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

А. Н. ПОПОВ, Р. Д. ШАРАПОВ

КОММЕНТАРИЙ

К ПОСТАНОВЛЕНИЮ 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"»

Санкт-Петербург
2024

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

А. Н. ПОПОВ, Р. Д. ШАРАПОВ

КОММЕНТАРИЙ

К ПОСТАНОВЛЕНИЮ 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"»

Под общей редакцией
доктора юридических наук, профессора А. Н. Попова

Санкт-Петербург
2024

УДК 343.2(076)
ББК 67.408я73
П58

А в т о р ы

А. Н. ПОПОВ, *д-р юрид. наук, профессор* — пп. 1—16 Постановления; Р. Д. ШАРАПОВ, *д-р юрид. наук, профессор* — пп. 17—24 Постановления.

Под общей редакцией
доктора юридических наук, профессора А. Н. ПОПОВА

Р е ц е н з е н т ы

Е. В. БЕЗРУЧКО, заведующий кафедрой уголовного права и криминологии факультета подготовки следователей Санкт-Петербургской академии Следственного комитета Российской Федерации, доктор юридических наук, профессор.

В. Н. САФОНОВ, доцент кафедры уголовного права Северо-Западного филиала Российского государственного университета правосудия, кандидат юридических наук, доцент.

Попов, А. Н.

П58 Комментарий к постановлению Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 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”» / А. Н. Попов, Р. Д. Шарапов ; под общ. ред. А. Н. Попова. — Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2024. — 82, [2] с.

ISBN 978-5-6051510-8-1

Комментарий представляет собой доктринальное толкование положений Постановления Пленума Верховного Суда Российской Федерации о судебной практике по рассмотрению уголовных дел о преступлениях в сфере компьютерной информации и иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Предназначен для обучающихся по программам высшего образования по укрупненной группе специальностей и направлений подготовки 40.00.00 Юриспруденция, а также программам профессиональной переподготовки и повышения квалификации работников органов прокуратуры.

УДК 343.2(076)
ББК 67.408я73

ISBN 978-5-6051510-8-1

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Научно-технический прогресс имеет как положительные, так и отрицательные стороны. К негативным факторам научно-технического развития общества можно отнести «модернизацию» преступности, появление нового вида преступлений.

В научной литературе оперируют такими понятиями, как «компьютерные преступления», «преступления в сфере компьютерной информации», «информационные преступления», «киберпреступления», «цифровые преступления», «информационно-телекоммуникационные преступления» и т. д.

Единого устоявшегося термина в науке в отношении новых видов преступлений в настоящее время не существует.

В Уголовном кодексе Российской Федерации предусматривается ответственность за большое количество разнообразных преступлений, совершаемых с использованием программно-технических средств и различных сетей, а также содержится специальная глава, объединяющая нормы об ответственности за совершение преступлений в сфере компьютерной информации.

Не случайно Верховный Суд Российской Федерации на Пленуме, состоявшемся 15 декабря 2022 года, принял постановление № 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”». В данном Постановлении Пленум обратил внимание на вопросы квалификации двух групп преступлений: преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Рекомендации Пленума Верховного Суда Российской Федерации по квалификации данных видов преступлений, несомненно, положительно скажутся на правоприменительной практике.

Анализ данных рекомендаций и является целью настоящего Комментария.

ПОСТАНОВЛЕНИЕ
ПЛЕНУМА ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ
ОТ 15 ДЕКАБРЯ 2022 ГОДА № 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”»

В связи с вопросами, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет дать судам следующие разъяснения.

По делам о преступлениях в сфере компьютерной информации

[Законодательство Российской Федерации об информации, информационных технологиях и о защите информации]

1. Обратить внимание судов на необходимость при рассмотрении уголовных дел о преступлениях, предусмотренных статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации (далее также — УК РФ), руководствоваться положениями федеральных законов, которые регламентируют вопросы создания, распространения, передачи, защиты информации и применения информационных технологий, в част-

ности федеральных законов от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и других федеральных законов, подзаконных актов, технических регламентов, а также ратифицированных Российской Федерацией международных договоров и соглашений, посвященных указанным вопросам и борьбе с преступлениями в сфере компьютерной информации, в частности Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в городе Душанбе 28 сентября 2018 года).

Диспозиции ст. 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации (далее — УК РФ) носят бланкетный характер. Иначе говоря, для того чтобы применять данные статьи УК РФ, необходимо обращаться к анализу иных нормативных актов различного уровня.

В настоящее время существует достаточно развитое законодательство об информации, информационных технологиях и о защите информации, состоящее из федеральных законов Российской Федерации, указов Президента Российской Федерации, постановлений Правительства Российской Федерации, документов уполномоченных федеральных органов, государственных стандартов Российской Федерации в области защиты информации, а также различных нормативно-методических и руководящих документов.

К основным нормативным актам в области информационной безопасности относятся:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12 декабря 2023 г.) «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 26 июля 2017 г. № 187-ФЗ (ред. от 10 июля 2023 г.) «О безопасности критической информационной инфраструктуры Российской Федерации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 6 февраля 2023 г.) «О персональных данных»;

Федеральный закон от 29 июля 2004 г. № 98-ФЗ (ред. от 14 июля 2022 г.) «О коммерческой тайне»;

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ (ред. от 4 августа 2023 г.) «Об электронной подписи»;

Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 (ред. от 11 марта 2024 г.) «О средствах массовой информации»;

Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 24 июля 2023 г.) «О национальной платежной системе»;

Федеральный закон от 7 июля 2003 г. № 126-ФЗ (ред. от 6 апреля 2024 г.) «О связи»;

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 (ред. от 4 августа 2024 г.) «О государственной тайне;

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Непосредственное отношение к информационной безопасности имеет Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в г. Душанбе 28 сентября 2018 г.).

Дать полную характеристику всех нормативных актов в области информационной безопасности в рамках данной работы не представляется возможным, поэтому ограничимся краткой характеристикой только называемых в комментируемом Постановлении Пленума Верховного Суда Российской Федерации.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие:

при осуществлении права на поиск, получение, передачу, производство и распространение информации;

применении информационных технологий;

обеспечении защиты информации.

Третья группа общественных отношений, регулируемых данным Федеральным законом, непосредственно касается информационной безопасности.

В статье 16 Федерального закона «Об информации, информационных технологиях и о защите информации» определяется, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

на обеспечение защиты информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

реализацию права на доступ к информации.

В данной статье также сформулированы требования, предъявляемые к обладателю информации, оператору информационной системы, которые обязаны обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации;

нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» определяются понятия: информация; информационные технологии; информационная система; информационно-телекоммуникационная сеть; обладатель информации; доступ к информации; конфиденциальность информации; предоставление информации; распространение информации; электронное сообщение; документированная информация: электронный документ; оператор информационной системы; сайт в сети «Интернет»; страница сайта в сети «Интернет» (интернет-страница); доменное имя; сетевой адрес; владелец сайта в сети «Интернет»; провайдер хостинга; поисковая система (ст. 2) .

Поскольку анализируемый Закон является основным в сфере информационной безопасности, понятия и термины, даваемые в нем, подлежат применению и при анализе уголовно-правовых отношений, возникающих в сфере компьютерной информации.

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», как сказано в самом Законе, регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Понятие «критическая информационная инфраструктура» раскрывается в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» как объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

К объектам критической информационной инфраструктуры относится все то, что имеет существенное влияние на благополучие населения и состояние экономики страны. В частности, это могут быть отдельные сектора экономики — энергетика, финансы, транспорт и т. п., системы управления, средства связи, инфрастуктура населенных пунктов и т. д.

В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» проводится категорирование объектов критической информационной инфраструктуры и устанавливается ответственный за ведение реестра объектов критической информационной инфраструктуры.

В данном Законе определяется, что субъект критической информационной инфраструктуры обязан создать систему безопасности объекта критической информационной инфраструктуры, и устанавливаются требования по обеспечению безопасности объектов критической информационной инфраструктуры в зависимости от значимости объекта критической информационной инфраструктуры.

В Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 29 сентября 2018 г. определяются термины: вредоносная программа, информационные технологии, информационная система, компьютерная система, компьютерная информация, несанкционированный доступ к информации.

В соответствии с Соглашением Стороны признают в качестве уголовно наказуемых следующие деяния в сфере информационных технологий, если они совершены умышленно:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

При этом определение понятий «существенный вред», «тяжкие последствия» и «существенный ущерб» Стороны отнесли к компетенции национального законодателя.

В Соглашении также определяется порядок взаимоотношений Сторон в борьбе с преступлениями в сфере информационных технологий.

[Компьютерная информация]

2. Судам следует учитывать, что исходя из пункта 1 примечаний к статье 272 УК РФ под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее — компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках — накопителях, флеш-картах и т. п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

В пункте 2 комментируемого Постановления Пленума Верховного Суда Российской Федерации раскрывается термин «компьютерная информация». Фактически в Постановлении воспроизводится примечание к ст. 272 УК РФ. Компьютерная информация — это информация, представленная в виде электрических сигналов.

Электрические сигналы кодируются в двоичной системе двумя цифрами — 0 и 1, поскольку электронно-вычислительное устройство (компьютер) может воспринимать только наличие или отсутствие электрического импульса.

Для двоичного кода принят специальный термин — «бит». Для того чтобы из нулей и единиц появились осмысленные данные, восемь бит группируются в байт. Смысл и содержание каждого байта определяется последовательностью находящихся в нем нулей и единиц. Например, в современных программах значения байта передаются цифрами от 00000000 до 11111111.

Иначе говоря, компьютерная информация — это сведения, сообщения и данные, представленные в виде определенным образом упорядоченной группы сигналов (импульсов) или определенным образом упорядоченных участков специального устройства.

Компьютерная информация, представленная в структурированном электронном виде на каком-либо носителе, получила название «файл».

Каждый компьютерный файл имеет обязательные атрибуты, позволяющие его идентифицировать: наименование, расширение (отражающее тип хранящейся в нем информации — текстовой, графической и т. д.), размер (объем) хранимой в нем информации, время создания или изменения данного файла и др.

Из диспозиции ст. 272 УК РФ следует, что компьютерная информация в момент неправомерного доступа не обязательно должна находиться в определенном месте.

В тексте Постановления обращается внимание на то, что компьютерная информация может находиться на различных компьютерных устройствах или передаваться по каналам электрической связи. Дается открытый примерный перечень компьютерных устройств, на которых может находиться компьютерная информация в процессе совершения преступления. И это правильно, ибо научно-технический прогресс лишает законодателя возможности дать в законе исчерпывающий перечень компьютерных устройств. На смену одним компьютерным устройствам достаточно быстро приходят другие компьютерные устройства.

Однако нельзя не обратить внимание на то, что уже в настоящее время определение компьютерной информации, данное в примечании к ст. 272 УК РФ, не соответствует современному уровню развития науки и техники в сфере информационных технологий. В частности, компьютерная информация может быть представлена не только в виде электрических сигналов. Например, по оптоволоконному кабелю информация передается в виде световых сигналов. Активно разрабатываются и применяются фотонные и квантовые компьютеры, работающие на иных физических принципах.

В широко распространенных в настоящее время электронных устройствах информация представлена в виде электрических сигналов. В основе электрических сигналов лежит движение электронов. Упорядоченное движение электронов порождает электрический ток. В фотонных устройствах и компьютерах используется передача фотонов. Упорядоченное движение фотонов порождает свет. Информация в фотонных устройствах представлена в виде световых сигналов.

Квантовые компьютеры не используют в своей работе электрический сигнал или свет. Их действие не основано на использовании двоичного кода, поскольку вычисления на основе двоичного кода занимают очень много времени. Квантовые компьютеры производят вычисления мгновенно, поскольку их действие основано на использовании кубитов (квантовых битов), благодаря которым квантовые компьютеры за несколько минут решают задачи, на решение которых самые мощные электронные компьютеры потратили бы десятки тысяч лет.

Представляется, что компьютерная информация в статьях главы 28 УК РФ выступает в качестве предмета преступления.

[Компьютерные устройства]

При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом.

В пункте 2 Постановления также раскрывается понятие компьютерного устройства — электронное устройство, способное осуществлять прием, обработку, хранение и передачу информации, закодированной в форме электрических сигналов, а также иное электронное устройство, если оно позволяет осуществлять сбор и передачу компьютерной информации, взаимодействовать с иными компьютерными устройствами или с внешней средой, как промышленного, так и кустарного производства.

Тем самым Пленум Верховного Суда Российской Федерации дал весьма широкое толкование понятия компьютерного устройства, что позволяет отнести к компьютерному устройству, например, биометрический паспорт, пластиковую карту с электронным чипом, бытовые устройства, имеющие в своем составе микропроцессоры, контрольно-кассовые аппараты и т. д.

Иначе говоря, компьютерным устройством можно признать любое техническое устройство, если оно в своем составе имеет

электронный чип или микропроцессор и позволяет совершать какие-либо операции с компьютерной информацией. Например, принимать, хранить, передавать информацию, закодированную в форме электрических сигналов, осуществлять взаимодействие с иными устройствами или внешней средой. При этом функциональное назначение компьютерного устройства может быть любым. Оно не должно быть предназначено только для обработки информации.

Напомню, что в предыдущей редакции ст. 272 УК РФ говорилось о том, что компьютерная информация — это информация, находящаяся на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети. Применительно к данной редакции статьи вопрос об отнесении к компьютерным устройствам предметов хозяйственно-бытового назначения был актуален.

Поскольку в настоящее время понятие компьютерной информации не связывается с местом ее нахождения и функционалом устройства, постольку любое устройство, так или иначе предназначенное для обработки информации, закодированной в форме электрических сигналов, может быть признано компьютерным устройством.

Данный вывод в определенной степени представляется революционным, но он основывается на действующей редакции ст. 272 УК РФ и рекомендациях Пленума Верховного Суда Российской Федерации.

[Охраняемая законом компьютерная информация]

3. По смыслу части 1 статьи 272 УК РФ 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.

В пункте 3 Постановления Пленума Верховного Суда Российской Федерации дается определение компьютерной инфор-

мации, охраняемой законом. Пленум выделяет два вида информации, охраняемой законом:

информация, составляющая какую-либо тайну (государственную, коммерческую, служебную, личную, семейную, иную);

информация, которую обладатель информации признал конфиденциальной и в отношении которой установил определенные средства защиты.

В статье 5 Федерального закона «Об информации, информационных технологиях и о защите информации» информация в зависимости от категории доступа подразделяется на два вида:

общедоступную информацию;

информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Кроме того, информация в зависимости от порядка ее предоставления или распространения подразделяется:

на информацию, свободно распространяемую;

информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Следовательно, в каждом конкретном случае мы должны определять вид информации и правовой режим ее использования. При этом необходимо руководствоваться следующими обязательными правилами.

Во-первых, в соответствии со ст. 8 Федерального закона «Об информации, информационных технологиях и о защите информации» граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных законом.

Во-вторых, согласно ст. 7 данного Федерального закона общедоступная информация, т. е. общеизвестные сведения и иная информация, доступ к которой не ограничен, может использоваться любыми лицами и организациями по их усмотрению.

В-третьих, имеется вид информации, доступ к которой не может быть ограничен никем. В соответствии со ст. 8 анализируемого Федерального закона не может быть ограничен доступ:

к нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

информации о состоянии окружающей среды (экологической информации);

информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации);

иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Вопрос о том, охраняется ли информация законом, должен решаться в каждом конкретном случае на основании всех законодательно установленных требований, а не только на основании наличия специального закона.

Государственный стандарт в области информационной безопасности, ГОСТ Р 50922-2006, определяет защиту информации как деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Государственный стандарт выделяет четыре вида защиты информации (правовую, техническую, физическую и криптографическую) и семь способов защиты информации (от утечки, от несанкционированного воздействия, от непреднамеренного воздействия, от разглашения, от несанкционированного доступа, от преднамеренного воздействия, от иностранной разведки)[1].

