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation scientific supervisor **MOROZOVA Yulia Vladimirovna,** Associate Professor of the Department of criminal law, criminology and criminal executive law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law)
КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)	**CRIMINOLOGICAL CHARACTERISTICS OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)**
В статье рассматривается криминологическая характеристика преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»). Разработаны предложения по совершенствованию мер профилактики преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).	The article examines the criminological characteristics of crimes committed using information and telecommunication networks (including the Internet). Proposals have been developed to improve measures to prevent crimes committed using information and telecommunications networks (including the Internet).

Ключевые слова: квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	**Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet
КОЗЕНКОВА Александра Юрьевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ЛЕГАЛИЗАЦИЮ (ОТМЫВАНИЕ) ДЕНЕЖНЫХ СРЕДСТВ ИЛИ ИНОГО ИМУЩЕСТВА, ПРИОБРЕТЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, СОВЕРШАЕМУЮ ПУТЕМ ПРИОБРЕТЕНИЯ КРИПТОВАЛЮТЫ** В статье рассматриваются некоторые проблемы уголовной ответственности, предусмотренной за легализацию (отмывание) денежных средств или иного имущества, приобретенных преступным путем, совершаемую путем приобретения криптовалюты. Разработаны предложения по совершенствованию практики применения уголовного законодательства об ответственности, предусмотренной за легализацию (отмывание) денежных средств или иного имущества, приобретенных преступным путем, совершаемую путем приобретения криптовалюты. **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», легализация (отмывание) денежных средств, криптовалюта	**KOZENKOVA Alexandra Yuryevna,** student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor **SOME PROBLEMS OF CRIMINAL LIABILITY FOR THE LEGALIZATION (LAUNDERING) OF FUNDS OR OTHER PROPERTY ACQUIRED BY CRIMINAL MEANS, COMMITTED BY ACQUIRING CRYPTOCURRENCIES** The article discusses some problems of criminal liability for the legalization (laundering) of funds or other property acquired by criminal means, committed by acquiring cryptocurrencies. Proposals have been developed to improve the practice of applying criminal legislation on liability for the legalization (laundering) of funds or other property acquired by criminal means, committed by acquiring cryptocurrency **Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet, money laundering, cryptocurrency
КОМАРОВА Полина Алексеевна, слушатель Санкт-Петербургского университета МВД России	**KOMAROVA Polina Alekseevna,** student at the St. Petersburg University of the Ministry of Internal Affairs of Russia

научный руководитель **ТЕРТЫЧНАЯ Илона Викторовна,** доцент кафедры криминалистики Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент	scientific supervisor **TERTYCHNAYA Ilona Viktorovna,** Associate Professor of the Department of criminology of the St. Petersburg University of the Ministry of Internal Affairs of Russia, Candidate of Science (Law), Associate Professor
О НЕКОТОРЫХ ВОПРОСАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ОБОРОТОМ КРИПТОВАЛЮТ	**ON SOME ISSUES OF INVESTIGATION OF CRIMES RELATED TO THE TURNOVER OF CRYPTOCURRENCIES**
В статье проанализированы некоторые вопросы, связанные с расследованием преступлений, предметом которых является криптовалюта. Обозначены значительные пробелы, связанные с правовым регулированием контроля и оборота криптовалюты в Российской Федерации. Проанализированы проблемы методики расследования данной группы преступлений.	The article analyzes some issues related to the investigation of crimes, the subject of which is cryptocurrency. Significant gaps have been identified related to the legal regulation of the control and turnover of cryptocurrencies in the Russian Federation. The problems of the investigation methodology of this group of crimes are analyzed.
Ключевые слова: правовое регулирование, расследование преступлений, анонимность, информатизация, криптовалюта, цифровая валюта, биткоин	**Keywords:** legal regulation, crime investigation, anonymity, informatization, cryptocurrency, digital currency, bit coin
КОМИНА Вероника Игоревна, студент Института кибербезопасности и цифровых технологий Российского технологического университета — МИРЭА научный руководитель **ШЕВЕЛЕВА Ксения Владимировна,** старший преподаватель кафедры правового обеспечения национальной безопасности Института кибербезопасности и цифровых технологий Российского технологического университета — МИРЭА	**KOMINA Veronika Igorevna,** Student of the Institute of Cybersecurity and Digital Technologies of the Russian University of Technology — MIREA scientific supervisor **SHEVELEVA Ksenia Vladimirovna,** Senior Lecturer at the Department of legal support of national security at the Institute of Cybersecurity and Digital Technologies of the Russian Technological University — MIREA
ОТДЕЛЬНЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ ПРОТИВ ЖИЗНИ И ЗДОРОВЬЯ ЧЕЛОВЕКА, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ IT-ТЕХНОЛОГИЙ	**CERTAIN TYPES OF CRIMES AGAINST HUMAN LIFE AND HEALTH COMMITTED USING IT TECHNOLOGIES**
С развитием технологий возникают новые угрозы, включая преступления, совершаемые с использованием IT-технологий, которые могут нанести вред жизни и здоровью людей. В статье рассмотрены две группы преступлений, а именно: кибербуллинг и киберпреследование, а также киберпреступления, направленные на имплантируемые медицинские устройства. Автор приходит к выводу о том, что для решения данных проблем требуется комплексный подход, включая внесение изменений в Уголовный кодекс Российской Федерации.	With the development of technology, new threats arise, including crimes committed using IT technologies that can harm people's lives and health. The article considers two groups of crimes, namely: cyber bullying and cybercrime, as well as cybercrimes aimed at implantable medical devices. The author concludes that a comprehensive approach is required to solve these problems, including changes in the Criminal Code of the Russian Federation.

