

ЦИФРОВОЙ ЭКСТРЕМИЗМ

Кристина Александровна МАРАХОВА

Донбасский государственный университет юстиции

kristinamarahova9@gmail.com

Научный руководитель старший преподаватель кафедры уголовного права и уголовного процесса ФГБОУ ВО «Донбасский государственный университет юстиции» (ДГУЮ Минюста России), **Валерий Эдуардович ПЕРЕНЕСЕНКО**, valrada@mail.ru

Аннотация. Цифровая среда стала главным полигоном для экстремистской идеологии, обнажив уязвимость квалификационных конструкций. Актуальность исследования обусловлена императивом адаптации уголовного закона к латентным формам киберпреступности. Новизна заключается в отказе от плоского восприятия интернета: предложена авторская трехуровневая матрица оценки использования сетевых ресурсов, впервые позволяющая дифференцировать степень криминального воздействия на массовое сознание. Материалы адресованы теоретикам и практикам, предлагая работающие инструменты разграничения составов преступлений. Цель работы – выработка вектора реформирования УК РФ для устранения пробелов в квалификации цифрового терроризма.

Ключевые слова: экстремизм, терроризм, даркнет, криптовалюта, квалификация, шифрование, расследование.

DIGITAL EXTREMISM

Kristina A. MARAKHOVA

Donbass State University of Justice

kristinamarahova9@gmail.com

Scientific adviser – senior Lecturer at the Department of Criminal Law and Criminal Procedure of the FSBEI HE “Donbas State University of Justice” (DSUJ), **V. E. PERENESSENKO**, valrada@mail.ru

Abstract. The digital environment has become the primary testing ground for extremist ideology, exposing vulnerabilities in existing qualification frameworks.

The study's relevance stems from the imperative to adapt criminal law to latent forms of cybercrime. The novelty lies in rejecting a simplified view of the Internet: the authors propose an original three-level matrix for assessing network resource usage, which for the first time allows differentiating the degree of criminal impact on mass consciousness. The materials offer practitioners working tools for distinguishing crime compositions. The goal is to develop a vector for reforming the Criminal Code to eliminate qualification gaps in digital terrorism.

Keywords: extremism, terrorism, darknet, cryptocurrency, qualification, encryption, investigation.

Современное состояние преступности экстремистского и террористического характера характеризуется масштабной миграцией криминальной активности в сетевое информационное пространство. По данным Генеральной прокуратуры Российской Федерации, в последние годы наблюдается устойчивый рост числа преступлений, совершенных с использованием информационно-телекоммуникационных сетей. Если в 2020 году их доля составляла около тридцати процентов от общего числа выявленных преступлений экстремистской направленности, то к 2024 году этот показатель превысил шестьдесят процентов. Зарубежный правотворческий опыт, в частности директивы Европейского союза о борьбе с терроризмом, демонстрирует аналогичный глобальный тренд, вынуждая государства вырабатывать новые подходы к криминализации деяний, связанных с использованием даркнета, зашифрованных мессенджеров и децентрализованных платформ. В российской правоприменительной практике также формируется специфический подход, однако он сталкивается с существенными трудностями при разграничении смежных составов преступлений и оценке степени влияния сетевой среды на общественную опасность деяния.

Масштаб и характер данной угрозы приобретают беспрецедентные размеры. Как справедливо отмечает в своих трудах В.С. Овчинский, криминальная цифровая среда обладает свойством «усиления» деструктивного по-

тенциала, превращая локальные угрозы в глобальные вызовы безопасности [8, с. 45]. Преступные формирования используют цифровые технологии не просто как вспомогательное средство, а как фундаментальную основу своей деятельности, обеспечивающую анонимность, трансграничность и массовость воздействия. Применение защищенных каналов связи, криптовалют для финансирования и алгоритмов для вербовки создает существенный барьер для традиционных методов правоохранительной деятельности. Однако именно осознание глубины этой угрозы позволяет сформулировать адекватные вызовам времени правовые и криминалистические механизмы противодействия.