[1] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения : национальный стандарт Российской Федерации : утв. и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст. Доступ из справ.-правовой системы «КонсультантПлюс».

Соответственно, информация ограниченного доступа, в отношении которой применяются законодательно определенные меры защиты, подлежит уголовно-правовой охране.

4. В статьях главы 28 Уголовного кодекса Российской Федерации следует понимать:

[Компьютерная программа]

под компьютерной программой, с учетом положений статьи 1261 Гражданского кодекса Российской Федерации, — 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;

В пункте 4 Постановления Пленум Верховного Суда Российской Федерации дал определение компьютерной программы, сделав ссылку на ст. 1261 Гражданского кодекса Российской Федерации (далее также — ГК РФ). В данной статье Гражданского кодекса говорится об авторских правах на компьютерные программы. Компьютерные программы имеют такой же режим гражданско-правовой охраны, как и произведения литературы. Из приведенного определения можно сделать вывод, что к компьютерной программе относится не только собственно программа, но и подготовительные материалы, полученные в ходе разработки программы, включая порождаемые программой аудиовизуальные отображения.

Программа определяется как совокупность данных и команд, предназначенных для функционирования компьютерных устройств.

Команда есть не что иное, как задание процессору компьютерного устройства на выполнение какого-либо действия, а данные — это комплекс файлов, необходимых для функционирования программы.

Составной частью компьютерной программы являются материалы, полученные в ходе разработки программы. К подготовительным материалам относятся:

« – комментарии, содержащиеся в исходном коде программы. Такие комментарии, как правило, не исполняются самим компьютером, а необходимы для других разработчиков программы

и иных лиц, которые впоследствии будут изучать исходный код самой программы;

– документация по отдельным аспектам работы программы, созданная во время разработки программы для других лиц, участвующих в ее создании, тестировании или внедрении;

– черновики исходного кода, предварительные версии программы;

– описание отдельных форматов файлов, протоколов передачи данных и иных механик работы программы»[2].

Аудиовизуальное отображение, получаемое в ходе функционирования программы, может быть интерфейсом программы.

В зависимости от типа и специфики решаемых задач различают прикладные и системные компьютерные программы. Системные программы предназначены для функционирования программно-технической системы в целом (Windows, Linux, MacOS и др.). Прикладные программы призваны решать различные прикладные задачи, например печатание текста (Word), сканирование (FineReader), составление таблиц (Excel), работа с графикой (Paint) и т. п.

Программа пишется на одном из языков программирования и представляет собой текст, в котором прописаны команды по выполнению ряда последовательных действий. Существуют разные языки программирования ((ассемблер, C++, JavaScript, Python и т. д.). Выбор языка программирования определяется решаемыми целями и задачами в силу того, что каждый язык программирования обладает своими особенностями.

[Уничтожение компьютерной информации]

под уничтожением компьютерной информации — приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;

В связи с определением понятия «уничтожение компьютерной информации» возникают вопросы. Например, можно ли уда-

[2] Алексейчук А. А. Подходы к квалификации сложного программного обеспечения // Право цифровой экономики — 2020 (16) : ежегодник-антология / рук. и науч. ред. М. А. Рожкова. М., 2020. С. 351—352.

ление информации признавать уничтожением ее, ибо при удалении информация, как правило, легко восстанавливается любым пользователем, даже если он не обладает специальными познаниями? Дело в том, что после удаления компьютерная информация не уничтожается, а просто помечается как удаленная. Вся «удаленная» информация остается на жестком диске. Как правило, операционная система настроена таким образом, что «удаленную» информацию можно посмотреть в «корзине для мусора», где хранится вся удаленная информация. Это с одной стороны. С другой стороны, уничтожить компьютерную информацию, например с винчестера, можно только или путем многократного перезаписывания информации[3], находящейся на жестком диске, или с использованием специальных программно-технических средств, или посредством физического уничтожения материального носителя информации.

Пленум Верховного Суда Российской Федерации удаление информации, т. е. фактически покушение на уничтожение информации, признал оконченным составом уничтожения компьютерной информации. При этом он подчеркнул, что уничтожение информации признается оконченным преступлением независимо от возможности ее последующего восстановления. Главное, что виновным совершено деяние, направленное на уничтожение информации, т. е. приведение всей компьютерной информации или ее части в непригодное для использования состояние. При этом, по мнению Пленума, приведение компьютерной информации в подобное состояние совершается с целью утраты возможности восстановления информации. Тем самым Пленум рекомендует признавать данное преступление совершаемым только с прямым умыслом. Представляется, что подобное ограничение сужает сферу применения ст. 272 УК РФ. Неправомерный доступ к охраняемой законом компьютерной информации может привести компьютерную информацию в непригодное для использования состояние и при косвенном умысле, и при неосторожности в виде легкомыслия или небрежности. При этом неосторожное деяние может привести к не менее тяжким последствиям, чем умышленное уничтожение компьютерной информации.

[3] Информация с дисков SSD может быть уничтожена и путем однократной перезаписи информации, так как после перезаписи данных на них не остается намагниченных участков.

[Блокировка компьютерной информации]

под блокированием компьютерной информации — воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);

При блокировании компьютерная информация не уничтожается и не повреждается, однако создаются препятствия для свободного использования данной информации законными пользователями. Блокирование может осуществляться разными способами. Пленум Верховного Суда Российской Федерации указывает на следующие:

воздействие на саму информацию;

воздействие на средства доступа к ней;

воздействие на источник хранения информации.

Срок блокирования информации может быть как постоянным, так и временным. Он не имеет уголовно-правового значения, т. е. может быть любым. Важен сам факт блокирования информации.

При блокировании информации обладатель информации, ее владелец или законный пользователь, может не знать о том, что информация кем-то была блокирована. На наш взгляд, подобное деяние все равно образует оконченный состав преступления.

В Постановлении Пленума Верховного Суда Российской Федерации говорится об искусственном затруднении или ограничении доступа законных пользователей к компьютерной информации. Выражение «искусственное затруднение или ограничение доступа» предполагает, что блокирование компьютерной информации совершается умышленно.

Однако, по нашему мнению, блокирование компьютерной информации может происходить и по неосторожности. Например, если лицо при неправомерном доступе открыло какой-либо файл, то обладатель информации в этот момент может быть лишен возможности производить с данным файлом какие-либо манипуляции. Субъект неправомерного доступа лишил обладателя информации возможности производить операции над от-

крытым файлом. При этом данное лицо не производило с компьютерной информацией таких действий, как уничтожение, модификация, копирование. Оно только знакомилось с какой-либо информацией, но в этот момент оно блокировало информацию для обладателя информации. Иначе говоря, виновный по отношению к блокированию информации может совершать преступление и по неосторожности. Он может без достаточных оснований легкомысленно рассчитывать на то, что его неправомерный доступ останется без последствий, или не предвидеть блокирование информации, но при необходимой внимательности и предусмотрительности должен был и мог предвидеть последствия своего деяния в виде блокирования информации.

[Модификация компьютерной информации]

под модификацией компьютерной информации — внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;.

Исходя из данного определения модификация компьютерной информации — это любые изменения компьютерной информации независимо от целей и задач. Представляется, что Пленум Верховного Суда Российской Федерации дал расширительное толкование понятия «модификация». Дело в том, что изменение компьютерной информации может быть направлено на ее адаптацию, которая имеет нормативно разрешенный характер.

Например, в ст. 1270 ГК РФ понятия «модификация» и «адаптация» различаются. Под модификацией в ГК РФ понимаются любые изменения программы для ЭВМ или базы данных, за исключением адаптации, т. е. изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных. Адаптация также предполагает изменение компьютерной информации, однако данное изменение не может быть признано модификацией информации. Дело в том, что современные программы бывают очень сложными. Они могут требовать доработки для использования в той или иной информационно-программной среде. Адаптация осуществляется путем декомпилирования программы или базы данных. Декомпилирование — преобразование объективного машиночитаемого кода в исходный текст, доступный для непосредственного восприятия человеком. Без адаптации добиться работоспособности про-

граммы или базы данных невозможно. Лицо, правомерно владеющее программой или базой данных или уполномоченное на их обслуживание, имеет право на изменение информации в целях ее адаптации.

Таким образом, следует признать, что модификация — это любые изменения компьютерной информации, за исключением ее адаптации. И с точки зрения уголовного закона изменение компьютерной информации в виде ее модификации уголовно наказуемо, а изменение в виде адаптации — нет.

[Копирование компьютерной информации]

под копированием компьютерной информации — перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т. п.);

По мнению Пленума Верховного Суда Российской Федерации, копирование компьютерной информации — это ее воспроизведение в любой материальной форме.

Данное определение вызывает вопросы. При воспроизведении информации должно происходить ее буквальное повторение или для ответственности за копирование информации достаточно установить, что произошло ознакомление с информацией и лицо зафиксировало, например, на бумаге, ее основной смысл? Представляется, что в последнем случае копирования информации не было. Не будет, на наш взгляд, копирования информации и в том случае, если лицо запомнило информацию и воспроизвело ее буквально на другом носителе по памяти. Кроме того, как нам представляется, нет копирования информации при ее распечатывании на принтере, фотографировании, переписывании от руки, так как информация не воспроизводится в электронном виде. Суть копирования информации — это воспроизведение ее в электронном виде на другом электронном носителе информации. А посылается компьютерная информация по электронной почте, передается по WhatsApp или отправляется в Telegram, не имеет никакого значения. Так, в ст. 1280 ГК РФ говорится, что лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообла-

дателя изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования.

Представляется, что копирование программы или базы данных и копирование компьютерной информации — это тождественные понятия.

Из анализа ст. 1280 ГК РФ однозначно можно сделать вывод о том, что копирование — это воспроизведение информации в электронном виде, а не фотографирование, распечатка или переписывание информации. В этих случаях воспроизведение информации имеется, а копирования компьютерной информации нет. Уголовная ответственность в подобных случаях не может наступать за преступления в сфере компьютерной информации, так как компьютерная информация в соответствии с примечанием к ст. 272 УК РФ представляется в форме электрических сигналов, а не какой-либо иной. Следовательно, и копирование компьютерной информации может быть только в форме электрических сигналов.

Квалификация действий лица, выполнившего фотографирование, распечатку или переписку информации с экрана компьютера, может быть осуществлена по иным статья Уголовного кодекса Российской Федерации, например по статье об ответственности за нарушение тайны переписки, нарушение служебной или коммерческой тайны и т. д.

Как абсолютно справедливо отмечает А. А. Гребеньков, копирование компьютерной информации — это перенос ее на другой носитель при сохранении представления в форме электрических сигналов независимо от средств хранения, обработки и передачи, в том числе формата представления[4].

По нашему мнению, теоретически копирование информации может быть совершено и по неосторожности, когда в результате неправомерного доступа компьютерная информация была скопирована на иное компьютерное устройство.

---

[4] Гребеньков А. А. Копирование информации как признак составов информационных преступлений // Наука, техника и образование. 2016. № 9 (27). С. 74—76.

[Нейтрализация средств защиты компьютерной информации]

под нейтрализацией средств защиты компьютерной информации — воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например, осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

В данном абзаце п. 4 Постановления Пленум Верховного Суда Российской Федерации дал толкование понятия «нейтрализация средств защиты компьютерной информации» как воздействие на средства защиты информации, а также на средства контроля эффективности защиты информации. При этом воздействие на средства защиты информации осуществляется с целью утраты ими функций как по защите компьютерной информации, так и по контролю эффективности такой защиты.

Таким образом, нейтрализация средств защиты компьютерной информации осуществляется только с прямым умыслом.

[Неправомерный доступ к компьютерной информации]

5. Применительно к статье 272 УК РФ 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 независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

Пленум Верховного Суда Российской Федерации определил, что неправомерный доступ — это «получение или использование… информации». Однако возможность получения или использования и непосредственное получение и использование информации — это не одно и то же. Например, в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» доступ к ин-

формации определяется как «возможность получения информации и ее использования».

Представляется, что Пленум в части определения неправомерного доступа к компьютерной информации дал расширительное его толкование, поскольку с точки зрения объективной стороны состава преступления, предусмотренного ст. 272 УК РФ, сам факт неправомерного доступа к компьютерной информации не дает оснований для привлечения лица к уголовной ответственности. Неправомерный доступ должен быть связан с последующими действиями по уничтожению, блокированию, модификации либо копированию информации. Например, включение чужого компьютера без намерения совершить действия, предусмотренные в ст. 272 УК РФ, на наш взгляд, не образует признаков данного состава преступления.

Иначе говоря, ознакомление с компьютерной информацией не образует признаков состава преступления, предусмотренного ст. 272 УК РФ. Однако данные действия могут содержать признаки какого-либо иного состава преступления, например предусмотренного ст. 138 УК РФ («Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»).

Видимо, в данном случае Пленум исходил из технической формулировки, где доступ определяется как *ознакомление с информацией*, ее обработка, в частности копирование, модификация или уничтожение информации[5].

Неправомерность доступа к компьютерной информации в Постановлении Пленума определена трояко:

без согласия обладателя информации;

при отсутствии необходимых для доступа полномочий;

в нарушение порядка доступа к компьютерной информации, установленного нормативными правовыми актами.

При этом доступ может осуществляться как непосредственно, так и удаленно.

Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения» оперирует понятием «правила разграничения доступа»[6]. В соответствии с пра-

[5] Средства вычислительной техники. Защита от несанкционированного доступа к информации. Термины и определения : Руководящий документ : утв. Решением председателя Гостехкомиссии России от 30 марта 1992 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[6] Там же.

вилами разграничения доступ к компьютерной информации может быть санкционированным или несанкционированным. Санкционированный доступ не нарушает правила разграничения доступа. Несанкционированный доступ к компьютерной информации нарушает правила разграничения доступа. Он может осуществляться с использованием штатных средств, представляемых средствами вычислительной техники, а также с использованием автоматизированных систем.

Суммируя сказанное, следует сделать вывод, что неправомерным признается доступ:

повлекший уничтожение, блокирование, модификацию или копирование информации;

осуществляемый а) без согласия обладателя информации;
б) при отсутствии необходимых для доступа полномочий;
в) в нарушение порядка доступа к компьютерной информации, установленного нормативными правовыми актами;

совершенный с использованием как штатных, так и специально созданных программно-технических средств;

произошедший как непосредственно, так и удаленно.

[Момент окончания преступлений, предусмотренных ст. 272 и 274 УК РФ]

6. Обратить внимание судов на то, что преступления, предусмотренные статьями 272 и 274 УК РФ, признаются оконченными, когда указанные соответственно в части 1 статьи 272 УК РФ или в части 1 статьи 274 УК РФ деяния повлекли наступление общественно опасных последствий (одного или нескольких) в виде уничтожения, блокирования, модификации либо копирования такой информации, а по статье 274 УК РФ также в виде причинения крупного ущерба.

С учетом этого в ходе рассмотрения каждого дела о преступлении, предусмотренном статьями 272 или 274 УК РФ, подлежат установлению не только совершение неправомерного доступа к компьютерной информации или нарушение соответствующих правил, но и общественно опасные последствия, возможность наступления которых охватывалась умыслом лица, осуществившего такой доступ или допустившего нарушение правил, а также наличие причинной связи между данными действиями и наступившими последствиями. Об отсутствии такой связи может свидетельствовать, в частности, наступление указанных последствий в результате технических неисправностей компьютерных устройств или ошибок при функционировании компьютерных программ.

В случае, когда наступление одних общественно опасных последствий повлекло наступление других (например, модификация информации в виде изменения пароля к учетной записи повлекла блокирование информации — ограничение доступа пользователя к этой записи), все такие последствия должны быть указаны в приговоре.