Ключевые слова: преступления против жизни и здоровья, IT-технологии, кибербуллинг, киберпреследование, имплантируемые медицинские устройства	**Keywords:** crimes against life and health, IT technologies, cyberbullying, cybercrime, implantable medical devices
КУЛЬПИН Алексей Андреевич, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **КОРШУНОВА Ольга Николаевна,** заведующий кафедрой прокурорского надзора и участия прокурора в рассмотрении уголовных, гражданских и арбитражных дел Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, доктор юридических наук, профессор	**KULPIN Alexey Andreevich,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **KORSHUNOVA Olga Nikolaevna,** Head of the Department of prosecutorial supervision and participation of the prosecutor in the consideration of criminal, civil and arbitration cases of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Doctor of Science (Law), Professor
К ВОПРОСУ ОБ ИНФОРМАЦИИ ОБ УЧАСТНИКАХ СВО В СИСТЕМЕ ОБСТОЯТЕЛЬСТВ, ПОДЛЕЖАЩИХ ИССЛЕДОВАНИЮ И ДОКАЗЫВАНИЮ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ, ПРЕДУСМОТРЕННЫХ СТАТЬЕЙ 207.3 УК РФ	**ON THE ISSUE OF INFORMATION ABOUT THE PARTICIPANTS OF THE SVO IN THE SYSTEM OF CIRCUMSTANCES TO BE INVESTIGATED AND PROVED IN CASES OF CRIMES PROVIDED FOR IN ARTICLE 207.3 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
Автор анализирует сущность и отличительные черты фейковых новостей, их манипулятивную направленность. Особое внимание уделяется внутренним и внешним источникам дезинформации о спецоперации, каналам распространения дезинформации через социальные сети и мессенджеры. Рассмотрены конкретные примеры распространения фейков о ходе боевых действий, жертвах среди мирного населения, примеры распространения информации, дискредитирующей российскую армию, т. е. совершения действий, предусмотренных ст. 207.3 УК РФ. Показано их негативное влияние на общественное мнение в России и место в системе обстоятельств, подлежащих исследованию и доказыванию.	The author analyzes the essence and distinctive features of fake news, their manipulative orientation. Special attention is paid to internal and external sources of disinformation about the special operation, channels for their dissemination through social networks and messengers. Specific examples of the spread of fakes about the course of hostilities, civilian casualties, and examples of the dissemination of information discrediting the Russian army, i.e., the commission of actions provided for in Article 207.3 of the Criminal Code of the Russian Federation, are considered. Their negative impact on public opinion in Russia and their place in the system of circumstances to be investigated and proved are shown.
Ключевые слова: фейки, информация, обстоятельства, подлежащие исследованию и доказыванию, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет»	**Keywords:** fakes, information, circumstances to be investigated and proven. the use of information and telecommunication networks, including the Internet
ЛЕБЕДЕВА Кристина Александровна, курсант Санкт-Петербургского университета МВД России	**LEBEDEVA Kristina Alexandrovna,** Cadet of the St. Petersburg University of the Ministry of Internal Affairs of Russia

научный руководитель **ВАСИЛЬЕВ Федор Юрьевич,** доцент кафедры уголовного процесса Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент	scientific supervisor **VASILIEV Fedor Yurievich,** Associate Professor of the Department of criminal procedure at the St. Petersburg University of the Ministry of Internal Affairs of Russia, Candidate of Science (Law), Associate Professor
СОВЕРШЕНСТВОВАНИЕ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА РАСПРОСТРАНЕНИЕ ЗАВЕДОМО ЛОЖНОЙ ИНФОРМАЦИИ (ЧАСТЬ 2 СТАТЬИ 128.1 УК РФ)	**IMPROVEMENT OF CRIMINAL LEGISLATION ON LIABILITY FOR THE DISSEMINATION OF DELIBERATELY FALSE INFORMATION (PART 2 OF ARTICLE 128.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)**
Статья посвящена совершенствованию части 2 статьи 128.1 УК РФ. В правоприменительной практике привлечение к ответственности по данным статьям вызывает некоторые трудности в связи с расплывчатостью понятий, указанных в диспозиции. Привлечение к ответственности за совершение преступления посредством использования средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») в настоящее время является одной из трудоемких задач, поскольку выявить субъект преступного деяния становится все сложнее из-за появления многочисленных сервисов, позволяющих преступнику оставаться анонимным.	The article is devoted to the improvement of part 2 of Article 128.1 of the Criminal Code of the Russian Federation. In law enforcement practice, prosecution under these articles causes some difficulties due to the vagueness of the concepts specified in the disposition. Bringing to justice for committing a crime through the use of mass media or electronic or information and telecommunication networks (including the Internet) is currently one of the time-consuming tasks, since it is becoming increasingly difficult to identify the subject of a criminal act due to the emergence of numerous services that allow the criminal to remain anonymous.
Ключевые слова: уголовная ответственность, сеть «Интернет», заведомо ложные сведения, клевета	**Keywords:** criminal liability, the Internet, knowingly false information, slander
МАКАЕВА Варвара Витальевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**MAKAEVA Varvara Vitalevna**, Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich**, Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor’s office of the Russian Federation, Candidate of Science (Law), Associate Professor
ИСПОЛЬЗОВАНИЕ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ	**THE USE OF SOCIAL MEDIA IN THE COMMISSION OF CRIMES**
В статье рассматриваются вопросы использования социальных сетей при совершении	The article discusses the use of social networks in the commission of crimes. The causes and