Для изучения вопроса необходимо уточнить понятийный аппарат. В доктрине существуют различные подходы к определению сетевого информационного пространства. Так, А. А. Васильев рассматривает его преимущественно как структурный элемент глобального информационного пространства, ограниченный рамками технической коммуникации [1, с. 12]. В то же время, другие исследователи, в частности Я. Г. Ищук и соавторы, полагают, что это социально-технологическая среда специфической формы взаимодействия, в которой возможно осуществление преступной деятельности [4, с. 58]. Сравнивая данные подходы, можно отметить, что второе определение шире охватывает социальный аспект, что представляется более точным и предпочтительным для криминалистического анализа. Сетевое информационное пространство является родовым понятием по отношению к электронным информационно-телекоммуникационным сетям и сети Интернет. Оно включает в себя не только общедоступные сети, но и закрытые сегменты, корпоративные и ведомственные сети, а также сети связи нового поколения и децентрализованные пиринговые сети. Устойчивость таких систем к внешнему воздей-

ствию требует от правоохранительных органов применения инновационных методов выявления и фиксации следов преступной деятельности.

Анализ судебно-следственной практики, методология которого опирается на фундаментальные труды таких исследователей, как Д.Г. Скориков и А.В. Матюшкина [6; 9], позволяет систематизировать преступления террористического характера, совершаемые в сети: от публичных призывов и оправдания терроризма до организации террористического сообщества, где вербовка осуществляется через манипуляцию сознанием пользователей в социальных сетях. При этом дистанционный способ обучения террористической деятельности стал доминирующим именно благодаря возможностям сетевого пространства, что требует от следствия применения специализированных криминалистических методик работы с цифровыми следами. Логичным продолжением данного анализа является рассмотрение преступлений экстремистского характера, которые тесно переплетаются с террористическими и часто служат для них идеологической базой. Переход от террористических к экстремистским составам обусловлен единой методологией их совершения в цифровой среде. Сетевая среда многократно усиливает общественную опасность экстремистских проявлений, таких как публичные призывы к экстремистской деятельности, возбуждение ненависти либо вражды и организация экстремистского сообщества. Специфика финансирования экстремистской деятельности в сети заключается в использовании краудфандинговых платформ и криптовалют, что существенно затрудняет отслеживание финансовых потоков.

Особого внимания заслуживает технический арсенал преступников, активно использующих мессенджеры со сквозным шифрованием. Перечисленные инструменты объединяет принцип конфиденциальности по умолчанию. Сравнивая их с традиционными средствами связи, можно констатировать,

что они не просто скрывают содержание переписки, но и минимизируют метаданные, что делает классические методы оперативно-розыскной деятельности (например, детализацию соединений) малоэффективными. Это подтверждается современной криминалистической практикой, где раскрытие таких преступлений все чаще опирается на анализ поведенческих паттернов и агентурные методы.

Важным шагом в унификации правоприменения стало принятие п. 20 Постановления Пленума Верховного Суда РФ № 37 от 15 декабря 2022 года, разъяснившего, что преступление признается совершенным с использованием информационно-телекоммуникационных сетей, если хотя бы одно из умышленных действий, входящих в объективную сторону, было выполнено с их помощью.¹ Краткий анализ данного положения показывает его двойственную природу. С одной стороны, оно расширяет возможности квалификации и унифицирует практику. С другой стороны, такое широкое толкование рискует привести к избыточной криминализации, поскольку под него может подпасть даже минимальное, вспомогательное использование сети (например, отправка одного сообщения), что нивелирует специфику сетевых преступлений и нарушает принципы справедливости и дифференциации ответственности.

Для разрешения указанного противоречия предлагается разграничить использование сетевого информационного пространства по характеру его применения на три уровня. Первый уровень предполагает использование сети как вспомогательного средства, когда оно носит эпизодический, информационный характер и не создает самостоятельной угрозы объекту посягатель-

¹ Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» [Электронный ресурс] // КонсультантПлюс. — URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 16.09.2026).

ства, и такое использование не должно влиять на квалификацию. Второй уровень характеризуется использованием сети как условия совершения преступления, при котором она выступает средой, облегчающей приготовление к преступлению; данные деяния должны квалифицироваться с учетом правил о приготовлении к преступлению, но без автоматического применения квалифицирующих признаков, если сеть не была непосредственным орудием. Третий уровень представляет собой использование сети как инструмента совершения преступления, когда она является необходимым и ключевым элементом объективной стороны, и именно в этом случае использование сети должно признаваться квалифицирующим или отягчающим обстоятельством.