В пункте 6 Постановления Пленума Верховного Суда Российской Федерации констатируется, что преступления, предусмотренные ст. 272 и 274 УК РФ, признаются оконченными лишь в том случае, если, например, неправомерный доступ привел к последствиям в виде уничтожения, блокирования, модификации или копирования информации. Однако уничтожение, блокирование, модификация или копирование информации, причинение крупного ущерба не могут признаваться последствиями преступлений, предусмотренных ст. 272 и 274 УК РФ, если они наступили не в результате действий лица, осуществившего неправомерный доступ или нарушение правил. Иначе говоря, когда между деянием лица и наступившими последствиями нет причинной связи.

Последствия, предусмотренные ст. 272 и 274 УК РФ, могут наступить, например, в результате программно-технических неисправностей компьютерных устройств. В подобных случаях, несмотря на неправомерный доступ или нарушение соответствующих правил, а также наличие последствий, составов преступлений, предусмотренных ст. 272 и 274 УК РФ, в деянии лица не будет.

Однако если предусмотренные в законе последствия наступили в результате деяния виновного лица, то содеянное им образует признаки данных составов преступлений. При этом множественные последствия, наступившие в результате деяния виновного лица, не образуют множественности преступлений.

[Покушение на преступление, предусмотренное ст. 272 УК РФ]

7. Преступление, предусмотренное статьей 272 УК РФ, считается оконченным с момента наступления хотя бы одного из последствий, указанных в части 1 данной статьи, независимо от длительности неправомерного доступа, причин, по которым он прекратился, а также объема информации, которая была скопирована, модифицирована, блокирована или уничтожена.

Если лицо, намереваясь осуществить уничтожение, блокирование, модификацию или копирование охраняемой законом компьютерной информации, выполнило все действия, необходимые для неправомерного доступа к компьютерной информации, либо осуществило такой доступ, однако ни одно из последствий, предусмотренных частью 1 статьи 272 УК РФ, не наступило по независящим от него обстоятельствам (например, в результате срабатывания автоматизированных средств защиты информации или действий лиц, осуществляющих ее защиту), такие действия следует квалифицировать как покушение на совершение данного преступления.

В пункте 7 Постановления обращается внимание на возможность квалификации содеянного как покушения на преступление, предусмотренное ст. 272 УК РФ. Особенность данного состава преступления заключается в том, что преступление признается оконченным при наступлении любого последствия, предусмотренного в законе, независимо от того, к каким последствиям стремился виновный. Например, виновный желал скопировать компьютерную информацию, для этого он произвел блокирование средств защиты информации. Скопировать информацию ему не удалось, однако поскольку блокирование информации состоялось, то преступление, предусмотренное ст. 272 УК РФ, признается оконченным. Отсюда следует вывод, что для вменения покушения на преступление, предусмотренное ст. 272 УК РФ, необходимо установить, что, с одной стороны, последствия отсутствуют, а с другой — что виновным совершен неправомерный доступ к охраняемой законом компьютерной информации. Сложность заключается в том, что сам факт неправомерного доступа, при отсутствии доказательств того, что лицо намеревалось совершить уничтожение, блокирование, модификацию или копирование компьютерной информации, не может быть квалифицирован как покушение на преступление, предусмотренное ст. 272 УК РФ.

[Вредоносные компьютерные программы или иная компьютерная информация]

8. В статье 273 УК РФ к иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить до-

стижение целей, перечисленных в части 1 статьи 273 УК РФ, например ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Уголовную ответственность по статье 273 УК РФ влекут действия по созданию, распространению или использованию только вредоносных компьютерных программ либо иной компьютерной информации, то есть заведомо для лица, совершающего указанные действия, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Статьей 273 УК РФ предусматривается уголовная ответственность за сам факт создания, распространения или использования программ или иной информации, предназначенных для уничтожения, модификации, блокирования, копирования или нейтрализации средств защиты информации.

В пункте 8 Постановления раскрывается понятие «иная компьютерная информация». Пленум Верховного Суда Российской Федерации к иной вредоносной компьютерной информации относит любые сведения, которые не являются компьютерной программой, однако позволяют обеспечить наступление указанных в законе последствий. В качестве примера приводятся такие сведения, как ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы кодов компьютерных программ, способные к причинению последствий в виде уничтожения, модификации, блокирования, копирования или нейтрализации средств защиты информации.

Представляется, что иная вредоносная компьютерная информация — это компьютерная информация, которая во взаимодействии с иными компьютерными программами способна приводить к вредоносным последствиям.

[Объективная сторона преступления, предусмотренного ст. 273 УК РФ]

9. Судам следует иметь в виду, что объективная сторона преступления, предусмотренного статьей 273 УК РФ, состоит в выполнении одного или нескольких перечисленных в ней действий.

Создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютер-

ной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты.

В пункте 9 Постановления дается определение создания вредоносных компьютерных программ или иной вредоносной компьютерной информации.

В соответствии с данным определением создание — это деятельность, направленная на получение вредоносной программы или вредоносной компьютерной информации. Технически создание вредоносной программы или вредоносной информации может осуществляться с «нуля» или путем внесения изменений в существующие программы. При этом вредоносность программы или информации определяется их способностью причинять указанные в законе последствия в виде несанкционированного уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты, а также несанкционированного доступа к охраняемой законом компьютерной информации.

[Момент окончания преступления, предусмотренного ст. 273 УК РФ]

10. Для квалификации действий лица по части 1 статьи 273 УК РФ как оконченного преступления достаточно установить 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.

Создание вредоносной компьютерной программы признается оконченным преступлением независимо от получения готовой к применению программы. Пленум Верховного Суда Российской Федерации указывает на то, что преступление в виде создания вредоносной программы признается оконченным с момента создания хотя бы части (фрагмента) кода вредоносной компьютерной программы. Главный критерий — это возможность с помощью данного кода осуществлять неправомерный доступ к компьютерной информации.

При отсутствии такого кода преступление, по рекомендации Пленума, должно подлежать квалификации как оконченное преступление на основании создания иной компьютерной информации.

Таким образом, Пленум рекомендует признавать создание вредоносной компьютерной программы или иной вредоносной компьютерной информации оконченным преступлением с момента начала создания соответствующей программы или соответствующей компьютерной информации. Поскольку создание программы или информации может толковаться и как процесс, и как результат деятельности, постольку моментом окончания данного преступления и признается начало процесса.

Обращает на себя внимание не совсем удачное формулирование положений Постановления. Пленум почему-то связывает момент окончания создания вредоносной компьютерной программы с началом написания кода программы, направленной на осуществление неправомерного доступа. Хотя логичнее было указать на начало создания кода программы, предназначенной для причинения указанных в законе последствий.

Кроме того, на наш взгляд, не всякое начало написания кода вредоносной программы может быть признано созданием иной вредоносной компьютерной информации. Не всегда начало написания кода программы позволяет обеспечить достижение целей в виде указанных в законе последствий, как это требуется для признания компьютерной информации вредоносной.

Поэтому в тексте Постановления Пленума следовало бы увязать момент окончания преступления с моментом начала создания соответствующей программы или компьютерной информации с соответствующими целями.

[Распространение вредоносных программ или информации]

11. Распространение вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами.

Как указывается в пункте 11 Постановления Пленума Верховного Суда Российской Федерации, распространение вредоносных программ или вредоносной компьютерной информации может осуществляться любым способом. Суть распространения состоит в предоставлении доступа к вредоносным программам или информации иным лицам.

Чаще всего распространение вредоносных программ или информации происходит путем использования:

электронной почты, когда злоумышленник распространяет письма с вложениями или ссылки на сайты с вредоносными программами или информацией;

зараженных носителей информации;

всплывающих окон, содержащих вредоносную информацию или программу;

уязвимостей в системе безопасности;

дефектов в программном обеспечении или оборудовании;

скрытой загрузки;

несанкционированного доступа к компьютеру или сетям;

однородности компьютерных сетей, работающих под управлением одной операционной системы;

комбинирования различных вредоносных программ[7].

[Использование вредоносных программ или информации]

Под использованием вредоносных компьютерных программ или иной вредоносной компьютерной информации судам следует понимать действия, состоящие в их применении, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты.

Если действия виновного лица содержат в себе элементы как распространения, так и использования вредоносной компьютерной программы или иной вредоносной компьютерной информации, оба эти действия должны быть указаны в приговоре.

Использование вредоносных компьютерных программ или вредоносной компьютерной информации — это их применение для достижения последствий, указанных в законе.

[7] См. подробнее: URL: https://www.kaspersky.ru/resource-center/threats/types-of-malware?ysclid=lwdzlmx3bu48586141 (дата обращения: 20.05.2024).

Пленум Верховного Суда Российской Федерации указывает, что все действия, связанные с вредоносными программами и информацией, должны быть указаны в приговоре. Виновный может как создавать, так и распространять и использовать вредоносные программы и информацию. При этом, если речь идет о конкретной вредоносной программе или информации, не образуется множественности преступлений. Однако если виновный создавал одну вредоносную программу, распространял другую, а использовал третью, то, на наш взгляд, в этом случае содеянное должно квалифицироваться по совокупности трех преступлений.

[Непреступные цели использования вредоносных программ или информации]

Следует иметь в виду, что не образует состава преступления использование такой программы или информации лицом на принадлежащих ему компьютерных устройствах либо с согласия собственника компьютерного устройства, не преследующее цели неправомерного доступа к охраняемой законом компьютерной информации и не повлекшее несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты (например, в образовательных целях либо в ходе тестирования компьютерных систем для проверки уязвимости средств защиты компьютерной информации, к которым у данного лица имеется правомерный доступ), равно как и создание подобных программ для указанных целей.

Использование вредоносных программ или информации необходимо отличать от случаев похожих, когда отсутствуют признаки состава преступления, предусмотренного ст. 273 УК РФ. В Постановлении Пленума указывается на следующие обстоятельства:

использование программы или информации осуществлялось на собственном компьютерном устройстве;

оно осуществлялось с согласия собственника компьютерного устройства;

использование программы или информации не преследовало цели неправомерного доступа к охраняемой законом компьютерной информации;

использование программы или информации не повлекло несанкционированного уничтожения, блокирования, модифика-

ции, копирования компьютерной информации или нейтрализации средств ее защиты;

использование программы или информации осуществлялось в образовательных целях либо в ходе тестирования средств защиты информации в компьютерных системах, к которым у лица имеется правомерный доступ.

Создание программ или информации для образовательных целей или для тестирования средств защиты информации также не образует признаков состава преступления, предусмотренного ст. 273 УК РФ.

Таким образом, Пленум увязал отсутствие состава преступления, предусмотренного ст. 273 УК РФ, в виде создания и использования вредоносных компьютерных программ или компьютерной информации с отсутствием неправомерных целей, а также совершением указанных действий на собственных устройствах или на устройствах, в отношении которых имелось разрешение их собственника.

Обращает на себя внимание то, что распространение вредоносных компьютерных программ или информации всегда признается преступлением, независимо от целей их распространения.

[Нарушение правил, предусмотренных в ст. 274 УК РФ]

12. При квалификации действий лица по статье 274 УК РФ судам необходимо установить, какие именно правила из перечисленных в части 1 данной статьи были нарушены, а также возложена ли на это лицо обязанность соблюдать указанные правила.

Данные правила могут быть установлены федеральными законами и подзаконными нормативными правовыми актами, а также инструкциями или иными локальными нормативными актами организаций, если они приняты в развитие указанных законов и подзаконных актов, не противоречат им и не изменяют их содержание. Обязанность соблюдения правил, установленных локальным нормативным актом, должна быть доведена до сведения лица, которому вменяется совершение соответствующего преступления (например, при подписании трудового договора, соглашения на использование сетей или оборудования либо отдельного акта ознакомления с такими правилами).

В пункте 12 Постановления Пленума Верховного Суда Российской Федерации обращается внимание на то, что суды должны в каждом конкретном случае устанавливать, какие именно

правила из перечисленных в законе были нарушены. В части 1 ст. 274 УК РФ говорится о следующих правилах:

правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации;

правила эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования;

правила доступа к информационно-телекоммуникационным сетям.

В Постановлении определяется, что данные правила могут быть установлены:

федеральными законами;

подзаконными нормативными актами;

инструкциями или иными локальными нормативными актами организаций, если они приняты в развитие указанных законов и подзаконных актов, не противоречат им и не изменяют их содержание.

Кроме того, Пленум Верховного Суда Российской Федерации обращает внимание на то, что обязанность соблюдения тех или иных правил должна быть доведена до сведения лица, которому инкриминируется преступление, связанное с нарушением правил.

Представляется, что ознакомление с обязанностью соблюдения соответствующих правил должно удостоверяться подписью лица, обязанного соблюдать данные правила. В комментируемом Постановлении приводятся примеры, когда возможно доведение информации до сведения обязанного лица. Это может происходить при подписании:

трудового договора;

соглашения на использование сетей или оборудования;

отдельного акта ознакомления с такими правилами.

[Квалификация преступления по ч. 1 ст. 274.1 УК РФ]

13. Действия лица квалифицируются по части 1 статьи 274.1 УК РФ, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в статье 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по статье 273 УК РФ.

Преступление, предусмотренное ч. 1 ст. 274.1 УК РФ, аналогично преступлению, предусмотренному ст. 273 УК РФ. Отличие заключается в том, что предметом преступления, описанного ст. 274.1 УК РФ, являются объекты критический информационной инфраструктуры. Критическая информационная инфраструктура определяется в законе как объекты критической информационной инфраструктуры, а также электросети, используемые для организации взаимодействия таких объектов. Под объектами критической информационной инфраструктуры понимаются:

информационные системы;

информационно-телекоммуникационные сети;

автоматизированные системы управления субъектов критической информационной инфраструктуры.

В Постановлении обращается внимание на то, что вредоносные программы и иная вредоносная информация должны быть заведомо предназначены для незаконного воздействия на объекты критической информационной инфраструктуры. В противном случае содеянное должно быть квалифицировано по ст. 273 УК РФ.

[Квалификация преступления по ч. 2 ст. 274.1 УК РФ]

При этом следует учитывать, что использование вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается частью 2 статьи 274.1 УК РФ и дополнительной квалификации по статье 273 УК РФ не требует.

Преступление, предусмотренное ч. 2 ст. 274.1 УК РФ, аналогично преступлению, предусмотренному ст. 272 УК РФ. Отличие в том, что по ч. 2 ст. 274.1 УК РФ квалифицируется неправомерный доступ, осуществляемый к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре. Сам неправомерный доступ может быть осуществлен как с использованием вредоносных компьютерных программ либо иной вредоносной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру, так и с ис-

пользованием иных вредоносных программ или вредоносной компьютерной информации.

Независимо от предназначения вредоносных программ или информации при посягательстве на критическую информационную инфраструктуру деяние виновного образует признаки состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ. Для оконченного состава преступления требуется наступление последствий в виде причинения вреда критической информационной инфраструктуре Российской Федерации.

[Тяжкие последствия как квалифицирующий признак преступлений, предусмотренных ст. 272—274.1 УК РФ]

14. Под тяжкими последствиями как квалифицирующим признаком в статьях 272—274.1 УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т. п.

В случае, когда подсудимому вменяется признак создания угрозы наступления тяжких последствий, должна быть установлена реальность такой угрозы.

Тяжкие последствия или создание угрозы их наступления в качестве квалифицирующего признака предусмотрены в ч. 4 ст. 272 УК РФ, ч. 3 ст. 273 УК РФ, ч. 2 ст. 274 УК РФ. В части 5 ст. 274.1 УК РФ повышенная ответственность установлена только за причинение тяжких последствий, без создания угрозы их наступления.