преступлений. Анализируются причины и условия криминализации социальных сетей. Исследуется классификация преступлений, которые совершены с помощью социальных сетей. Выделяются правила безопасности использования социальных сетей. **Ключевые слова:** квалификация преступлений, использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», социальные сети, преступления	conditions of criminalization of social networks are analyzed. The classification of crimes committed with the help of social networks is being investigated. The safety rules for using social networks are highlighted. **Keywords:** qualification of crimes, use of information and telecommunication networks, including the Internet, social networks, crimes
МАЛЬЦЕВА Ульяна Павловна, **ФАБРИЧНОВА Виктория Дмитриевна,** студенты Северо-Западного филиала Российского государственного университета правосудия научный руководитель **РАХМАНОВА Екатерина Николаевна**, заведующий кафедрой уголовного права Северо-Западного филиала Российского государственного университета правосудия, доктор юридических наук, доцент **ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КАК СПОСОБ НАРУШЕНИЯ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ: ПРОБЛЕМЫ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ** В статье рассматриваются некоторые проблемы, связанные с использованием киберпространства для совершения преступлений, посягающих на неприкосновенность частной жизни. Исследованы вопросы новых способов совершения указанных преступлений, а также аспекты понятия и пределов частной жизни. Разработаны предложения по совершенствованию уголовного законодательства в контексте использования современных технологий при нарушении неприкосновенности частной жизни. **Ключевые слова:** частная жизнь, киберпространство, сеть «Интернет», информация, искусственный интеллект, личная тайна, распространение сведений	**MALTSEVA Ulyana Pavlovna,** **FABRICHNOVA Victoria Dmitrievna,** Students of the North-Western Branch of the Russian State University of Justice scientific supervisor **RAKHMANOVA Ekaterina Nikolaevna,** Head of the Department of criminal law of the North-Western Branch of the Russian State University of Justice, Doctor of Science (Law), Associate Professor **THE INFORMATION AND TELECOMMUNICATION NETWORKS AS A WAY OF VIOLATING PRIVACY: PROBLEMS AND CRIMINAL LAW ASPECTS** The article discusses problems of using the cyberspace to commit crimes that infringe on privacy. Attention is drawn to the new ways of committing these crimes and aspects of the concept and limits of private life. Proposals have been developed to improve criminal legislation in the context of using information technologies for violation of privacy. **Keywords:** private life, cyberspace, the Internet, information, artificial intelligence, personal privacy, dissemination of information
МАМАЕВА Гульназ Зурабовна, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России)	**MAMAYEVA Gulnaz Zurabovna,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia)

научный руководитель **ДЖАНТУХАНОВА Милана Висадиевна,** преподаватель юридического колледжа Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России)	scientific supervisor **DZHANTUKHANOVA Milana Visadievna,** lecturer at the Law College of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia)
РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ СЕТЕЙ	**DEVELOPMENT OF LEGISLATION ON LIABILITY FOR OFFENCES COMMITTED THROUGH THE OF COMPUTER NETWORK**
Рассмотрены основные этапы становления уголовного законодательства об ответственности за совершение преступлений с использованием информационно-телекоммуникационных технологий. Показана статистика, подчеркивающая особое место компьютерной информации в жизни общества. Анализируются основные группы преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.	The main stages of the formation of criminal legislation on responsibility for committing crimes using information and telecommunication technologies are considered. Statistics emphasizing the special place of computer information in the life of society are shown. The main groups of crimes committed using information and telecommunication technologies are analyzed. Legal conflicts are noted, the solution of which will contribute to the effective prevention of the offenses under consideration.
Ключевые слова: уголовное право, уголовное законодательство, компьютерная информация, компьютерные сети, информационно-телекоммуникационные технологии, профилактика	**Keywords:** criminal law, criminal legislation, computer information, computer networks, information and telecommunication technology, prevention
МАРТЫНЕНКО Полина Денисовна, студент магистратуры Северо-Западного филиала Российского государственного университета правосудия научный руководитель **БЕЗБОРОДОВ Дмитрий Анатольевич,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия кандидат юридических наук, доцент	**MARTYNENKO Polina Denisovna,** Graduate student at the North-Western Branch of the Russian State University of Justice scientific supervisor **BEZBORODOV Dmitry Anatolyevich**, Associate Professor of the Department of criminal law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor
НЕЗАКОННЫЕ ПОЛУЧЕНИЕ И РАЗГЛАШЕНИЕ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ, НАЛОГОВУЮ И БАНКОВСКУЮ ТАЙНУ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ	**ILLEGAL ACQUISITION AND DISCLOSURE OF INFORMATION CONSTITUTING COMMERCIAL, TAX, AND BANKING SECRECY USING ELECTRONIC OR INFORMATION-TELECOMMUNICATION NETWORKS**
Подробно рассматривается преступление, предусмотренное статьей 183 УК РФ, которое может быть совершено с применением	The crime provided for in Article 183 of the Criminal Code of the Russian Federation,

