УДК 343.32(045)

В.Е. Зварыгин, А.М. Ахатова

ПРЕСТУПЛЕНИЯ ЭКСТРЕМИСТСКОГО И ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СЕТЕВОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА[1]

С учетом цифровизации всего общества возможности трансграничного оборота информации в сетевом информационном пространстве все чаще используются преступными террористическими и экстремистскими организациями в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации. Основным отличием таких преступлений является их ориентированность на цифровые технологии как основного средства коммуникации и способа достижения цели. В статье дается авторское определение понятия сетевого информационного пространства, под которым понимается совокупность глобальных (GAN – Global Area Network), региональных (MAN – Metropolitan Area Network, локальных (LAN – Local Area Network) и иных информационно-телекоммуникационных сетей, связывающих или способных связывать информационные системы посредством использования комплексов сетевых протоколов, главной целью которого является предоставление возможности реализации различных форм и видов коммуникации. Рассматривается проблема применения п. 20 ППВС РФ № 37 от 15.12.2022 года. Приводится перечень преступлений экстремистского и террористического характера, совершаемых с использованием сетевого информационного пространства. Представлен анализ судебно-следственной практики по данным составам. Сделан вывод о необходимости постепенного внесения в уголовный кодекс дополнений в части добавления квалифицирующего признака «с использованием компьютерной информации либо с использованием электронных, информационно-телекоммуникационных сетей, включая сеть Интернет, в отдельные составы преступлений экстремистской и террористической направленности, где он будет учтен как отягчающий признак, либо дополнить ст. 63 УК РФ аналогичным признаком.

Ключевые слова: экстремизм, терроризм, сетевое информационное пространство, компьютерная информация, информационно-телекоммуникационная сеть, сеть Интернет, уголовное право, квалификация преступлений, трансграничность, общественная опасность.

DOI: 10.35634/2412-9593-2023-33-5-864-871

Согласно п. 7 Доктрины Информационной безопасности Российской Федерации (далее – РФ) информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства[2].

С учетом интеграции технических средств во все сферы жизни общества, компьютерная информация стала не только предметом посягательства, но и способом, а также средством совершения большинства преступлений экстремистского и террористического характера, где в качестве объектов уголовно-правовой охраны выступают основы конституционного строя и безопасность государства, общественная безопасность.

При совершении посягательств на вышеуказанные объекты уголовно-правовой охраны преступными организациями используются механизмы внешнего деструктивного информационного, информационно-психологического воздействия на индивидуальное, групповое и общественное сознание. Это осуществляется путем распространения негативных социальных и моральных установок, противоречащих традициям, убеждениям и верованиям народов РФ[3]. При этом преследуются цели дестабилизации политической и социальной ситуации в стране.

[1] Исследование проведено при финансовой поддержке ФГБОУ ВО «Удмуртский государственный университет» («Научный потенциал») в соответствии с приказом ректора от 14.04.2023 № 476/01-01-04 «О проведении в 2023 году конкурса междисциплинарных научно-исследовательских работ (грантов) молодых ученых, преподавателей и сотрудников УдГУ».

[2] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ // СПС «КонсультантПлюс».

[3] п. 87 Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СПС «КонсультантПлюс».

Эти деяния, как правило, обладают повышенной степенью общественной опасности в силу оперативности и массовости распространения информации на неограниченный круг лиц в сетевом информационном пространстве [3]. Этому способствует использование защищенных каналов связи, обеспечивающих анонимность (например, VPN) [13], позволяющее скрывать фактическое место нахождения преступных лиц. К таким же способам относится неправомерный доступ к компьютерной информации, позволяющий уничтожать, блокировать, модифицировать, копировать необходимую информацию в целях осуществления преступной деятельности. Кроме того, использование сетевого информационного пространства позволяет поддерживать контакты внутри преступных организаций, когда ее участники находятся на значительном удалении друг от друга [11], распределять роли между членами преступных формирований, вовлекать в нее участников, в частности, несовершеннолетних, планировать совершение новых преступлений.