В пункте 14 Постановления Пленума достаточно подробно раскрыт характер тяжких последствий. Они, как правило, связаны с нарушением работы предприятия, учреждения, организации в целом, получением доступа к информации, охраняемой специальным законом, причинение смерти или тяжкого вреда здоровью людей.

Приведенный перечень последствий является открытым. Суд может отнести к тяжким последствиям и иные, которые, по его мнению, могут быть признаны тяжкими.

При вменении такого квалифицирующего признака, как создание угрозы наступления тяжких последствий, необходимо исходить, как рекомендует Пленум, из реальности угрозы.

К сожалению, Пленум Верховного Суда Российской Федерации не дал определения реальности угрозы.

Теоретически выделяют три вида угрозы: потенциальная, реальная и реализованная. Потенциальная угроза представляет собой абстрактную возможность наступления последствий. Она может реализоваться лишь при наличии определенных обстоятельств, которых пока нет в действительности. При реальной угрозе обстоятельства, могущие за собой повлечь наступление последствий, предусмотренных в законе, имеются в действительности. Реальность угрозы причинения тяжких последствий заключается в ее способности причинить последствия, предусмотренные законом. Реальность угрозы наступления последствий предполагает, что опасность наступления тяжких последствий имеется в наличии

[Совокупность преступлений, предусмотренных ст. 272 и 273 УК РФ]

15. Судам следует иметь в виду, что, когда вредоносная компьютерная программа использовалась для осуществления неправомерного доступа к компьютерной информации и это повлекло наступление последствий, предусмотренных частью 1 статьи 272 УК РФ, действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ.

В данном пункте Постановления Пленума обращается внимание на совокупность преступлений, совершаемых в сфере компьютерной информации. Нормы о преступлениях, предусмотренных ст. 272 и 273 УК РФ, имеют разную законодательную конструкцию, поэтому предполагается разный момент окончания преступлений. Данное обстоятельство обязательно должно учитываться при квалификации преступлений. Преступление, предусмотренное ст. 273 УК РФ, признается оконченным с момента совершения названного в законе деяния (создание, использование, распространение вредоносных программ или иной вредоносной компьютерной информации). Это преступление с так называемым формальным составом. Сам факт использования вредоносной программы признается оконченным преступлением независимо от наступления последствий.

Следовательно, использование вредоносной программы с целью осуществления неправомерного доступа к охраняемой ком-

пьютерной информации, повлекшее любое из указанных в законе последствий (уничтожение, блокирование, модификация, копирование информации), требует квалификации содеянного по совокупности преступлений, предусмотренных ст. 273 и 272 УК РФ.

[Совокупность преступлений, предусмотренных ст. 272—274.1 УК РФ, а также иных преступлений]

16. Если действия, предусмотренные статьями 272—274.1 УК РФ, выступали способом совершения иных преступлений (например, модификация охраняемой законом компьютерной информации производилась с целью нарушения авторских или смежных прав, нарушения неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений либо неправомерный доступ к ней осуществлялся с целью совершения кражи или мошенничества), они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями Уголовного кодекса Российской Федерации. В частности, мошенничество в сфере компьютерной информации (статья 159.6 УК РФ), 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.

В пункте 16 Постановления Пленума так же обращается внимание на совокупность преступлений, однако, в отличие от предыдущего пункта, не совокупность двух и более преступлений в сфере компьютерной информации, а совокупность преступлений в сфере компьютерной информации и иных преступлений.

В подобных случаях речь идет о том, что преступления в сфере компьютерной информации выступают способом совершения иных преступлений. Поскольку сфера ответственности за преступления, предусмотренные в главе 28 УК РФ, ограничена действиями, совершаемыми в сфере компьютерной информации, постольку иные преступные деяния требуют дополнительной квалификации. Они имеют иные объект и объективную сторону посягательства.

Однако в отношении хищения, ответственность за совершение которого установлена ст. 159.6 УК РФ, это не совсем так.

Норма, изложенная в ст. 159.6 УК РФ, является специальной по отношению к норме ст. 272 УК РФ. Оба преступления за-

ключаются в осуществлении неправомерного доступа к охраняемой законом компьютерной информации посредством использования программно-технических средств, т. е. ответственность установлена за манипуляции с компьютерной информацией, приводящие к уничтожению, блокированию, модификации или копированию компьютерной информации.

При совпадении объективной стороны имеется отличие в объекте посягательства. Поэтому и в случае совершения хищения с использованием программно-технических средств требуется квалификация по совокупности преступлений, предусмотренных ст. 272 и 159.6 УК РФ. Если же виновный при этом использовал вредоносные программу или иную компьютерную информацию для обеспечения доступа или преодоления средств защиты, то содеянное требует, помимо составов, предусмотренных ст. 159.6 и 272 УК РФ, вменять состав преступления, предусмотренный ст. 273 УК РФ.

По делам о преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «интернет»

[Электронные и информационно-телекоммуникационная сети]

17. Под информационно-телекоммуникационной сетью в соответствующих статьях Особенной части Уголовного кодекса Российской Федерации 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.

Для признания наличия в действиях подсудимого признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей 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.

В общей структуре преступности в России преступления, совершенные с использованием информационно-телекоммуникационных технологий (далее — киберпреступления[8]), характеризуются беспрецедентным в сравнении с другими видами преступлений ежегодным увеличением удельного веса. В 2023 году зарегистрировано 677 тыс. таких преступлений, что на 29,7 % больше, чем в 2022 году. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,5 % в 2022 году до 34,8 % в 2023 году[9]. На прошедшем в Генеральной прокуратуре Российской Федерации в июле 2020 года заседании Координационного совещания руководителей правоохранительных органов было отмечено, что за последние 5 лет число киберпреступлений возросло в 25 раз, а их раскрываемость остается низкой (25 %)[10]. С использованием информационно-телекоммуникационных технологий совершается каждое третье преступление.

В числе киберпреступлений не только посягательства, которые в силу специфики признаков состава преступления могут быть совершены не иначе как с использованием информационно-телекоммуникационных технологий (преступления в сфере компьютерной информации, хищение безналичных и электрон-

[8] В учебно-методическом пособии «Серия университетских модулей: Киберпреступность», разработанном под эгидой ООН, киберпреступление определяется как действие, нарушающее закон, которое совершается с использованием информационно-коммуникационных технологий (ИКТ) и либо нацелено на сети, системы, данные, веб-сайты и (или) технологии, либо способствует совершению преступления (https://www.unodc.org/e4j/ru/cybercrime/module-1/key-issues/cybercrime-in-brief.html). См. также: Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ-Правоведъ. 2019. № 4 (91). С. 78—82.

[9] Состояние преступности в России за январь—декабрь 2023 года : сборник / МВД России, ФКУ ГИАЦ // Министерство внутренних дел Российской Федерации : офиц. сайт. URL: https://мвд.рф (дата обращения: 16.01.2024).

[10] Генеральная прокуратура Российской Федерации : офиц. сайт. URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 16.01.2024).

ных денежных средств), но и все чаще разного рода общеуголовные (террористическая деятельность, незаконный оборот наркотических средств и психотропных веществ, порнографических материалов, оружия и боеприпасов, развратные действия, организация занятия проституцией и пр.), экономические (незаконная организация и проведение азартных игр, легализация (отмывание) имущества, приобретенного преступным путем, и пр.), государственные (государственная измена и шпионаж, преступления экстремистской направленности и пр.), служебные (злоупотребление должностными полномочиями, взяточничество и пр.) и другие преступления. Совершение некоторых преступлений с использованием информационно-телекоммуникационных технологий, например развратных действий, убийств[11], было сложно представить до появления широкого доступа к сети «Интернет» и значительного распространения беспроводных средств связи индивидуального пользования, позволяющих в кратчайшие сроки доносить большие объемы информации, в том числе с элементами негативной суггестии, до конкретных получателей.

Характерным признаком киберпреступлений является способ их совершения — с использованием информационно-телекоммуникационных сетей. В ряде составов преступлений данный способ посягательства является конститутивным (криминообразующим) признаком (например, ч. 3 ст. 137, ст. 159.6, ст. 171.2, ст. 185.3, ст. 282 УК РФ). Чаще всего совершение преступления с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») предусматривается в качестве квалифицирующего признака состава преступления, являющегося одним из основных средств дифференциации уголовной ответственности. В настоящее время такие составы преступлений зафиксированы более чем в двух десятках статей Особенной части УК РФ. Некоторым вопросам квалификации таких преступлений и посвящены разъяснения Пленума Верховного Суда Российской Федерации, содержащиеся в пп. 17—24 настоящего Постановления.

---

[11] Таковы широко известные случаи распространения в сети «Интернет» инструкции «Как стать феей огня из „Винкс" в домашних условиях?», явно рассчитанной на массовое убийство детей и их близких (см.: Шарапов Р. Д. Квалификация преступлений, связанных с вовлечением в самоубийство и иное опасное для жизни поведение // Уголовное право. 2017. № 6. С. 78).

Вместе с тем действующее уголовное законодательство характеризуется отсутствием единого подхода к технике нормативного описания соответствующего способа преступления. В одних случаях в содержание данного способа наряду с информационно-телекоммуникационными сетями, в том числе сетью «Интернет», включается использование электронных сетей (ч. 1 ст. 185.3, ч. 2 ст. 205.2, п. «б» ч. 2 ст. 228.1, ч. 11 ст. 258.1, ч. 2 ст. 260.1 УК РФ и др.). В других случаях описание способа киберпреступления исчерпывается указанием на использование информационно-телекоммуникационных сетей (включая сеть «Интернет»), а об электронных сетях не упоминается (ст. 110.2, ч. 2 ст. 128.1, п. «б» ч. 3 ст. 133, п. «в» ч. 2 и п. «в» ч. 4 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222.1, п. «д» ч. 2 ст. 230 УК РФ и др.). Такая непоследовательность создавала затруднения в правоприменительной практике. С одной стороны, правоприменитель считал необходимым искать различия между электронными и информационно-телекоммуникационными сетями в условиях, когда понятие электронной сети в законодательстве не определено, с другой стороны, ставился вопрос о возможности вменения квалифицирующего признака, предусматривающего использование информационно-телекоммуникационных сетей, в том числе сети «Интернет», по делам о преступлениях, совершенных с использованием электронных сетей (например, телефонной связи)[12].

Так, по уголовному делу о покушении на сбыт наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») государственный обвинитель заявил об исключении из приговора квалифицирующего признака «с использованием электронных сетей» на том основании, что подсудимым В. совершены преступления посредством использования программного приложения Telegram в сети «Интернет». Суд не согласился с доводом, обосновав это тем, что «Интернет — это международная глобальная компьютерная сеть. В свою очередь, компьютерная (электронная) сеть — это система обмена информацией. Таким

[12] См. подробно: 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») // Криминалистъ. 2021. № 3 (36). С. 32—38.

образом, намерение В. передать информацию по сети „Интернет" одновременно связано и с использованием электронной сети»[13].

Среди доктринальных суждений превалирует суждение о том, что понятия электронной и информационно-телекоммуникационной сети совпадают[14].

В абзаце 2 п. 17 Постановления Пленум устранил описанные затруднения, разъяснив, что для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. Поэтому преступление надлежит признавать совершенным с использованием информационно-телекоммуникационной сети вне зависимости от технических особенностей сети, которую использовал виновный («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» — абз. 3 п. 17 Постановления).

Для целей квалификации преступлений Пленум продублировал определение информационно-телекоммуникационной сети, которое содержится в 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. Данное понятие одинаково применимо ко всем статьям Особенной части УК РФ, в которых предусматривается соответ-

---

[13] Апелляционное определение Верховного суда Чувашской Республики от 5 сентября 2017 г. по делу № 22-2023/2017. Доступ из справ.-правовой системы «КонсультантПлюс».

[14] 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 ; Токманцев Д. В. К вопросу о понятии и моменте окончания незаконного сбыта наркотиков, совершенного с использованием сети интернет или других информационно-телекоммуникационных сетей // Вестник Сибирского юридического института МВД России. 2022. № 3 (48). С. 77—84 ; Куликов А. В., Шелег О. А. Эффективность применения квалифицирующего признака «использование информационно-коммуникационных технологий» в составах преступлений, связанных с распространением наркотических средств, и его влияние на назначение наказания // Известия Тульского государственного университета. Экономические и юридические науки. 2023. №. 3. С. 28—36.

ствующий признак состава преступления. Характерным признаком такой сети является передача информации, доступ к которой осуществляется с использованием средств вычислительной техники. Под средствами вычислительной техники понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[15]. Речь идет о компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (п. 1 примечания к ст. 272 УК РФ). В литературе средства вычислительной техники приравниваются в своем значении к компьютеру[16].

Исключается возможность считать информационно-телекоммуникационной сетью линию связи, по которой передается информация не в форме электрических сигналов без использования средств вычислительной техники (компьютерных устройств) (традиционная почтовая связь, обмен световыми сигналами, связь при помощи беспилотных летательных аппаратов или животных и т. п.).

Из законодательной конструкции составов киберпреступлений следует, что сеть «Интернет» включается в понятие электронных и информационно-телекоммуникационных сетей (в статьях УК РФ почти повсеместно используется дописка — (включая сеть «Интернет»). Следовательно, указанные сети не исчерпываются Интернетом. Поэтому Пленум специально подчеркнул, что сеть «Интернет» является одним из видов электронных и информационно-телекоммуникационных сетей.

В действующем законодательстве Российской Федерации не содержится легального определения понятия сети «Интернет». Такое определение имеется в Модельном законе об основах регулирования Интернета стран СНГ: «Интернет — глобальная

---

[15] Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : Руководящий документ : утв. Решением председателя Гостехкомиссии России 30 марта 1992 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[16] Летелкин Н. В. Об определении признаков и понятия «информационно-телекоммуникационная сеть» в отечественном уголовном законодательстве // Вопросы российского и международного права. 2018. Т. 8, № 3А. С. 218.

информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц»[17]. Признается, что эта дефиниция наиболее полно и точно отражает функциональные особенности, информационно-технологические, технические и социальные аспекты рассматриваемого явления, кроме того, находит закрепление в официальном акте межгосударственного органа[18]. Преступление следует квалифицировать как совершенное с использованием сети «Интернет» независимо от сегмента этой информационно-телекоммуникационной сети, который задействовал преступник (например, DarkNet).

В числе других видов электронных и информационно-телекоммуникационных сетей, использование которых предусматривается в качестве способа киберпреступлений, Пленум выделяет сети операторов связи, локальные сети организаций, домашние локальные сети. Однако наиболее важной представляется заключительная часть разъяснений комментируемого пункта постановления, где сказано, что электронными и информационно-телекоммуникационными сетями могут признаваться 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.

---

[17] Модельный закон об основах регулирования Интернета : принят в г. Санкт-Петербурге 16 мая 2011 г. Постановлением 36-9 на 36-ом пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ. Доступ из справ.-правовой системы «КонсультантПлюс».

[18] Сухопаров В. П. Теоретические и нормативно-правовые подходы к определению понятия сети Интернет // Конституционное и муниципальное право. 2022. № 2. С. 52—56 ; Дерхо Д. С. Правовое регулирование оказания услуг по предоставлению доступа к сети Интернет в РФ / подготовлен для системы КонсультантПлюс». 2023. Доступ из справ.-правовой системы «КонсультантПлюс».

В итоге информационно-телекоммуникационной сетью для целей квалификации преступлений следует считать любую линию связи (проводную и беспроводную, локальную и территориально-распределенную) между двумя или более компьютерными устройствами.

[Сайт в сети «Интернет»]

18. При квалификации действий, совершенных с использованием сети «Интернет», судам 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» (далее также — интернет-страница) — часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет».