электронных носителей и сетей. В связи с развитием информационных технологий все чаще персональная информация хранится в электронном виде, что предопределяет возможность совершения преступлений иного характера и способа. **Ключевые слова:** коммерческая тайна, налоговая тайна, банковская тайна, информационно-телекоммуникационные сети, электронные сети, конфиденциальная информация, компьютерные преступления	which can be committed using electronic media and networks, is considered in detail. Due to the development of information technologies, personal information is increasingly stored in electronic form, which determines the possibility of committing crimes of a different nature and method. **Keywords:** commercial secrecy, tax secrecy, banking secrecy, information and telecommunication networks, electronic networks, confidential information, computer crimes
МАТЮШКИНА Александра Сергеевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **КРАВЧЕНКО Роман Михайлович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук **НЕКОТОРЫЕ ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ «ИНТЕРНЕТ-СОБСТВЕННОСТИ»** В статье обозначены проблемы правового регулирования, в том числе уголовно-правовой охраны, виртуального «имущества», рассматривается зарубежный опыт и судебная практика Российской Федерации. Анализируется возможность отнесения «интернет-собственности» к предмету преступлений против собственности. Приводятся возможные квалификации деяний, связанных с посягательством на внутриигровые предметы. **Ключевые слова**: виртуальное «имущество», интернет-собственность, ответственность в киберпространстве, хищение внутриигровых предметов, имущественный вред, цифровые права	**MATYUSHKINA Alexandra Sergeevna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **KRAVCHENKO Roman Mikhailovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law) **SOME PROBLEMS OF CRIMINAL LAW PROTECTION OF «INTERNET PROPERTY»** The article identifies the problems of legal regulation, including criminal law protection, virtual "property", examines foreign experience and judicial practice of the Russian Federation. The possibility of attributing "Internet property" to the subject of crimes against property is analyzed. Possible qualifications of acts related to encroachment on in-game items are given. **Keywords:** virtual «property», Internet property, responsibility in cyberspace, theft of in-game items, property damage, digital rights
МИЩЕНКО Дарья Сергеевна, **СОБОЛЕВА Дарья Сергеевна,** студенты Санкт-Петербургской академии Следственного комитета Российской Федерации	**MISHCHENKO Darya Sergeevna,** **SOBOLEVA Darya Sergeevna,** Students of the St. Petersburg Academy of the Investigative Committee of the Russian Federation

научный руководитель **СЕРДЮК Павел Леонидович,** доцент кафедры уголовного права и криминологии, Санкт-Петербургской академии Следственного комитета Российской Федерации, кандидат юридических наук	scientific supervisor **SERDYUK Pavel Leonidovich,** Associate Professor of the Department of criminal law and criminology, St. Petersburg Academy of the Investigative Committee of the Russian Federation, Candidate of Science (Law)
УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПОСРЕДНИЧЕСТВА ВО ВЗЯТОЧНИЧЕСТВЕ (СТАТЬЯ 291.1 УК РФ), В ТОМ ЧИСЛЕ СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)	**CRIMINAL LAW CHARACTERISTICS OF MEDIATION IN BRIBERY (ARTICLE 291.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION), INCLUDING THOSE COMMITTED USING INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)**
В статье рассматриваются вопросы ответственности за посредничество во взяточничестве, связанные с описанием объективной стороны преступления, способов его совершения, квалификацией деяния. Анализируются способы использования информационно-телекоммуникационной сети (включая сеть «Интернет») посредниками во взяточничестве, взяткополучателями и взяткодателями.	The article discusses the issues of responsibility for mediation in bribery related to the description of the objective side of the crime, the methods of its commission, and the qualification of the act. The ways of using the information and telecommunication network (including the Internet) by intermediaries in bribery, bribe-takers and bribe-takers are analyzed.
Ключевые слова: взяточничество, посредник во взяточничестве, коррупция, предмет взятки, сеть «Интернет»	**Keywords:** bribery, intermediary in bribery, corruption, the subject of a bribe, the Internet
НАЗАРЕНКО Ирина Сергеевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**NAZARENKO Irina Sergeevna,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor
ПРОБЛЕМЫ КВАЛИФИКАЦИИ РЕАБИЛИТАЦИИ НАЦИЗМА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ ЛИБО ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, В ТОМ ЧИСЛЕ СЕТИ «ИНТЕРНЕТ» (СТАТЬЯ 354.1 УК РФ)	**PROBLEMS OF QUALIFICATION OF REHABILITATION OF NAZISM USING MASS MEDIA OR INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET (ARTICLE 354.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)**
В статье рассматриваются вопросы применения статьи 354.1 УК РФ при квалификации преступления, связанного с реабилита-	The article discusses the application of Article 354.1 of the Criminal Code of the Russian Federation in the qualification of crimes related to the rehabilitation of Nazism. Criminal