Основным отличием таких преступлений является их ориентированность на цифровые технологии как основного средства коммуникации и способа достижения цели [2]. Это позволяет расширять возможности для совершения преступления террористической и экстремисткой направленности.

Тем не менее, на практике судами при вынесении приговоров нередко усматривается использование элементов сетевого информационного пространства даже в тех составах, где он не предусмотрен в качестве основного, квалифицирующего или особо квалифицирующего признака.

В данной работе мы предлагаем к рассмотрению составы преступлений террористической и экстремисткой деятельности, совершаемые в сетевом информационном пространстве.

I. Преступления террористического характера.

1) *Террористический акт (ст. 205 УК РФ),* который может быть выражен, в частности, в совершении действий, устрашающих население. Угроза совершения преступлений находит место в печатной, визуальной, аудиовизуальной и иных формах [14]. Примером может являться распространение недостоверной информации в социальных сетях о планировании террористических актов в России Службой безопасности Украины в 2022 году [5].

2) *Содействие террористической деятельности (ст. 205[1] УК РФ).* Нередко в сетевом информационном пространстве такое содействие выражается в даче советов, указаний, финансировании терроризма, предоставлении информации или орудий совершения преступления. Так, Определением Судебной коллегии по делам военнослужащих ВС РФ от 24.12.2020 по делу № 223-УД20-6-А6 лицо было осуждено за содействие террористической деятельности в форме финансирования терроризма, совершенное в сети «Интернет» путем публикации в интернет-приложении «Zello» графического изображения, а также голосовых сообщений, содержащих признаки оправдания терроризма[4]).

3) *Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205[2] УК РФ).* Механизмы внешнего деструктивного информационного, информационно-психологического воздействия могут быть различны: письменный, путем отправки сообщений, в виде аудио или видеозаписей, прямых эфиров и т. д. Примером может служить Кассационное определение Судебной коллегии по делам военнослужащих ВС РФ от 28.06.2023 № 222-УД23-37-А6, в котором лицо было признано виновным в размещении им в социальной сети публикаций, содержащих признаки пропаганды идеологии деятельности международной террористической организации «Исламское государство»[5]).

4) *Прохождение обучения в целях осуществления террористической деятельности (ст. 205[3] УК РФ).* При изучении судебной и следственной практики все чаще встречаются решения, в которых лица проходили соответствующее обучение с использованием дистанционного способа. В качестве примера отметим возбужденное уголовное дело в отношении несовершеннолетнего за прохождение обучения террористической деятельности с использованием мобильного устройства в период с октября 2022 г. по июнь 2023 г. [10]

5) *Организация террористического сообщества и участие в нем (ст. 205[4] УК РФ). Организация деятельности террористической организации и участие в деятельности такой организации (ст. 205[5]*

[4] Определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 24.12.2020 по делу № 223-УД20-6-А6 // СПС «КонсультантПлюс».

[5] Кассационное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 28.06.2023 № 222-УД23-37-А6 // СПС «КонсультантПлюс».

УК РФ). Зачастую, подписываясь или добавляясь в аккаунт пользователей, вербовщики вводят лиц в заблуждение, навязывая при этом радикальные идеологические и политические взгляды, акцентируя внимание на несправедливость в обществе [9]. Так, одной из первых террористических организации, использующих сетевое информационное пространство, является «Аль-Каида».

6) *Организация незаконного вооруженного формирования или участие в нем (ст. 208 УК РФ).* Так, Определением Первого кассационного суда общей юрисдикции от 01.11.2022 № 77-5177/2022 лицо было признано виновным за оказание финансовых услуг путем онлайн-перевода посредством платежной системы «Золотая Корона» для финансирования и материального обеспечения вооруженного формирования Сирии. При этом лицо поддерживало связь с участниками преступного формирования посредством социальной сети «Одноклассники» и мессенджера «WhatsApp»[6].