В настоящем пункте Постановления Пленум воспроизвел содержащиеся в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятия некоторых информационно-телекоммуникационных средств, используемых в сети «Интернет» и часто применяемых виновными при совершении киберпреступлений в интернет-пространстве (хищений чужого имущества с использованием фишинговых сайтов, поддельных интернет-магазинов; публичных призывов к осуществлению террористической или экстремисткой деятельности, размещенных на сайтах и интернет-страницах; сбыта наркотиков посредством интернет-сайтов[19] и пр.).

В отличие от упомянутого Федерального закона, в котором сайт в сети «Интернет» определяется как совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к кото-

[19] По данным Роскомнадзора, более 104 000 интернет-страниц с информацией о наркотиках было заблокировано в России в 2023 году, это на 25 % больше, чем в 2022 году (78 800 страниц). См.: Тюняева (Бочкарёва) М. В рунете резко выросло число блокировок сайтов за публикации о наркотиках // Ведомости. 2024. 16 янв. URL: https://www.vedomosti.ru/techology/articles/2024/01/16/1015198-v-runete-rezko-viroslo-chislo-blokirovok-saitov-za-publikatsii-o-narkotikah (дата обращения: 18.01.2024).

рой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет», в аналогичном определении, предлагаемом Пленумом, электронные вычислительные машины заменены на компьютерные устройства. Тем самым вновь подчеркнута неразрывная связь информационно-телекоммуникационной сети, включая сеть «Интернет», с компьютерными устройствами.

Почти дословно воспроизведено понятие страницы сайта в сети «Интернет» (интернет-страницы), приведенное в п. 14 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации».

Другие специальные термины, которые входят в содержание разъясняемых понятий, также определены в Федеральном законе «Об информации, информационных технологиях и о защите информации». В частности, доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет» (п. 15 ст. 2); сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему (п. 16 ст. 2); владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте (п. 17 ст. 2).

Праворазъяснительные положения о сайте и странице сайта в сети «Интернет» призваны обеспечить единство понимания этих терминов, которые часто употребляются в описательно-мотивировочной части судебных решений.

[Место совершения преступлений с использованием электронных сетей]

19. 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 (напри-

мер, при публичных призывах к осуществлению экстремистской деятельности — территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого лица, или использовалось компьютерное устройство для размещения в сети «Интернет» информации, содержащей призывы к осуществлению экстремистской деятельности).

В процессе уголовного судопроизводства по делам о преступлениях, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», ответ на вопрос о месте совершения такого преступления вызывает затруднения, обусловленные особенностями дистанционного способа посягательства. Особенности эти состоят в том, что преступник, совершающий противоправные действия с использованием компьютерных устройств, может находиться в одном географическом месте, тогда как общественно опасные последствия наступают в другом месте, а потерпевший находится в третьем месте. Например, по уголовным делам о хищениях безналичных денег, которые совершаются с использованием сети «Интернет», суды демонстрировали различные подходы к решению этого вопроса. Местом преступления признавалось место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или где открыт банковский счет, которым может распоряжаться обвиняемый, адрес места нахождения владельца денежных средств, местонахождение платежных терминалов (место нахождения серверного оборудования), из которых потерпевшие осуществили перевод электронных денежных средств, место нахождения лица, подозреваемого в совершении преступления, равно как и место, где были обнаружены следы преступления, место, где имущество стало подконтрольным виновному, место, где совершены действия, направленные на безналичный перевод денежных средств[20].

Пленум разъяснил, что местом совершения такого преступления является место совершения виновным противоправных действий, входящих в объективную сторону состава преступления. Из чего следует, что территориальная локализация других признаков объективной стороны состава преступления (место

[20] Степанов П. П., Грибанова Д. В. Место совершения хищения безналичных денег и территориальная подсудность уголовного дела // Уголовное право. 2023. № 9. С. 49—62.

наступления общественно опасных последствий либо характеризующее причинную связь место нахождения потерпевшего, на которого виновный воздействует путем передачи компьютерной информации[21], место нахождения компьютерных устройств, используемых виновным удаленно) не имеет значения для определения места преступления. Для правильного уяснения правовой позиции приведен пример определения места совершения преступления, предусмотренного ч. 2 ст. 280 УК РФ (территория, на которой лицом использовалось компьютерное устройство).

Одновременно с принятием комментируемого Постановления Пленум внес изменения аналогичного свойства в два других постановления, в которых ранее разъяснялся вопрос о месте окончания мошенничества и кражи, предметом которых являются безналичные или электронные денежные средства (местом окончания таких преступлений, как разъяснялось до внесения соответствующих изменений, является место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета). Местом совершения кражи с банковского счета, а равно кражи в отношении электронных денежных средств (п. «г» ч. 3 ст. 158 УК РФ), исходя из особенностей предмета и способа данного преступления, является, как правило, место совершения лицом действий, направленных на незаконное изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет) (п. 25.2 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2002 г. № 29 (ред. от 15 декабря 2022 г. «О судебной практике по делам о краже, грабеже и разбое»). Местом совершения мошенничества, состоящего в хищении безналичных денежных средств, исходя из особенностей предмета и способа данного преступления, является, как прави-

[21] Действия потерпевшего, введенного в заблуждение виновным, по передаче последнему имущества (права на имущество), согласно имеющемуся мнению, находятся за границами деяния, вменяемого субъекту мошенничества, становясь уже частью причиняющей цепочки (Есаков Г. А. Место совершения преступления при хищении: новый подход судебной практики // Уголовное право. 2023. № 3. С. 54—60).

ло, место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств (абз. 3 п. 5 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Принятые разъяснения адресованы судам для определения территориальной подсудности уголовных дел, что подтверждается не только прямым упоминанием об этом в комментируемом Постановлении, но и указаниями о необходимости определять подсудность уголовного дела о краже и мошенничестве, предметом которых являются безналичные или электронные денежные средства, по месту совершения лицом действий, направленных на незаконное изъятие денежных средств (п. 25.3 постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2022 г. № 29 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о краже, грабеже и разбое», п. 5.1 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о мошенничестве, присвоении и растрате»).

Очевидно, что эти разъяснения пригодны для использования органами предварительного расследования при установлении места совершения деяния, содержащего признаки преступления, в зависимости от которого определяется территориальная подследственность уголовного дела (ч. 1 ст. 152 Уголовно-процессуального кодекса Российской Федерации (далее также — УПК РФ)).

В итоге, если, например, «при совершении лицом в городе А. в отношении потерпевшего, находившегося в тот момент в городе Б., обманных действий, в результате которых потерпевший переводит денежные средства с банковского счета, который находится в городе М., на счет банка в городе С., расследоваться мошенничество должно в городе А., там же и должно быть рассмотрено судом»[22].

Определение Пленумом места совершения преступления, совершенного с использованием информационно-телекоммуникационной сети, соответствует уже известной правовой позиции высшей судебной инстанции по вопросу о месте совершения

[22] Степанов П. П., Грибанова Д. В. Указ. соч.

административного правонарушения. Таковым является место совершения противоправного действия независимо от места наступления его последствий, а если такое деяние носит длящийся характер, — место окончания противоправной деятельности, ее пресечения; если правонарушение совершено в форме бездействия, то местом его совершения следует считать место, где должно было быть совершено действие, выполнена возложенная на лицо обязанность (абз. 17 п. 3 постановления Пленума Верховного Суда Российской Федерации от 24 марта 2005 г. № 5 (ред. от 23 декабря 2021 г.) «О некоторых вопросах, возникающих у судов при применении Кодекса Российской Федерации об административных правонарушениях»).

В совокупности приведенные разъяснения выражают идею о том, что место совершения преступления определяется временем его совершения, и наоборот. Эти неразрывно связанные между собой физические величины характеризуют юридическое темпорально-пространственное измерение преступления как правового явления. Местом совершения преступления логично считать то место, в котором протекает время преступления. Поскольку понятие последнего нормативно определено (ч. 2 ст. 9 УК РФ), то местом совершения преступления надлежит считать то место, в котором совершено общественно опасное действие (бездействие) независимо от места наступления последствий. Поэтому сформулированный Пленумом подход находит объяснение в том числе благодаря тому, что в последние годы «суды стали исходить из того, что по смыслу уголовно-процессуального закона (ст. 32 УПК РФ) место совершения преступления неразрывно связано со временем его совершения (ч. 2 ст. 9 УК РФ)»[23].

[Использование электронных сетей]

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.

[23] Степанов П. П., Грибанова Д. В. Указ. соч.

В частности, по признаку, предусмотренному пунктом «б» части 2 статьи 228.1 УК РФ, при незаконном сбыте наркотических средств квалифицируются действия лица, которое с использованием сети «Интернет» подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств.

По указанному признаку 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).

Положения, предусмотренные в п. 20 Постановления, относятся к разряду ключевых по своей значимости. Сформулированные правовые позиции выходят за рамки традиционных представлений о правилах квалификации преступлений и могут неоднозначно оцениваться в теории и практике уголовного права.

Пленум указал, что 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. Это означает, что присутствующий в ряде составов преступлений квалифицирующий признак «с использованием информационно-телекоммуникационных сетей, в том числе сети „Интернет”» может инкриминироваться по уголовному делу как в тех случаях, когда виновный выполнял (или имел намерение выполнить) объективную сторону преступления, используя такие сети (что соответствует буквальному пониманию уголовного закона), так и в случаях, когда использование сетей имело место только на стадии приготовления к преступлению, а стадия покушения на преступление и оконченное преступление не сопровождались указанным способом посягательства.

Содержание этой правовой позиции продемонстрировано Пленумом на примере преступления, предусмотренного п. «б» ч. 2 ст. 228.1 УК РФ. По данной уголовно-правовой норме могут

квалифицироваться «действия лица, которое с использованием сети „Интернет" подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств. По указанному признаку 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)». Некоторые из перечисленных противоправных действий, а именно подыскание источника незаконного приобретения наркотиков или соучастников преступления, связь между соучастниками в ходе подготовки преступления, не входят в объективную сторону сбыта, образуют стадию приготовления к преступлению и при недоведении лицом преступления до конца по не зависящим от него обстоятельствам квалифицируются как приготовление к сбыту наркотических средств, психотропных веществ или их аналогов. Но поскольку при совершении указанных действий субъект преступления использовал информационно-телекоммуникационные сети, включая сеть «Интернет», содеянное следует квалифицировать по ч. 1 ст. 30, п. «б» ч. 2 ст. 228.1 УК РФ, в том числе если установлено, что сбывать наркотики лицо намеревалось без использования указанных сетей (например, при личной встрече с приобретателем).

Таким образом, перестала быть актуальной существующая в теории уголовного права и судебной практике позиция, согласно которой если место встречи для передачи наркотических средств, психотропных веществ или их аналогов было оговорено посредством проводного, сотового телефона или радиостанции, электронной почты, а их передача осуществлялась 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[24]. В соответствии с новым разъяснением Пленума содеянное нужно квалифицировать по п. «б» ч. 2 ст. 228.1 УК РФ, если виновный *использовал средства массовой информации либо электронные или информационно-телекоммуникационные сети (включая сеть «Интернет») на любой стадии умышленного преступления либо, готовясь к преступлению, имел намерение их использовать при совершении преступления.* В частности, такая квалификация возможна как минимум в следующих случаях:

при «дистанционном сбыте», когда передача наркотика в пользу другого лица совершена при отсутствии непосредственного контакта между сбытчиком и приобретателем путем сообщения с использованием информационно-телекоммуникационной сети информации о месте хранения (тайника-закладки) наркотика либо размещения в сети «Интернет» информации о возможности приобретения наркотиков или передача такой информации посредством электронного сообщения[25];

если приобретение, хранение, перевозка, изготовление, переработка наркотиков с целью последующего сбыта[26] совершены

---

[24] Определение Верховного Суда Российской Федерации от 15 декабря 2015 г. № 48-АПУ15-45 ; Определение Верховного Суда Российской Федерации от 17 января 2018 г. № 48-АПУ17-30 ; Определение Шестого кассационного суда общей юрисдикции от 7 июля 2021 г. № 77-2888/2021 ; Постановление Президиума Челябинского областного суда от 1 июля 2015 г. № 44у-63/2015 (Доступ из справ.-правовой системы «КонсультантПлюс») ; Винокуров В. Н., Агафонов А. В. Особенности квалификации сбыта наркотических средств с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Уголовное право. 2023. № 1. С. 3—12 ; Хромов Е. В. Указ. соч. С. 34—35.

[25] Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021) // Бюллетень Верховного Суда Российской Федерации. 2021. № 12 ; Определение Верховного Суда Российской Федерации от 9 марта 2021 г. № 41-УД20-55 // Бюллетень Верховного Суда Российской Федерации. 2022. № 5 ; Определение Верховного Суда Российской Федерации от 13 мая 2021 г. № 25-УД21-6-К4 // Бюллетень Верховного Суда Российской Федерации. 2022. № 7 ; Обзор судебной практики Верховного Суда Российской Федерации № 1 (2022) // Бюллетень Верховного Суда Российской Федерации. 2022. № 8.

[26] Эти действия входят в объективную сторону сбыта наркотиков (п. 13.2 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 (ред. от 16 мая 2017 г.) «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами»).

с использованием информационно-телекоммуникационной сети интернет-покупка, передача/получение соучастником электронного сообщения о месте хранения наркотика и др.)[27];

если приобретение, хранение, перевозка, изготовление, переработка наркотиков, а равно приготовительные к сбыту действия совершены без использования информационно-телекоммуникационной сети, но в целях последующего «дистанционного сбыта»[28];

если приготовительные к сбыту действия совершены с использованием информационно-телекоммуникационной сети (подыскание источника приобретения, соучастников, связь между соучастниками в ходе подготовки и пр.).

Если исходить из буквального толкования уголовного закона и следовать выводу о том, что квалифицирующие признаки состава преступления являются средством дифференциации уголовной ответственности лиц, совершивших действия (бездействие), предусмотренные диспозициями статей Особенной части УК РФ (исполнителей преступления)[29], и не могут выполнять такую функцию в отношении лиц, виновных только в приготовлении к преступлению без квалифицирующих признаков или являющихся организаторами, подстрекателями или пособниками преступления исполнителя без квалифицирующих признаков (такие лица непосредственно не совершают действия (бездействие), входящие в объективную сторону преступлений, предусмотренных статьями Особенной части УК РФ), то позиция Пленума о возможности вменения обсуждаемого квалифицирующего признака по уголовному делу о приготовлении к преступлению, когда не установлено, что лицо намеревалось использовать информационно-телекоммуникационные сети

[27] Определение Шестого кассационного суда общей юрисдикции от 20 мая 2021 г. № 77-2237/2021 ; Определение Шестого кассационного суда общей юрисдикции от 7 июля 2021 г. № 77-2888/2021 ; Определение Восьмого кассационного суда общей юрисдикции от 4 июля 2022 г. № 77- 2731/2022 (Доступ из справ.-правовой системы «КонсультантПлюс»).

[28] Определение Верховного Суда Российской Федерации от 17 октября 2013 г. № 50-АПУ13-26. Доступ из справ.-правовой системы «КонсультантПлюс».

[29] Лесниевски-Костарева Т. А. Дифференциация уголовной ответственности. Теория и законодательная практика. М., 2000. С. 175 ; Кругликов Л. Л., Васильевский А. В. Дифференциация ответственности в уголовном праве. СПб., 2002. С. 171—174.

при совершении действий, входящих в объективную сторону преступления, может быть охарактеризована в лучшем случае как расширительное толкование уголовного закона, в худшем случае — как применение уголовного закона по аналогии.

Разумно поставить и другие вопросы, связанные с оценкой обсуждаемой правовой позиции высшей судебной инстанции.