цией нацизма. Установлена уголовная ответственность за публичное непризнание установленных приговором Международного военного трибунала решений, а также за одобрение деяний, запрещенных данным приговором. Анализируются проблемы применения статьи 354.1 УК РФ, проблемы определения оконченного состава преступления, а также его разграничение со смежными составами, предусмотренными разными частями данной нормы, и с другими статьями УК РФ на основе примеров судебной практики. **Ключевые слова:** реабилитация нацизма, осквернение, сеть «Интернет», уголовная ответственность	liability has been established for public non-recognition of the decisions established by the verdict of the International Military Tribunal, as well as for approving acts prohibited by this verdict. The article analyzes the problems of applying Article 354.1 of the Criminal Code of the Russian Federation, the problems of determining the completed corpus delicti, as well as its differentiation from related constitutions provided for by different parts of this norm, and with other articles of the Criminal Code of the Russian Federation based on examples of judicial practice. **Keywords:** rehabilitation of Nazism, desecration, Internet, criminal liability
НУРМАГОМЕДОВА Патимат Саидбеговна, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель **КЕРИМОВА Заира Абдурахмановна,** преподаватель юридического колледжа Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) **ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»** В настоящее время тема способов совершения преступлений и проблем их квалификации является достаточно значимой. В статье рассматриваются преступления, совершенные посредством сети «Интернет» и информационно-телекоммуникационных технологий, а также проблемы раскрытия и квалификации такого вида преступлений. **Ключевые слова:** сеть «Интернет», коммуникационные технологии, преступление, хищение, информационно-телекоммуникационная сеть	**NURMAGOMEDOVA Patimat Saidbekovna,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **KERIMOVA Zaira Abdurakhmanovna,** Lecturer at the Law College of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) **PROBLEMS OF QUALIFICATION OF CRIMES COMMITTED USING THE INTERNET** Currently, the topic of methods of committing crimes and the problems of their qualification is quite significant. The article discusses crimes committed through the Internet and information and telecommunication technologies, as well as the problems of disclosure and qualification of this type of crime. **Keywords:** Internet, communication technologies, crime, theft, information and telecommunication network
ПЕРОВ Даниил Викторович, студент Северо-Западного филиала Российского государственного университета правосудия научный руководитель **КРАСНОВА Кристина Александровна,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**PEROV Daniil Viktorovich,** Student of the North-Western Branch of the Russian State University of Justice scientific supervisor **KRASNOVA Kristina Alexandrovna**, Associate Professor of the Department of criminal law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor

ОСОБЕННОСТИ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ С ПОМОЩЬЮ СОЦИАЛЬНЫХ СЕТЕЙ	**FEATURES OF OBTAINING EVIDENCE OF CRIMES COMMITTED USING SOCIAL NETWORKS**
Современный мир переполнен информацией, а также большее ее количество располагается в сети «Интернет». Ее могут использовать в различных, как в благих, так и в криминальных, целях. Вопрос изъятия и процессуальной фиксации такой информации не регулируется действующим законодательством, что затрудняет использование этой информации в качестве доказательств. В статье рассматриваются проблемы, связанные с эффективностью получения доказательств причастности к преступлениям, совершенным с помощью сети «Интернет».	Modern world is overflowing with information, and more of it is located on the Internet. It can be used for various purposes, both for good and criminal purposes. The issue of withdrawal and procedural fixation of such information is not regulated by the current legislation, which makes it difficult to use this information as evidence. The article discusses the problems related to the effectiveness of obtaining evidence of involvement in crimes committed using the Internet.
Ключевые слова: информация, социальные сети, преступления, гаджеты, экспертиза, статья 185 Уголовно-процессуального кодекса Российской Федерации, статья 74 Уголовно-процессуального кодекса Российской Федерации	**Keywords:** Information, social networks, crimes, gadgets, expertise, Article 185 of the Code of Criminal Procedure of the Russian Federation, Article 74 of the Code of Criminal Procedure of the Russian Federation
ПЕТРУХИНА Алина Андреевна, **СИВЦЕВА Анжелика Александровна,** студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**PETRUKHINA Alina Andreevna,** **SIVTSEVA Angelika Alexandrovna,** Students of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Science (Law), Associate Professor
ИСПОЛЬЗОВАНИЕ СЕТИ «ИНТЕРНЕТ» ПРИ СОВЕРШЕНИИ ГОСУДАРСТВЕННОЙ ИЗМЕНЫ	**THE USE OF THE INTERNET IN THE COMMISSION OF TREASON**
В статье рассматриваются некоторые вопросы совершения государственной измены с использованием сети «Интернет». Авторы обращаются к понятиям «государственная измена» и «способ совершения преступления». В связи с компьютеризацией и цифровизацией общества распространяются случаи совершения рассматриваемого преступления с использованием сети «Интернет», что вызывает некоторые проблемы в правоприменительной практике, которые необходимо решить.	The article discusses some issues of committing high treason using the Internet. The authors refer to the concepts of «high treason» and «method of committing a crime». In connection with the computerization and digitalization of society, cases of the commission of the crime in question using the Internet are spreading, which causes some problems in law enforcement practice that need to be solved.

Ключевые слова: государственная измена, сотрудничество с иностранной организацией, государственная безопасность, использование сети «Интернет»	**Keywords:** high treason, cooperation with a foreign organization, state security, using the Internet
РАБАДАНОВА Сабият Рабадановна, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель **СЕЛИМОВА Анара Маратовна,** доцент кафедры теории государства и права Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России)**,** кандидат юридических наук **ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ РЕЛИГИОЗНОМУ ЭКСТРЕМИЗМУ В СЕТИ «ИНТЕРНЕТ»** В статье определены сущностное понимание религиозного экстремизма и особенности организационно-правовой профилактики этого явления. Жертвами этого страшного явления становятся, как правило, дети, подростки и молодежь, которых легко заманить в паутину идеологического обмана. Религиозный экстремизм опасен не только разрушением социальных объектов и ценностей, убийствами и терроризмом. Более опасна сама идеология экстремизма, искажающая мировоззрение и дух человека. **Ключевые слова:** религиозный экстремизм, причины и условия распространения в сети «Интернет», сеть «Интернет»	**RABADANOVA Sabiyat Rabadanovna,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **SELIMOVA Anara Maratovna,** Associate Professor of the Department of Theory of State and Law of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Candidate of Science (Law) **ORGANIZATIONAL AND LEGAL BASES OF COUNTERING RELIGIOUS EXTREMISM ON THE INTERNET** The article defines the essential understanding of religious extremism and the features of the organizational and legal prevention of this phenomenon. The victims of this terrible phenomenon are, as a rule, children, teenagers and young people, who are easily lured into the web of ideological deception. Religious extremism is dangerous not only by the destruction of social facilities and values, murders and terrorism. The ideology of extremism itself is more dangerous, distorting the worldview and spirit of a person. **Keywords:** religious extremism, causes and conditions of spread on the Internet, the Internet
РАХМАТУЛЛИН Руслан Ленарович, ТУРКОВСКИЙ Никита Олегович, студенты Северо-Западного филиала Российского государственного университета правосудия научные руководители **ДВОРЖИЦКАЯ Марина Андреевна,** старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук; **ПИСАРЕВСКАЯ Елена Анатольевна,** доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент	**RAKHMATULLIN Ruslan Lenarovich, TURKOVSKY Nikita Olegovich,** Students of the North-Western Branch of the Russian State University of Justice scientific supervisors **DVORZHITSKAYA Marina Andreevna,** Senior Lecturer at the Department of Criminal Law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law); **PISAREVSKAYA Elena Anatolyevna,** Associate Professor of the Department of Criminal Law of the North-Western Branch of the Russian State University of Justice, Candidate of Science (Law), Associate Professor