По результатам проведенной работы сформулированы конкретные выводы. Во-первых, сетевое информационное пространство мутировало из нейтральной среды в самостоятельный криминогенный фактор, качественно изменяющий объективную сторону преступлений экстремистской и террористической направленности. Во-вторых, действующая судебная практика, экстенсивно трактующая использование сетей, приводит к размыванию границ между оконченным преступлением и приготовлением, нарушая принцип индивидуализации уголовной ответственности. В-третьих, технологическая асимметрия, обусловленная повсеместным шифрованием и использованием децентрализованных финансов, делает традиционные следственные методы заведомо неэффективными без их радикальной методологической перестройки.

В целях преодоления выявленных проблем требуется реализация комплекса конкретных мер, адресованных различным субъектам правоприменения. Теоретикам уголовного права и криминологии необходимо разработать доктринальное обоснование и предложить конкретные формулировки для внесения изменений в статьи 205.2, 280, 282 и 63 Уголовного кодекса РФ, за-

крепив в законе предложенную трехуровневую типологию использования сети. Кроме того, целесообразно инициировать научную дискуссию о введении специальной нормы, предусматривающей ответственность за создание и администрирование цифровых платформ, изначально предназначенных для пропаганды экстремизма, что позволит сместить фокус правоприменения с рядовых потребителей контента на организаторов цифровой криминальной инфраструктуры.

Практикам же – следователям, дознавателям и оперативным работникам – в условиях сквозного шифрования рекомендуется сместить акцент с попыток перехвата контента на криминалистический анализ конечных точек устройств, поведенческую биометрию, открытую разведку источников (OSINT) и перекрестную идентификацию аккаунтов. Поскольку технические средства перехвата часто оказываются бессильны, необходимо активнее использовать агентурные методы внедрения в закрытые сетевые сообщества. Параллельно с этим следует инициировать создание межведомственных аналитических центров, оснащенных системами на базе искусственного интеллекта для автоматического трекинга криптовалютных транзакций и выявления паттернов краудфандинга экстремистских организаций.

Наконец, на организационном уровне первостепенное значение приобретает инициирование разработки нормативных актов, обязывающих разработчиков децентрализованных платформ внедрять механизмы законного доступа для правоохранительных органов по судебному решению, либо предусматривающих ответственность IT-компаний за отказ от содействия в раскрытии преступлений террористического характера. Реализация данного комплекса научно обоснованных мер позволит обеспечить адекватную дифференциацию уголовной ответственности и сформировать эффективный государственный ответ на вызовы цифровой эпохи.

Список источников

1. Васильев А. А., Ибрагимов Ж. И., Васильева О. В. Даркнет как ускользающая сфера правового регулирования // Юрислингвистика. 2019. № 12. С. 11–13.
2. Дремова Ю.Г. Национальные инновационные системы: учебное пособие для вузов. М.: Издательство Юрайт, 2023. 180 с. URL: <https://urait.ru/bcode/520392>
4. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая криминология: учебное пособие. Москва: Академия управления МВД России, 2021. 244 с.
5. Лапин Е.С. Теория оперативно-розыскной деятельности: учебник и практикум для вузов. 7-е изд., перераб. и доп. М.: Юрайт, 2023. 439 с.
6. Матюшкина А.В., Федичкина И.М. Способы совершения преступлений экстремистской направленности // XII Державинские чтения в Республике Мордовия: материалы Всерос. науч.-практ. конф., Саранск, 22 апреля 2016 г. Саранск, 2016. С. 378–383
7. Мухин С. М. Преступления в сети Darknet: краткая характеристика, проблемы противодействия // Альманах молодого исследователя. 2018. № 5. С. 110–114.
8. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. Москва: Норма: ИНФРА-М, 2018. 352 с.
9. Скориков Д.Г., Васильев Д.В., Горкина Е.В. Криминалистическая характеристика преступлений экстремистской направленности // Современные проблемы науки и образования. 2014. № 6. С. 1728

10. Соловьев В. С., Осипенко А. Л. Рынок нелегальных товаров и услуг в Darknet и Telegram-каналах // Уголовная политика и культура противодействия преступности. 2018. № 1. С. 138–141.

14. Денисов Ю. Д. Противодействие экстремизму в сети Интернет // Законность. 2009. № 6. С. 3–5.

15. Аристархова Т.А. Соккрытие следов и иные формы противодействия расследованию экстремистских преступлений против прав и законных интересов человека и гражданина // Известия Тульского государственного университета. Экономические и юридические науки. 2015. № 1-2. С. 24–30

Информация об авторах

К. А. МАРАХОВА – студент 4 курса.

Information about the authors

K. A. MARAKHOVA – 4th year student.