Во-первых, новый подход к квалификации преступлений, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», влечет ухудшение положения лиц, которые использовали информационно-телекоммуникационные сети только на стадии приготовления к преступлению. Потому что согласно прежней позиции судебной практики, «исходя из положений закона, виновное лицо может быть осуждено по квалифицирующему признаку п. «б» ч. 2 ст. 228.1 УК РФ только в тех случаях, когда это лицо с использованием электронных или информационно-телекоммуникационных сетей (включая сеть „Интернет") выполняет объективную сторону состава преступления, т. е. сбыта наркотических средств и психотропных веществ»[30]. Следовательно, правомерно вести речь о том, что лица, совершившие указанные посягательства до 15 декабря 2022 года, не должны нести уголовную ответственность за преступление с учетом квалифицирующего признака «с использованием электронных или информационно-телекоммуникационных сетей, включая сеть „Интернет"», если не установлен их умысел на выполнение объективной стороны преступления указанным способом, поскольку, как это следует из ч. 1 ст. 10 УК РФ, уголовно-правовое регулирование, ухудшающее положение лица, обратной силы не имеет[31].

Во-вторых, анализируемое разъяснение Пленума распространяется на любое преступление, состав которого предусматривает квалифицирующий (реже криминообразующий) признак

---

[30] Определение Верховного Суда Российской Федерации от 15 декабря 2015 г. № 48-АПУ15-45 ; Определение Шестого кассационного суда общей юрисдикции от 7 июля 2021 г. № 77-2888/2021 и др. (Доступ из справ.-правовой системы «КонсультантПлюс»).

[31] Яни П. С. Роль практикообразующих документов Верховного Суда Российской Федерации в решении вопросов квалификации преступлений, предусмотренных главой 25 Уголовного кодекса (на примере квалификации незаконного оборота наркотических средств) // Криминалистъ. 2021. № 2 (35). С. 73—79.

«с использованием электронных или информационно-телекоммуникационных сетей, включая сеть „Интернет”». В настоящее время таковой содержится более чем в двух десятках статей Особенной части УК РФ. Поэтому нельзя исключить интерпретацию указанного разъяснения, из которой следует, что уголовная ответственность за приготовление к совершению такого преступления будет наступать с учетом вменения соответствующего квалифицирующего признака в том числе в случаях, когда само по себе преступление, к которому субъект готовился с использованием информационно-телекоммуникационных сетей, не относится к категории тяжких или особо тяжких. Например, приготовительные действия по поиску источника для незаконного приобретения огнестрельного оружия, если приобретение предполагалось путем личной встречи покупателя с продавцом, не влекут уголовную ответственность за приготовление к преступлению, предусмотренному ч. 1 ст. 222 УК РФ, поскольку такое преступление не является тяжким или особо тяжким. Однако если в процессе поиска лицо использовало информационно-телекоммуникационную сеть, в том числе сеть «Интернет», имея намерение приобрести оружие при личной встрече с продавцом, содеянное при условии несостоявшейся по не зависящим от лица обстоятельствам сделки может потребовать квалификации как приготовления к тяжкому преступлению, предусмотренному п. «в» ч. 3 ст. 222 УК РФ.

[Осуществление доступа к электронным сетям]

21. Доступ к электронным или 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 действий лиц как совершенных с использованием данных сетей необходимо установить, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

В комментируемом пункте Постановления Пленум, подтверждая имманентное свойство информационно-телекоммуникационной сети — связь между двумя или более компьютерными

устройствами, обращает внимание судов на индифферентность для квалификации преступлений того обстоятельства, с помощью каких компьютерных устройств виновный осуществлял доступ к электронным или информационно-телекоммуникационным сетям, в том числе сети «Интернет». Достаточно того, что компьютерное устройство технологически предназначено для доступа к информационно-телекоммуникационной сети и позволяет использовать компьютерные программы, имеющие разнообразные функции. Среди компьютерных программ, наиболее часто применяемых лицами при совершении преступлений с использованием информационно-телекоммуникационных сетей, браузеры (например, браузер Tor, используемый для доступа к DarkNet), программы, предназначенные для обмена сообщениями, — мессенджеры (например, WhatsApp, Viber, Telegram и др.), специальные приложения социальных сетей (например, VK Мессенджер, Rakuten Viber Messenger и др.). В числе компьютерных программ, которые могут обеспечивать доступ к сети «Интернет» в противоправных целях, — онлайн-игры, а также другие программы и приложения, например программы и соответствующие им мобильные приложения конференцсвязи (Discord, Skype и др.).

Условием квалификации преступления, совершенного с использованием информационно-телекоммуникационной сети, является установление того, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

[Совершение преступлений, предусмотренных ст. 242 и 242.1 УК РФ УК РФ, с использованием электронных сетей]

22. Судам следует иметь в виду особенности квалификации отдельных действий, предусмотренных статьями 242 и 242.1 УК РФ, в случаях, когда они совершаются с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

В частности, под распространением порнографических материалов в данных статьях понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Оно может совершаться путем направления в личном сообщении конкретному лицу (по электронной почте либо с использованием социальных сетей, мессенджеров или иных приложений), рассылки определенно-

му или неопределенному кругу лиц (например, в чат в мессенджере), размещения на личных страницах и на страницах групп пользователей, в том числе в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания.

Публичная демонстрация с использованием электронных сетей или информационно-телекоммуникационных сетей, включая сеть «Интернет», заключается в открытом показе порнографических материалов либо в предоставлении неограниченному числу лиц возможности просмотра таких материалов, однако без возможности самостоятельного их использования (путем сохранения на своем компьютерном устройстве, размещения на интернет-страницах от своего имени и т. п.). Как публичная демонстрация подлежат квалификации действия, совершенные в прямом эфире (в частности, на сайтах, позволяющих пользователям производить потоковое вещание, — стриминговых сервисах), а также состоящие в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах).

Рекламирование порнографических материалов представляет собой распространение любым способом, в любой форме и с использованием любых средств информации, адресованной неопределенному кругу лиц и направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. Для квалификации действий лица как рекламирования таких материалов или предметов с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», они могут выражаться в любой форме (например, рассылка сообщений в социальных сетях, мессенджерах или по электронной почте, размещение на личной странице социальных сетей), но должны быть направлены на достижение перечисленных целей.

При квалификации действий лица, связанных с распространением, публичной демонстрацией или рекламированием порнографических материалов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», не имеет значения факт нахождения таких материалов в свободном доступе на момент совершения указанных деяний.

Статьями 242 и 242.1 УК РФ предусматривается уголовная ответственность за незаконные изготовление и оборот порнографических материалов или предметов, а также за изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних. К числу квалифицирующих обстоятельств, предусмотренных данными статьями, относится совершение преступления с использованием информаци-

онно-телекоммуникационных сетей, в том числе сети «Интернет» (п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1 УК РФ).

В настоящем пункте Постановления Пленум обратил внимание на особенности квалификации отдельных действий (распространение, публичная демонстрация, рекламирование порнографических материалов или предметов), входящих в объективную сторону соответствующих преступлений, когда они совершены с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». Из содержания разъяснений следует несколько предварительных выводов.

Во-первых, наблюдается текстуальное их противоречие законодательной конструкции упомянутого квалифицирующего признака, который как в прежней редакции, так и в редакции действующей (введена в действие Федеральным законом от 6 марта 2022 г. № 38-ФЗ, вступившим в силу 17 марта 2022 г.), не содержит положения об использовании электронных сетей. Такая формальная нестыковка не может служить препятствием для квалификации преступления с учетом квалифицирующего признака в случае использования виновным электронных сетей (например, телефонной связи), поскольку, как разъяснено в п. 17 настоящего Постановления, для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются.

Во-вторых, не исключается вменение соответствующего квалифицирующего признака лицу, признанному виновным в совершении с использованием информационно-телекоммуникационной сети других альтернативных действий, предусмотренных диспозициями ст. 242 и 242.1 УК РФ (незаконные изготовление, перемещение через Государственную границу Российской Федерации порнографических материалов или предметов, вовлечение несовершеннолетнего в оборот порнографической продукции, незаконные приобретение, хранение материалов или предметов с порнографическими изображениями несовершеннолетних), особенности квалификации которых не стали предметом внимания Пленума.

В-третьих, толкование понятий распространения, публичной демонстрации и рекламирования порнографических материалов или предметов является применимым также к случаям, когда

указанные действия совершены обычном способом, без использования информационно-телекоммуникационных сетей.

При оценке распространения порнографических материалов и предметов, совершенного с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», суды ссылаются на положение п. 9 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в соответствии с которым распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. Это соответствует той оценке общественной опасности распространения порнографических материалов и предметов, согласно которой под распространением понимается передача указанных материалов или предметов для использования группе или неограниченному кругу лиц[32].

Вместе с тем согласно правовой позиции Конституционного Суда Российской Федерации нормы имеющего самостоятельный предмет регулирования Федерального закона «Об информации, информационных технологиях и о защите информации» относятся именно к информации и не предопределяют содержание и объем уголовно-правовых запретов в сфере оборота порнографических материалов[33].

Эта правовая позиция, вкупе с мнением о возможности квалификации по ст. 242, 242.1 УК РФ передачи порнографических материалов хотя бы одному лицу[34], повлияла на более широкое

---

[32] Комментарий к Уголовному кодексу Российской Федерации. В 4 т. Т. 3. Особенная часть. Раздел IX / А. В. Бриллиантов, А. В. Галахова, В. А. Давыдов [и др.] ; отв. ред. В. М. Лебедев. М., 2023. С. 189 ; Комментарий к Уголовному кодексу Российской Федерации. В 3 т. Т. 3. Особенная часть (разделы IX—XII) / П. В. Агапов, Д. А. Безбородов, Я. Ю. Васильева [и др.] ; под общ. ред. О. С. Капинус ; науч. ред. К. В. Ображиев, Н. И. Пикуров. 2-е изд., перераб. и доп. М., 2022. С. 295 ; Шарапов Р. Д. Преступления против общественной нравственности : учеб. пособие. СПб., 2022. С. 49—50.

[33] Определения Конституционного Суда Российской Федерации от 17 июля 2018 г. № 2047-О, от 19 июля 2016 г. № 1746-О (Доступ из справ.-правовой системы «КонсультантПлюс»).

[34] Комментарий к Уголовному кодексу Российской Федерации : (постатейный). В 2 т. Т. 2 / Российская акад. правосудия ; под ред. А. В. Бриллиантова. 2-е изд. М., 2015 ; Комментарий к Уголовному кодексу Российской Федера-

толкование понятия распространения порнографических материалов и предметов, принятое Пленумом. В частности, под распространением порнографических материалов в данных статьях понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Оно может совершаться в том числе путем направления в личном сообщении конкретному лицу (по электронной почте либо с использованием социальных сетей, мессенджеров или иных приложений) ссылки для загрузки (скачивания) файлов порнографического содержания.

Поскольку теперь согласно официальному толкованию уголовно наказуемым распространением порнографических материалов считается передача их не только неограниченному кругу лиц, но и хотя бы одному лицу, постольку содержание данного противоправного деяния соответствует принятому в уголовном праве понятию сбыта предметов, запрещенных к обороту.

Такая интерпретация разъяснения Пленума подтверждается не только его грамматической конструкцией, в которой направление ссылки для загрузки (скачивания) файлов порнографического содержания в личном сообщении конкретному лицу и рассылка такой информации определенному или неопределенному кругу лиц текстуально разграничены в качестве возможных способов распространения порнографических материалов, но и последующей практикой Верховного Суда Российской Федерации, указавшего в одном из решений, что «под распространением порнографических материалов понимается в *том числе* (выделено нами. — *Р. Ш.*) незаконное предоставление возможности их использования неопределенному кругу лиц»[35].

При оценке незаконного предоставления порнографических материалов конкретным лицам является справедливой рекомендация тщательно исследовать вопрос о малозначительности деяния (например, при передаче порнографических материалов между супругами или иными близкими лицами). Возможно предположить, что со временем по мере накопления оправда-

---

ции : (постатейный) / Т. К. Агузаров, А. А. Ашин, П. В. Головненков [и др.] ; под ред. А. И. Чучаева. М., 2012. С. 415.

[35] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 22 марта 2022 г. № 14-УДП22-1-К1 ; Обзор судебной практики Верховного Суда Российской Федерации № 2 (2023). П. 40 (Доступ из справ.-правовой системы «КонсультантПлюс»).

тельных решений вышестоящих судов такая рекомендация появится в тексте разъясняемого Постановления.

Публичная демонстрация представляет собой предоставление возможности просмотра порнографических материалов группе или неограниченному кругу лиц. Вопрос о наличии признака публичности демонстрации порнографических материалов должен разрешаться с учетом места, способа, обстановки и других обстоятельств. Публичный характер демонстрации может проявляться в использовании для этого информационно-телекоммуникационных сетей, в том числе мессенджеров (WhatsApp, Viber и др.), в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах), а также в массовой рассылке электронных сообщений абонентам мобильной связи, сообщений по электронной почте.

Важным представляется разъяснение о том, что действия, совершенные в прямом эфире (в частности, на сайтах, позволяющих пользователям производить потоковое вещание, — стриминговых сервисах), подлежат квалификации как публичная демонстрация порнографических материалов. Такой подход отражает высказанное в юридической литературе мнение о том, что к числу порнографических материалов нужно относить зрелищные мероприятия порнографического характера, в том числе выполнение лицом роли «веб-модели»[36]. Поэтому у судов не должно возникать сомнений в квалификации соответствующих действий, как это имело место в одном из уголовных дел.

Судом первой инстанции осужденный по п. «б» ч. 3 ст. 242 УК РФ признан виновным в том, что работал за денежное вознаграждение в качестве «веб-модели» и осуществлял общение с клиентами в онлайн режиме в «приватном чате» с обнажением

[36] Кобзева Е. В. Преступления против здоровья населения и общественной нравственности : учеб. пособие. М., 2014. С. 128 ; Зазирная М. М. Квалификация распространения порнографических видеоматериалов в режиме реального времени с использованием сети Интернет // Уголовное право. 2015. № 6. С. 16—22 ; Шарапов Р. Д. Квалификация преступлений, связанных с незаконным оборотом порнографических материалов и предметов // Законность. 2021. № 8. С. 43—48 ; Куфлева В. Н., Литовченко А. И Новеллы квалификации вебкам-контента как публично распространяемой порнографии // Теория и практика общественного развития. 2023. № 3. С. 127—131.

тела, демонстрацией своих половых органов, сценами мастурбации. Суд апелляционной инстанции, отменяя приговор на том основании, что судом не дана надлежащая оценка обстоятельствам дела, свидетельствующим об отсутствии осведомленности осужденного о фактах записи на материальный носитель проходивших в режиме реального времени «онлайн» трансляций и последующего распространения видеозаписей, вместе с тем указал, что «уголовная ответственность, предусмотренная ст. 242 УК РФ, наступает лишь за действия, связанные с изготовлением с целью распространения или распространением порнографических материалов, сама по себе демонстрация одним человеком сексуальной стороны своей жизни в режиме реального времени „онлайн" посредством сети Интернет неопределенному количеству лиц (например, организация порнографического шоу) может рассматриваться как совершение уголовно наказуемого деяния в рамках ст. 242 УК РФ только на основании заключения экспертов, располагающих специальными познаниями в области ряда социальных наук»[37].

В качестве критерия, позволяющего разграничить распространение порнографических материалов и публичную их демонстрацию, Пленум называет наличие или отсутствие у адресатов противоправных действий виновного возможности самостоятельного использования порнографических материалов. Предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования (путем сохранения на своем компьютерном устройстве, размещения на интернет-страницах от своего имени и т. п.) следует квалифицировать как распространение. Открытый показ либо иное предоставление неограниченному кругу лиц возможности просмотра таких материалов, однако без возможности самостоятельного их использования, должны квалифицироваться как публичная демонстрация.