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ВИРТУАЛЬНОЙ СОБСТВЕННОСТИ	**PROBLEMS OF CRIMINAL LAW PROTECTION OF VIRTUAL REALITY**
В статье рассматриваются некоторые проблемы уголовно-правовой охраны виртуальной собственности на примере виртуальных предметов в онлайн-играх. Исследованы понятия предмета преступления, предмета хищения, виртуальной собственности. Делается вывод о том, что сегодня в нашей стране складывается неопределенная ситуация, связанная с защитой виртуальной собственности в игре, в том числе уголовно-правовыми средствами. Авторами предлагаются различные пути решения обозначенной проблемы, в том числе расширение перечня объектов гражданских прав или конкретизация иного имущества (ст. 128 ГК РФ).	The article discusses some problems of criminal law protection of virtual property using the example of virtual objects in online games. The concepts of the subject of crime, the subject of theft, and virtual property are investigated. It is concluded that today in our country there is an uncertain situation related to the protection of virtual property in the game, including by criminal legal means. The authors propose various ways to solve this problem, including expanding the list of objects of civil rights or specifying other property (Article 128 of the Civil Code of the Russian Federation).
Ключевые слова: виртуальная собственность, имущество, хищение, предмет хищения, компьютерные преступления, пользовательское соглашение, онлайн-игра	**Keywords:** Keywords: virtual property, property, theft, object of theft, computer crimes, user agreement, online game
РОГАНОВА Дарья Сергеевна, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗИМИРЕВА Людмила Александровна,** старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридический наук	**ROGANOVA DARYA Sergeevna,** Student of the St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation scientific supervisor **ZIMIREVA Lyudmila Alexandrovna,** Senior Lecturer at the Department of criminal law, criminology and criminal executive law, St. Petersburg Law Institute (branch) of the University of prosecutor's office of the Russian Federation, Candidate of Science (Law)
КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЛИЦ, СОВЕРШАЮЩИХ КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ	**CRIMINOLOGICAL CHARACTERISTICS OF PERSONS COMMITTING COMPUTER CRIMES**
В статье рассматриваются вопросы, связанные с криминологической характеристикой личности преступника в сфере компьютерной информации. Автором исследуются теоретические и практические аспекты вышеназванного понятия, а также проанализирована судебная практика в рассматриваемой области. Отмечено, что знание криминологической характеристики личности имеет важное значение не только для фор-	The article discusses issues related to the criminological characteristics of the personality of a criminal in the field of computer information. The author examines the theoretical and practical aspects of the above-mentioned concept, and also analyzes judicial practice in the area under consideration. It is noted that knowledge of the criminological characteristics of a person is important not only for the formation of an evidence base, the correct qualification of an act in practice, but also for determining the

мирования доказательственной базы, правильной квалификации деяния в практической деятельности, но и определения мотивов, целей, способов совершения преступлений в данной области с целью их предотвращения и профилактики.	motives, goals, methods of committing crimes in this area in order to prevent them.
Ключевые слова: криминология, личность преступника, характеристика, информационные технологии, информационная инфраструктура, киберпреступления	**Keywords**: criminology, criminal personality, characteristics, information technology, information infrastructure, cybercrime
САРАПКИН Владимир Александрович, студент Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ЗАРУБИН Андрей Викторович,** доцент кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент	**SARAPKIN Vladimir Alexandrovich,** Student of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **ZARUBIN Andrey Viktorovich,** Associate Professor of the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation, Candidate of Law, Associate Professor
О НЕКОТОРЫХ ВОПРОСАХ КВАЛИФИКАЦИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЯ) ДЕНЕЖНЫХ СРЕДСТВ ИЛИ ИНОГО ИМУЩЕСТВА, ПРИОБРЕТЕННЫХ ПРЕСТУПНЫМ ПУТЕМ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ»	**ON SOME ISSUES OF QUALIFICATION OF LEGALIZATION (LAUNDERING) FUNDS OR OTHER PROPERTY ACQUIRED BY CRIMINAL MEANS USING THE INTERNET**
В статье рассматриваются отдельные проблемы квалификации легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем в электронной среде. Исследованы нормы законодательства, судебная практика, статистические данные, а также перспективы применения статей 174, 174.1 УК РФ при совершении преступления посредством сети «Интернет». Разработаны предложения по совершенствованию уголовного законодательства и судебной практики по делам о легализации денежных средств или иного имущества, приобретенных преступным путем с использованием информационно-телекоммуникационных технологий.	The article discusses certain problems of qualifying the legalization (laundering) of funds or other property acquired by criminal means in the electronic environment. The norms of legislation, judicial practice, statistical data, as well as the prospects for the application of Art. Art. 174, 174.1 of the Criminal Code of the Russian Federation using the Internet. Proposals have been developed to improve criminal legislation and judicial practice in cases of legalization using information and telecommunication technologies.
Ключевые слова: легализация, криптовалюта, сеть «Интернет», цифровая валюта	**Keywords:** legalization, cryptocurrency, Internet, digital currency