При толковании понятия «рекламирование порнографических материалов или предметов» Пленум использовал законода-

[37] Апелляционное определение Верховного суда Удмуртской Республики от 4 декабря 2014 г. № 22-3288/14. Доступ из справ.-правовой системы «КонсультантПлюс». См. также: Определение Судебной коллегии по уголовным делам Верховного Суда РСФСР от 28 сентября 1988 г. по делу Кузьмина и Ойринга // Бюллетень Верховного Суда РСФСР. 1989. № 5.

тельное определение рекламы как информации, распространенной любым способом, в любой форме и с использованием любых средств, адресованной неопределенному кругу лиц и направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке (п. 1 ст. 3 Федерального закона от 13 марта 2006 г. № 38-ФЗ (ред. от 23 апреля 2024 г.) «О рекламе»). Форма рекламирования (рассылка сообщений в социальных сетях, мессенджерах или по электронной почте, размещение на личной странице социальных сетей и т. п.) не влияет на квалификацию противоправных действий как совершенных с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет». Главным условием, характеризующим субъективную сторону рекламирования, является то, что противоправные действия направлены на достижение перечисленных целей, т. е. привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. В отличие от распространения порнографических материалов, которое может выражаться в их предоставлении конкретному лицу, рекламирование предполагает адресацию запрещенной информации неопределенному кругу лиц.

Преступления, связанные с распространением материалов порнографического характера, совершенные с использованием сети «Интернет», часто предполагают типичную схему действий преступников: создание специального интернет-сайта, на котором размещаются материалы порнографического характера. Чаще всего такие материалы копируются с других интернет-сайтов[38]. Положение о том, что факт нахождения порнографических материалов в свободном доступе на момент совершения противоправных деяний не имеет значения для квалификации действий лица, связанных с распространением, публичной демонстрацией или рекламированием порнографических материалов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», отражает сформированную позицию большинства

[38] Курьянова М. Н. Некоторые проблемы выявления и расследования преступлений, связанных с распространением материалов порнографического характера, совершенных с использованием сети «Интернет» (на примере Центрального федерального округа России) // Общество и право. 2009. № 4 (26). С. 232—234.

судов, которые не считают обоснованным довод сторон по уголовному делу (чаще всего стороны защиты) о том, что нахождение распространяемых, демонстрируемых или рекламируемых порноматериалов в свободном доступе в сети «Интернет» к моменту совершения лицом указанных действий исключает состав преступления.

По приговору районного суда Т. осужден за приобретение, хранение в целях распространения и распространение материалов с порнографическими изображениями несовершеннолетних, совершенные в отношении лица, не достигшего четырнадцатилетнего возраста. Суд апелляционной инстанции приговор отменил, уголовное дело в отношении Т. прекратил за отсутствием в его действиях состава преступления, в том числе по тому основанию, что файлы, которые Т. сохранил на своем компьютере, уже были распространены в сети «Интернет» и находились в свободном доступе. Суд кассационной инстанции не согласился с этим доводом и со ссылкой на п. 22 постановления Пленума Верховного Суда Российской Федерации «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”» признал выводы суда апелляционной инстанции в этой части противоречащими закону. Дело направлено на новое апелляционное рассмотрение в ином составе суда[39].

[Умышленный характер преступлений, совершаемых с использованием электронных сетей]

23. Обратить внимание судов на то, что при квалификации преступлений,, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», должно быть установлено, что лицо осуществляло такие деяния умышленно, осознавало содержание и общественную опасность соответствующих действий, включая характер распространяемой, рекламируемой или демонстрируемой информации, предоставление доступа к ней широкому кругу лиц, а также должны быть установлены другие обстоятельства, имеющие значение для юридической оценки содеянного.

[39] Кассационное определение Второго кассационного суда общей юрисдикции от 12 января 2023 г. № 77-11/2023. Доступ из справ.-правовой системы «КонсультантПлюс».

Пленум обратил внимание судов на то, что преступления, совершаемые с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», предполагают умышленную форму вины. Значение комментируемого разъяснения заключается в следующем.

Во-первых, не должны квалифицироваться по соответствующим статьям УК РФ деяния, которые хотя и связаны с использованием указанных сетей, однако совершены по неосторожности. Например, случайная рассылка или иная передача запрещенной информации другим лицам вследствие технической неграмотности, ошибки или невнимательность пользователя компьютерного устройства (сохранение информации на устройствах и в программах, предоставляющих к ней доступ другим лицам, без осведомленности об этом пользователя, ошибочная пересылка информации другим лицам вместо сохранения ее на запоминающем устройстве, случайный набор команды на пересылку запрещенного контента и т. п.) либо осознанное сохранение запрещенной информации в программе или компьютерном устройстве, к которым есть доступ других лиц, с расчетом без достаточных к тому оснований, что информация не станет достоянием кого-либо благодаря затруднению доступа к ней (сохранение файлов с информацией в труднодоступных директориях или придание им статуса неотображаемых (скрытых), переименование файлов и т. п.). Следует учитывать позицию судов: «наличие у обвиняемого компьютерной программы, позволяющей скачивать и раздавать файлы другим пользователям в автоматическом режиме, само по себе не свидетельствует о его прямом умысле на совершение преступлений, предусмотренных ст. 242 и 242.1 УК РФ»[40].

Во-вторых, указание Пленума на необходимость установления умышленной формы вины для квалификации данных преступлений без уточнения вида умысла, а также концентрация внимания на содержании интеллектуального элемента умыш-

[40] Постановление Президиума Московского городского суда от 25 августа 2017 г. // Бюллетень Верховного Суда Российской Федерации. 2019. № 4. С. 14—15 ; Определение Шестого кассационного суда общей юрисдикции от 5 марта 2020 г. № 77-214/2020 ; Определение Восьмого кассационного суда общей юрисдикции от 17 июня 2020 г. № 77-1042/2020 ; Определение Четвертого кассационного суда общей юрисдикции от 13 декабря 2021 г. № 77-4153/2021 (Доступ из справ.-правовой системы «КонсультантПлюс»).

ленной вины (осознавало содержание и общественную опасность соответствующих действий, включая характер распространяемой, рекламируемой или демонстрируемой информации, предоставление доступа к ней широкому кругу лиц) без упоминания волевого элемента может служить основанием для вывода о возможности совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», не только с прямым умыслом, но и с косвенным.

Такой вывод уже наблюдается в судебной практике, в частности по делам о незаконном распространении порнографических материалов.

Пока как среди правоприменителей, так и среди представителей уголовно-правовой доктрины превалирует точка зрения о том, что с субъективной стороны незаконные изготовление и оборот порнографических материалов или предметов, в том числе их распространение (ст. 242, 242.1 УК РФ), характеризуются прямым умыслом[41].

Разделяя это мнение, Верховный Суд Российской Федерации обозначил позицию, согласно которой 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, направ-

[41] Обзор судебной практики Кемеровского областного суда от 23 июня 2005 г. № 01-19/320 по делам о преступлениях, предусмотренных ст. 159, 160, 165, 242, 327 УК РФ. Доступ из справ.-правовой системы «ГАРАНТ» ; Апелляционное определение Пензенского областного суда от 14 декабря 2016 г. № 22-1278. Доступ из справ.-правовой системы «КонсультантПлюс» ; Комментарий к Уголовному кодексу Российской Федерации. В 4 т. Т. 3. С. 190—191 ; Настольная книга судьи по уголовным делам / Г. А. Есаков, А. И. Рарог, А. И. Чучаев ; отв. ред. А. И. Рарог. М., 2007 ; Кобзева Е. В. Преступления против здоровья населения и общественной нравственности : учеб. пособие. М., 2014. С. 128, 130 ; Шалагин А. Е. Преступления, связанные с организацией проституции и распространением порнографии (уголовно-правовое и криминологическое исследование) : монография. М., 2017. С. 120, 124 ; Филиппов П. А. Преступления против здоровья населения и общественной нравственности : монография. М., 2022. С. 635 ; Защита здоровья населения и общественной нравственности в уголовном праве: законодательный и правоприменительный аспекты / В. Н. Бурлаков, Л. В. Готчина, Л. Н. Плоткина, В. В. Семенова ; под ред. В. Н. Бурлакова : учеб. пособие. СПб., 2023. С. 138, 142.

ленные на передачу указанных материалов неограниченному кругу лиц, не расцениваются как распространение порнографических материалов, в том числе тогда, когда пользователи осознают факт общедоступности размещенных порноматериалов[42].

Например, Верховный Суд Российской Федерации, прекращая уголовное дело за отсутствием состава преступления в отношении П., осужденного по пп. «а», «г» ч. 2 ст. 242.1 УК РФ за хранение в целях распространения материалов с порнографическими изображениями несовершеннолетних, в том числе не достигших четырнадцатилетнего возраста, и за их распространение с использованием сети «Интернет», указал следующее. Предусмотренное ст. 242.1 УК РФ распространение материалов может быть совершено только с прямым умыслом, когда виновный осознает, что он распространяет материалы с порнографическими изображениями несовершеннолетних и желает этого. Сославшись в приговоре на осведомленность П. о том, что скопированные им файлы порнографического содержания при помощи компьютерной программы могут быть скопированы и иными пользователями сети «Интернет», имеющими доступ к программе «S», суд не дал оценки тому обстоятельству, что, копируя и сохраняя файлы на своем персональном компьютере, сам П. никому их не предлагал и не передавал.

Доказательства, свидетельствующие о том, что видеофайлы с порнографическими изображениями несовершеннолетних, указанные в обвинительном заключении и в приговоре, были распространены П., т. е. получены другими лицами в результате его целенаправленных действий, в материалах дела не содержатся и в приговоре не приведены. Данные файлы были скопированы из сети «Интернет» выборочно сотрудниками правоохранительных органов по их запросу без участия в этом П. с помощью программы, установленной на их компьютере.

Из показаний сотрудника полиции С. усматривается, что сбор сведений о лицах, имеющих на своих компьютерах порнографические материалы с изображениями несовершеннолетних, производился сотрудниками полиции с помощью стандартных про-

[42] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10 июля 2019 г. № 16-УД19-7 // Бюллетень Верховного Суда Российской Федерации. 2020. № 6 ; Определение Первого кассационного суда общей юрисдикции от 24 марта 2020 г. № 77-291/2020. Доступ из справ.-правовой системы «КонсультантПлюс».

грамм. Осуществив поиск, ими был установлен список пользователей, у которых на персональных компьютерах в свободном доступе имеются файлы обозначенной категории. Из нескольких IP-адресов и файлов, предлагаемых компьютерной программой, они выбрали IP-адрес П., получили доступ в хранилище его файлов, в котором находилось 154 файла в свободном доступе, из них выбрали два файла, которые, по их мнению, могли содержать порнографические материалы с изображениями несовершеннолетних, и загрузили данные файлы.

То обстоятельство, что П. было известно о сохранении скопированных на компьютер файлов в программе, позволяющей другим пользователям их копировать, не может свидетельствовать о его умысле на их распространение, поскольку на момент копирования им данных файлов они уже были распространены в сети «Интернет» и находились в свободном доступе.

Обнаружив материалы порнографического содержания в памяти компьютера, принадлежавшего П., органы предварительного следствия ограничились лишь двумя файлами, скопированными в ходе проведения указанного выше оперативно-разыскного мероприятия. Имелись ли на компьютере, а также на внешних носителях, принадлежавших П. и изъятых у него, и другие материалы аналогичного содержания и в каком количестве, не установлено.

Доводы П. о том, что он специально не занимался копированием файлов с порнографическими изображениями несовершеннолетних с целью их последующего распространения, не опровергнуты[43].

В связи с таким подходом в доктрине выдвинут тезис, который еще больше сужает рамки субъективной стороны преступных действий, связанных с распространением порнографических материалов: «Поскольку факт общедоступности порнографии, являющийся неизбежным в таких случаях последствием действий пользователя информационно-телекоммуникационной сети, в совокупности с вытекающим из ч. 2 ст. 25 УК РФ выводом о наличии у него прямого умысла не считается достаточным основанием уголовной ответственности за распространение порнографических материалов, постольку следует признать, что

[43] Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10 июля 2019 г. № 16-УД19-7 // Бюллетень Верховного Суда Российской Федерации. 2020. № 6.

с субъективной стороны распространение порнографических материалов или предметов характеризуется специальной целью — получение таких материалов или предметов группой или неограниченным кругом лиц»[44].

Изложенной позиции следует в своих решениях Конституционный Суд Российской Федерации, который отметил, что ст. 242 УК РФ «указывает на наличие прямого умысла, направленного на незаконное распространение порнографических материалов или предметов, как обязательного условия привлечения правонарушителя к ответственности»[45], в связи с чем данная норма отвечает требованию определенности, «не придан ей иной смысл и в постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 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”»[46].

Вместе с тем по одному из вышеупомянутых уголовных дел о преступлении, предусмотренном пп. «а», «г» ч. 2 ст. 242.1 УК РФ, Второй кассационный суд общей юрисдикции, отменяя решение суда апелляционной инстанции об отсутствии в действиях подсудимого состава преступления, допустил, что указанное преступление может быть совершено как с прямым, так и с косвенным умыслом.

Подробности дела состоят в том, что по приговору районного суда Т. осужден за приобретение, хранение в целях распространения и распространение материалов с порнографическими изображениями несовершеннолетних, совершенные в отношении лица, не достигшего четырнадцатилетнего возраста. Судом установлено, что подсудимый в имеющийся в личном пользовании компьютер с целью распространения материалов с порнографическим изображением несовершеннолетних, не достигших четырнадцатилетнего возраста, используя информаци-

[44] Шарапов Р. Д. Квалификация преступлений… С. 47.

[45] Определение Конституционного Суда Российской Федерации от 29 января 2009 г. № 41-О-О. Доступ из справ.-правовой системы «КонсультантПлюс».

[46] Определение Конституционного Суда Российской Федерации от 27 июня 2023 г. № 1757-О. Доступ из справ.-правовой системы «КонсультантПлюс».

онную сеть «Интернет», загрузил на жесткий магнитный диск через программу «eMule» 1 944 электронных файла, содержащих порнографические изображения несовершеннолетних, не достигших четырнадцатилетнего возраста, хранил их с целью последующего распространения, достоверно зная о том, что они являются доступными для других пользователей сети «Интернет», тем самым распространял указанные материалы.

Суд апелляционной инстанции, оправдывая подсудимого, исходил из того, что преступление, предусмотренное ст. 242.1 УК РФ, может быть совершено только с прямым умыслом, сослался на то, что, скачивая и храня файлы на своем компьютере, сам Т. никому их не передавал и не предлагал.

Однако суд кассационной инстанции принял во внимание то обстоятельство, что подсудимый владеет компьютером на уровне уверенного пользователя и осведомлен о том, что программа «eMule» скачивала и раздавала файлы, наименование которых отображается в программе. Отвергая довод суда апелляционной инстанции о том, что преступление, предусмотренное ст. 242.1 УК РФ, может быть совершено только с прямым умыслом, суд кассационной инстанции, ссылаясь на разъяснение, содержащееся в п. 23 комментируемого Постановления Пленума, заключил: «Таким образом, Пленум Верховного Суда РФ в своих разъяснениях указал, что преступные действия должны быть совершены умышленно, не утверждая, что умысел должен быть исключительно прямым, тем самым допуская и безразличное отношение виновного лица к наступившим последствиям, то есть совершение преступления с косвенным умыслом»[47].

Дословное воспроизведение этой позиции встречается в решениях других кассационных судов общей юрисдикции по аналогичным делам[48].

Думается, что для такой широкой трактовки обсуждаемого разъяснения Пленума, с помощью которого в судебной практике предпринимаются попытки расширить субъективную сторону

[47] Кассационное определение Второго кассационного суда общей юрисдикции от 12 января 2023 г. Доступ из справ.-правовой системы «КонсультантПлюс».

[48] Определение Первого кассационного суда общей юрисдикции от 16 марта 2023 г. № 77-1206/2023 ; Определение Девятого кассационного суда общей юрисдикции от 13 июня 2023 г. № 77-908/2023 (Доступ из справ.-правовой системы «КонсультантПлюс»).

распространения порнографических материалов за счет косвенного умысла, все же нет оснований.

В решении обсуждаемого вопроса предлагается исходить из следующих положений.

Во-первых, как известно, виды умысла отличаются друг от друга как по волевому элементу (при прямом умысле лицо желает наступления общественно опасных последствий, при косвенном умысле — не желает их наступления, но сознательно допускает эти последствия либо относится к ним безразлично), так и по интеллектуальному элементу (при прямом умысле лицо предвидит возможность или неизбежность наступления общественно опасных последствий, при косвенном умысле — только возможность наступления общественно опасных последствий).

Во-вторых, объективная сторона распространения порнографических материалов, по версии Пленума (п. 22 Постановления), исчерпывается незаконным предоставлением конкретным лицам либо неопределенному кругу лиц возможности их использования, в том числе путем размещения на личных страницах и на страницах групп пользователей, в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания. Преступление следует считать юридически оконченным с момента предоставления виновным другим лицам доступа к порнографическим материалам[49].

Так, М. признан виновным в том, что, являясь пользователем локальной файлообменной сети интернет-провайдера, умышленно хранил в целях распространения и распространял путем обеспечения общего доступа неограниченному количеству пользователей материалы с порнографическими изображениями несовершеннолетних, а также лиц, не достигших четырнадцатилетнего возраста. В ответ на доводы кассационной жалобы защитника о том, что осужденный не совершал активных действий по распространению порнографических материалов, а лишь создал возможность для их приобретения, люди сами принимали решение о скачивании данных материалов и самостоятельно совершали действия по их приобретению, суд кассационной ин-

[49] Доступ к информации — возможность получения информации и ее использования (п. 6 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

станции указал, что действия М. по п. «б» ч. 2 ст. 242.1 УК РФ (в ред. Федерального закона от 27 июля 2009 г. № 215-ФЗ) квалифицированы судом первой инстанции верно. Состав преступления, предусмотренного ст. 242.1 УК РФ, является формальным. Распространение порнографических материалов с изображениями несовершеннолетних и лиц, не достигших четырнадцатилетнего возраста, выразилось в обеспечении осужденным открытого общего доступа неограниченному количеству пользователей к своему компьютеру, где хранились файлы с указанной информацией[50].

В определении Верховного Суда Российской Федерации от 22 марта 2022 г. № 14-УДП22-1-К1 подчеркнуто, что «согласно диспозиции статьи 242.1 УК РФ инкриминируемое осужденному преступление не предполагает в качестве обязательного признака фактический просмотр кем-либо из посетителей страницы с размещенным на ней порнографическим сайтом; достаточно того, что, размещая в социальной сети „ВКонтакте" такой сайт, осужденный исходил из того, что он может быть просмотрен неопределенным кругом лиц»[51].

Наличие или отсутствие факта того, что другие пользователи информационно-телекоммуникационной сети воспользовались предоставленным доступом (перешли по гиперссылке, сохранив ее, скопировали информацию на запоминающее устройство своего оборудования или просто ознакомились с размещенной информацией), не имеет значения для уголовно-правовой оценки содеянного, так как это последствие лежит за границей юридически оконченного состава преступления. Если представить, что по не зависящим от виновного обстоятельствам размещенный им в сети порнографический контент никем не использован (не просмотрен, не скачан), содеянное является юридически оконченным преступлением, а не покушением на него. Напротив, если по не зависящим от виновного обстоятельствам ему не удалось предоставить другому лицу доступ к порнографической информации, скажем, при безуспешной попытке отправить содержимое по электронной почте на несуществующий адрес,

[50] Кассационное определение Тульского областного суда от 26 октября 2011 г. № 22-2581. Доступ из справ.-правовой системы «КонсультантПлюс».

[51] Обзор судебной практики Верховного Суда Российской Федерации № 2 (2023) : утв. Президиумом Верховного Суда Российской Федерации 19 июля 2023 г. П. 40. Доступ из справ.-правовой системы «КонсультантПлюс».

имеются основания для квалификации таких действий как покушение на преступление.

Поскольку форма вины определяется психическим отношением лица к общественно опасному последствию, являющемуся признаком состава преступления, следует вывод, что в вопросе о виде умысла в составах распространения порнографических материалов следует исходить из психического отношения виновного к первичному последствию своих действий (наличие у других лиц возможности использования запрещенной информации, т. е. доступа к ней), а не к вторичному последствию (фактическое использование запрещенной информации, т. е. когда другие лица воспользовались предоставленным доступом).

Это вторичное последствие может характеризовать цель противоправных действий виновного, если по уголовному делу будет установлено, что предоставление другим лицам возможности использования порнографических материалов сопровождалось (выражалось) такими целенаправленными действиями, как, например, прямое предложение воспользоваться размещенным на интернет-странице контентом, пересылка другому лицу в личном сообщении или рассылка в чате мессенджера ограниченному или неограниченному кругу пользователей, сохранение файлов в файлообменной сети под названиями, однозначно свидетельствующими о том, что на них содержатся порнографические изображения, и т. п.

Однако действия с компьютерной информацией порнографического содержания, приводящие к ее общедоступности в информационно-телекоммуникационной сети, могут быть не связаны со стремлением субъекта к тому, чтобы другие лица воспользовались предоставленным доступом (например, когда информация с целью личного ее использования сохраняется на компьютерном устройстве, к которому могут удаленно подключиться другие пользователи, на интернет-странице или на другом общедоступном ресурсе). В случае оценки таких действий как преступления безразличное отношение (сознательное допущение) субъекта к такому побочному для него последствию не делает преступление совершенным с косвенным умыслом, потому что психическое отношение к этому находящемуся за рамками состава преступления последствию не составляет интеллектуального и волевого элемента умысла.

По уголовным делам данной категории Пленум ориентировал суды на то, что в числе обстоятельств, указывающих на умышленную форму вины, должно быть установлено осознание виновным факта предоставления доступа к запрещенной информации широкому кругу лиц, о чем могут свидетельствовать такие обстоятельства, как обладание знаниями в области информационных технологий и навыками пользователя компьютерной техники, осведомленность об автоматическом размещении добавленных на свою страницу видеофайлов в новостной ленте «друзей» и о возможности их свободного просмотра, что подтверждается отметкой об ознакомлении с правилами пользования интернет-сайтом социальной сети при регистрации в ней, несовершение действий по запрету доступа другим пользователям социальной сети к своей странице, на которой размещены порноматериалы[52], указание пользователем папок с файлами, из которых он разрешает другим пользователям скачивание информации при помощи файлообменной программы[53], и т. п. В таком случае, несмотря на то что порнографический материал размещен на общедоступном ресурсе для личного пользования и не установлено, что субъект его передавал или предлагал другим лицам, интеллектуальный элемент умысла при распространении порнографических материалов состоит в том, что виновный предвидит не то что возможность, а неизбежность общедоступности порнографических материалов для других лиц, что предопределяет согласно предписанию ч. 2 ст. 25 УК РФ вывод о совершении преступления не с косвенным, а с прямым умыслом.

В свою очередь, копирование (скачивание) порнографической информации с сохранением ее в заведомо для виновного общедоступных местах на запоминающих устройствах или в интернет-ресурсах дает основание для квалификации содеянного не только как распространение порнографических материалов, наказуемое по ст. 242, 242.1 УК РФ, но и как их приобретение

[52] Обзор судебной практики Верховного Суда Российской Федерации № 2 (2023) : утв. Президиумом Верховного Суда Российской Федерации 19 июля 2023 г. П. 40 ; Кассационное определение Верховного Суда Российской Федерации от 8 декабря 2022 г. № 1-УДП22-10-К (Доступ из справ.-правовой системы «КонсультантПлюс»).

[53] Кассационное определение Верховного Суда Российской Федерации от 19 мая 2022 г. № 47-УДп22-3-К6. Доступ из справ.-правовой системы «КонсультантПлюс».

и хранение в целях распространения или публичной демонстрации, наказуемые по ст. 242.1 УК РФ.

Примечательно, что в числе фактических обстоятельств, которые должны составлять содержание интеллектуального элемента умысла лица, виновного в распространении, рекламировании или демонстрации запрещенной информации, назван факт предоставления доступа к такой информации широкому кругу лиц. Это соответствует характеру таких противоправных действий, как рекламирование и публичная демонстрация, которые нацелены на передачу запрещенной информации, в частности порнографических материалов, неограниченному (неопределенному) кругу лиц. Однако это положение диссонирует с ранее изложенной в п. 22 настоящего Постановления позицией Пленума о том, что распространение порнографических материалов предполагает незаконное предоставление соответствующей информации не только неопределенному кругу лиц, но и конкретному лицу. В таком несоответствии можно усмотреть не только формально-юридическую несогласованность разъяснений, но также действительную оценку представителями судейского сообщества степени общественной опасности распространения запрещенной информации в информационно-телекоммуникационных сетях, когда такое распространение адресовано неограниченному числу лиц. Это, в свою очередь, позволяет вновь подчеркнуть важность рекомендации тщательно исследовать вопрос о малозначительности деяния (ч. 2 ст. 14 УК РФ) в случае, когда умысел лица направлен на предоставление порноматериалов конкретному лицу.

К числу других обстоятельств, имеющих значение для юридической оценки содеянного, которые согласно разъяснению Пленума должны быть установлены при квалификации преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», относятся все иные обстоятельства, позволяющие установить наличие или отсутствие признаков состава соответствующего преступления, дать оценку индивидуальной степени общественной опасности содеянного фигурантом дела (время, место, особенности способа, обстановка, мотивы и цели, характер и размер причиненного вреда и другие обстоятельства совершения преступления, а также обстоятельства, исключающие преступность и наказуемость деяния (ст. 73 УПК РФ)).

[Привлечение специалистов по делам о преступлениях, предусмотренных ст. 272—274.1 УК РФ]

24. При возникновении в ходе рассмотрения уголовных дел о преступлениях, предусмотренных статьями 272, 273, 274 и 274.1 УК РФ, об иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», сомнений в том, относится ли, например, та или иная информация к компьютерной либо является ли технологическая система, использованная лицом при совершении преступления, электронной или информационно-телекоммуникационной сетью, а также для разъяснения технических терминов и других сложных вопросов, требующих специальных знаний, рекомендовать судьям привлекать к участию в судебном разбирательстве соответствующих специалистов.

Предусмотренные главой 28 УК РФ преступления в сфере компьютерной информации, а также другие преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», характеризуются такими признаками состава преступления, доказывание и квалификация которых может потребовать использования субъектами уголовно-процессуальной деятельности специальных знаний в области науки и техники. Наряду с производством судебной экспертизы для получения таких знаний могут привлекаться к участию в уголовном деле специалисты (ст. 58 УПК РФ). В частности, суды привлекают к участию в судебном разбирательстве соответствующего специалиста с целью разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию.

Исходя из комментируемого разъяснения, предметом допроса специалиста, привлеченного для участия в судебном разбирательстве по уголовному делу о киберпреступлении, могут быть вопросы о том, относится ли, например, та или иная информация к компьютерной, является ли технологическая система, использованная лицом при совершении преступления, электронной или информационно-телекоммуникационной сетью. Специалист может привлекаться также для разъяснения технических терминов и других сложных вопросов, требующих специальных знаний, круг которых определяется особенностями предмета преступления (компьютерная информация, вредоносная компьютерная программа), способа преступления (например, доступ к компьютерной информации, использование информационно-теле-

коммуникационной сети), последствий преступления (уничтожение, блокирование, модификация, копирование компьютерной информации) и других признаков состава преступления.

Важным является понимание того, что привлечение специалиста к участию в судебном разбирательстве по уголовным делам о киберпреступлениях, если об этом не ходатайствует сторона защиты (ч. 2.1 ст. 58 УПК РФ), не является обязательным во всех без исключения случаях. Как разъяснил Пленум, это требуется тогда, когда в ходе рассмотрения уголовного дела возникают сомнения в том, соответствуют ли фактические обстоятельства преступления тем признакам его состава, содержание которых составляют технические понятия (компьютерная информация, информационно-телекоммуникационная сеть и т. п.).

Если преступление совершено с использованием телефонной связи или общераспространенного компьютерного устройства (персонального компьютера, лэптопа, планшета, смартфона), подключенного к сети «Интернет», техническое назначение которых не вызывает сомнений, а материалы уголовного дела, связанные с использованием специальных знаний (заключения компьютерной экспертизы, заключения и протоколы допроса специалиста, результаты осмотра компьютерных устройств, документов, содержащих информацию о соединениях между абонентами и (или) абонентскими устройствами и пр.), не содержат неопределенности в их оценке, в привлечении специалиста к участию в судебном разбирательстве нет необходимости.

НОРМАТИВНЫЕ АКТЫ

1. Кодекс Российской Федерации об административных правонарушениях : Федеральный закон от 30 декабря 2001 г. № 195-ФЗ : текст с изм. и доп. на 22 июня 2024 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации : Федеральный закон от 13 июня 1996 г. № 63-ФЗ : текст с изм. и доп. на 12 июня 2024 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

3. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. № 187-ФЗ : текст с изм. и доп. на 10 июля 2023 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

4. О государственной охране : Федеральный закон от 27 мая 1996 г. № 57-ФЗ : текст с изм. и доп. на 4 авг. 2023 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

5. 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».

6. О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации : Федеральный закон от 8 июня 2020 г. № 168-ФЗ : текст с изм. и доп. на 28 дек. 2022 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

7. О национальной платежной системе : Федеральный закон от 27 июня 2011 г. № 161-ФЗ : текст с изм. и доп. на 19 дек. 2023 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

8. 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».

9. О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» : Федеральный закон от 24 апреля 2020 г. № 123-ФЗ. — Доступ из справ.-правовой системы «КонсультантПлюс».

10. О противодействии экстремистской деятельности : Федеральный закон от 25 июля 2002 г. № 114-ФЗ : текст с изм. и доп. на 15 мая 2024 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

11. О рынке ценных бумаг : Федеральный закон от 22 апреля 1996 г. № 39-ФЗ : текст с изм. и доп. на 11 марта 2024 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

12. О средствах массовой информации : Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 : текст с изм. и доп. на 11 марта 2024 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

13. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ : текст с изм. и доп. на 12 дек. 2023 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

14. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ : текст с изм. и доп. на 29 дек. 2022 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

15. Об организации предоставления государственных и муниципальных услуг : Федеральный закон от 27 июля 2010 г. № 210-ФЗ : текст с изм. и доп. на 25 дек. 2023 г. — Доступ из справ.-правовой системы «КонсультантПлюс».

16. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федеральный закон от 29 декабря 2022 г. № 572-ФЗ. — Доступ из справ.-правовой системы «КонсультантПлюс».

17. 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».

Научное издание

Александр Николаевич ПОПОВ
доктор юридических наук, профессор

Роман Дмитриевич ШАРАПОВ
доктор юридических наук, профессор

КОММЕНТАРИЙ

К ПОСТАНОВЛЕНИЮ 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"»

Редактор *Н. Я. Елкина*
Компьютерная правка и верстка *Н. В. Федорченко*, *И. А. Щербаковой*

Подписано в печать 26.08.2024. Формат 60x90/16.
Печ. л. 5,25. Тираж 500 экз. (1-й з-д 1—75). Заказ 22/24.

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

Отпечатано в Санкт-Петербургском юридическом институте (филиале)
Университета прокуратуры Российской Федерации
191014, Санкт-Петербург, Литейный просп., 44