СЕРДЮКОВ Роман Вадимович, студент Санкт-Петербургской академии Следственного комитета Российской Федерации научный руководитель **КАЛИНКИНА Анна Борисовна,** старший преподаватель кафедры уголовного права и криминологии академии Следственного комитета Российской Федерации	**SERDYUKOV Roman Vadimovich,** student of the St. Petersburg Academy of the Investigative Committee of the Russian Federation scientific supervisor **KALINKINA Anna Borisovna,** Senior Lecturer at the Department of criminal law and criminology of the Academy of the Investigative Committee of the Russian Federation
НЕКОТОРЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ	**SOME FEATURES OF THE INVESTIGATION OF CORRUPTION CRIMES RELATED TO THE USE OF CRYPTO CURRENCIES**
В статье анализируются некоторые проблемы расследования коррупционных преступлений, совершенных с использованием криптовалют. Предлагаются практические решения проблем, встающих перед правоохранителями в ходе следственной и прокурорской и оперативно-разыскной деятельности.	The article analyzes some problems of investigating crimes of corruption crimes committed using crypto currencies. Practical solutions to the problems faced by law enforcement officers in the course of investigative and prosecutorial and operational investigative activities are proposed.
Ключевые слова: криптовалюта, коррупционные преступления, мессенджер, взятка	**Keywords:** cryptocurrency, corruption crimes, messenger, bribe
СОЛОВЬЕВА Марианна Константиновна, студент Санкт-Петербургского государственного университета научный руководитель **ПРЯХИНА Надежда Ивановна,** доцент кафедры уголовного права Санкт-Петербургского государственного университета, кандидат юридических наук	**SOLOVYOVA Marianna Konstantinovna,** Student of St. Petersburg State University scientific supervisor **PRYAKHINA Nadezhda Ivanovna,** Associate Professor of the Department of criminal law at St. Petersburg State University, Candidate of Science (Law)
ЭЛЕКТРОННЫЙ ДОКУМЕНТ КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 327 УК РФ	**AN ELECTRONIC DOCUMENT AS THE SUBJECT OF A CRIME UNDER ARTICLE 327 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION**
В данном исследовании рассматриваются определение понятия подложного электронного документа и особенности квалификации альтернативных действий в отношении электронных документов по сравнению с бумажными в статье 327 УК РФ. Обозначены проблемы квалификации преступлений, связанных с электронными документами, а также соотношение этих преступлений с преступлениями в сфере компьютерной информации, и предложены пути их решения.	The article is devoted to the definition of the concept of a counterfeit electronic document and to qualification features of alternative actions with electronic documents in comparison with paper documents in the context of the crime under art. 327 CC RF. There are mentioned qualification problems concerning crimes connected with electronic documents and their correlation with computer crimes, and suggested ways of their solving.

Ключевые слова: электронный документ, подделка, квалификация преступлений, компьютерная информация	**Keywords:** electronic document, forgery, qualification of the crimes, computer information
СОЛОМАХИН Никита Максимович, ЯКОВЛЕВ Роман Михайлович, студенты Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации научный руководитель **ФЕДЫШИНА Полина Викторовна,** старший преподаватель кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации	**SOLOMAKHIN Nikita Maksimovich, YAKOVLEV Roman Mikhailovich**, Students of the St. Petersburg Law Institute (branch) University of prosecutor's office of the Russian Federation scientific supervisor **FEDYSHINA Polina Viktorovna,** Senior Lecturer at the Department of criminal law, criminology and penal enforcement law of the St. Petersburg Law Institute (Faculty) University of prosecutor's office of the Russian Federation
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ КАК СРЕДСТВО СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ В статье рассмотрено использование информационно-телекоммуникационных технологий как средства совершения преступления. Проведено разграничение смежных понятий, таких как «орудие» и «способ совершения преступления». Разработана и предложена аргументация на предмет введения и использования таких технологий в перечень отягчающих вину обстоятельств, содержащихся в ст. 63 УК РФ. **Ключевые слова:** информационно-телекоммуникационные технологии, отягчающее обстоятельство, средство совершения преступления, отмывание денежных средств	**INFORMATION-TELECOMMUNICATION TECHNOLOGIES AS A MEANS OF COMMITTING A CRIME** The article considers the use of information and telecommunication technologies as a means of committing a crime. The differentiation from related concepts such as instrument and method of committing a crime is carried out. The argumentation about introduction of the use of such technologies in the list of aggravating circumstances contained in article 63 of the Criminal Code of the Russian Federation is developed and offered. **Keywords:** information-telecommunication technologies, aggravating circumstance, means of committing a crime, money laundering
СПИРИДОНОВА Эвелина, ШУКУРОВА Ситора Абдусамиевна, студенты Северо-Западного филиала Российского государственного университета правосудия научный руководитель **ФИЛАТОВА Надежда Юрьевна,** старший преподаватель кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия	**SPIRIDONOVA Evelina, SHUKUROVA Sitora Abdusamievna,** Students of the North-Western Branch of the Russian State University of Justice scientific supervisor **FILATOVA Nadezhda Yuryevna,** Senior Lecturer at the Department of criminal law of the North-Western Branch of the Russian State University of Justice

ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНЕГО В СОВЕРШЕНИЕ ДЕЙСТВИЙ, ПРЕДСТАВЛЯЮЩИХ ОПАСНОСТЬ ДЛЯ ЖИЗНИ НЕСОВЕРШЕННОЛЕТНЕГО, С ПОМОЩЬЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»)	**INVOLVING A MINOR IN COMMITTING ACTIONS THAT POSE A DANGER TO THE LIFE OF A MINOR USING INFORMATION AND TELECOMMUNICATION NETWORKS (INCLUDING THE INTERNET)**
В статье проводится анализ общественной опасности совершения преступления в виде вовлечения несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего, с помощью информационно-телекоммуникационных сетей (включая сеть «Интернет»). Рассматривается также судебная практика по указанному составу. Особое внимание уделяется дискуссионному вопросу, касающемуся отличия вовлечения и склонения от агитации и пропаганды.	The article analyzes the social danger of committing a crime in the form of involving a minor in committing actions that pose a danger to the life of a minor, using information and telecommunication networks (including the Internet). Judicial practice on this composition is also considered. Particular attention is paid to the controversial issue regarding the difference between involvement and inducement from agitation and propaganda.
Ключевые слова: вовлечение, склонение, пропаганда, интернет, зацепинг, судебная практика	**Keywords:** involvement, inducement, propaganda, Internet, hooking, judicial practice
ТАЙМАЗОВ Курбан Багомедович, студент Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России) научный руководитель **РАДЖАБОВ Шамиль Раджабович,** доцент кафедры уголовного права и процесса Северо-Кавказского института (филиала) Всероссийского государственного университета юстиции (РПА Минюста России), кандидат юридических наук	**TAYMAZOV Kurban Bagomedovich,** Student of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia) scientific supervisor **RAJABOV Shamil Radjabovic,** Associate Professor of the Department of criminal law and procedure of the North Caucasus Institute (branch) All-Russian State University of Justice (RPA of the Ministry of Justice of Russia), Candidate of Science (Law)
ВИКТИМОЛОГИЧЕСКИЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ СОВРЕМЕННОГО РОССИЙСКОГО ОБЩЕСТВА	**THE VICTIMOLOGICAL ASPECTS OF THE DIGITALIZATION OF MODERN RUSSIAN SOCIETY**
В статье предпринята попытка вынести на научное обсуждение относительно новую проблему виктимологических аспектов цифровизации современного общества. Подчеркивая межотраслевой характер данной проблематики, автор стремился акцентировать внимание на вопросах защищенности и безопасности жертв преступлений	The article attempts to bring to scientific discussion a relatively new problem of victimological aspects of digitalization of modern society. Emphasizing the intersectoral nature of this issue, the author sought to focus on the issues of protection and safety of crime victims in the context of total digitalization of society. The study defines the parity or dualistic nature of digitalization as an object of

в условиях тотальной цифровизации общества. В исследовании определяется паритетный или дуалистический характер цифровизации как объекта виктимологического исследования, констатируется, что виктимологические исследования цифровизации должны основываться на широком понятии «жертвы преступления», а ее операциональное узкое значение может быть использовано не иначе как к конкретным видам преступлений в сфере компьютерной информации.	victimological research, states that victimological studies of digitalization should be based on the broad concept of "victim of crime", and its operational narrow meaning can be used only to specific types of crimes in the field of computer information.
Ключевые слова: цифровизация общества, жертвы преступлений в цифровом обществе, факторы виктимизации, уязвимость цифровизации, виктимологическая безопасность	**Keywords:** digitalization of a society, victims of a crime in a digital society, factors of the victimization, vulnerability of the digitalization, victimological security
ФРОЛЕНКОВ Георгий Викторович, слушатель Санкт-Петербургского университета МВД России научный руководитель **ТЕРТЫЧНАЯ Илона Викторовна,** доцент кафедры криминалистики Санкт-Петербургского университета МВД России, кандидат юридических наук, доцент	**FROLENKOV Georgy Viktorovich,** Student at the St. Petersburg University of the Ministry of Internal Affairs of Russia scientific supervisor **TERTYCHNAYA Ilona Viktorovna,** Associate Professor of the Department of criminology at the St. Petersburg University of the Ministry of Internal Affairs of Russia, Candidate of Law, Associate Professor
ИГРОВЫЕ ПРЕДМЕТЫ И ОПЕРАЦИИ С НИМИ — УГОЛОВНО-ПРАВОВОЙ АСПЕКТ	**GAME ITEMS AND OPERATIONS WITH THEM — CRIMINAL LEGAL ASPECT**
В настоящей статье сформулирован подход, согласно которому игровые предметы, цифровые предметы в компьютерных играх можно отнести к имуществу, тем самым определив их в качестве объекта уголовно-правовой охраны. Определяется перечень уголовно наказуемых деяний, связанных с использованием данных предметов.	This article formulates an approach according to which game objects, digital objects in computer games can be attributed to property, thereby defining them as an object of criminal law protection. A list of criminal offenses related to the use of these items is determined.
Ключевые слова: цифровые предметы, компьютерные игры, игровые предметы, объекты гражданских прав, киберпреступления	**Keywords:** digital items, computer games, game items, objects of civil rights, cybercrimes