II. Преступления экстремистского характера.

1) *Публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ).* Следует отметить внесение изменений в данную статью, в абз. 1 ч. 1 словами «публичное оправдание экстремизма или пропаганда экстремизма»[7]. Целью введения изменений является обеспечение средствами уголовно-правовой охраны физического развития и нравственного воспитания несовершеннолетних. Тем не менее рассматриваемое деяние наиболее часто совершается с использованием мессенджеров, социальных сетей. Однако необходимый квалифицирующий признак отсутствует как в действующей редакции, так и в законопроекте № 403956-8. Подтверждая вышесказанное, обратимся к Обзору судебной практики ВС РФ № 1 (2023). Так, Б. был осужден за публичные призывы к осуществлению террористической деятельности с использованием сети «Интернет»[8]. Тем не менее действия лица были квалифицированы по части первой данной статьи в связи с отсутствием необходимого (особо) квалифицирующего признака.

2) *Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности РФ (ст. 280[1] УК РФ).* Действия лица в сетевом информационном пространстве могут быть также направлены на формирование намерений у других лиц совершить преступления. Так, Г.А.А. осуществлял призывы к совершению данного преступления в одной из социальных сетей, на личной странице, доступной для общего пользования[9].

3) *Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ).* В абз. 2 п. 2.1 ППВС от 28.06.2011 № 11 (ред. от 28.10.2021) к данным, указывающим на признаки преступления, относится не только сам факт размещения в сети Интернет или иной сети текста, изображения, аудио- или видеофайла, но и иные сведения, указывающие на общественную опасность деяния[10]. Тем не менее, даже после вышедших разъяснений возникают трудности при квалификации преступлений, когда лицо систематически использует графические изображения («лайки», «дизлайки», «эмоджи»), репосты и комментарии для выражения собственного мнения о той или иной ситуации.

4) *Организация экстремистского сообщества (ст. 282[1] УК РФ). Организация деятельности экстремистской организации (ст. 282[2] УК РФ).* Рассматриваемые выше способы организации террористического сообщества также характеры для данного вида преступлений. Примером может являться уголовное дело, возбужденное в отношении несовершеннолетних, создавших экстремистское сообщество «Vesna Crew». Участники данного сообщества размещали в сети Интернет аудио, видеоконтент, направленный на привлечение как можно больше единомышленников.

5) *Финансирование экстремистской деятельности (ст. 282[3] УК РФ).* Привлечение средств физических лиц в различных географических регионах мира осуществляется как открытым путем, так и

---

[6] Определение Первого кассационного суда общей юрисдикции от 01.11.2022 № 77-5177/2022 // СПС «КонсультантПлюс».

[7] Законопроект № 403956-8 «О внесении изменений в статью 280 Уголовного кодекса Российской Федерации». URL: https://sozd.duma.gov.ru/bill/403956-8

[8] Обзор судебной практики Верховного Суда Российской Федерации № 1 (2023) (утв. Президиумом Верховного Суда РФ 26.04.2023) // СПС «КонсультантПлюс».

[9] Апелляционное определение Судебной коллегии по делам военнослужащих Верховного Суда Российской Федерации от 12.12.2019 № 222-АПУ19-2 // СПС «КонсультантПлюс».

[10] Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности» // СПС «КонсультантПлюс».

посредством обмана пользователей. Отдельные социальные сети (например, ВКонтакте) позволяют переводить денежные суммы на другой аккаунт получателя[11].

6) *Неоднократные пропаганда, публичное демонстрирование нацистской или экстремистской атрибутики или символики (ст. 282[3]УК РФ).*

При этом последствия общественно-опасных деяний, совершенных с использованием сетевого информационного пространства, не ограничиваются исключительно данным пространством и могут причинять вред иным общественным отношениям (например, жизни и здоровью, собственности, компьютерной информации).

Для определения сферы данного исследования необходимо раскрыть понятие и элементы сетевого информационного пространства. Несмотря на частое упоминание в законодательстве исследуемого термина, он не получил правого закрепления.

Тем не менее, понятие информационного пространства дается в разделе 3 Приказа Минстроя России от 07.02.2022 № 76/пр (ред. от 06.10.2022) «Об утверждении ведомственной программы цифровой трансформации Министерства строительства и жилищно-коммунального хозяйства Российской Федерации на очередной финансовый 2022 год и плановый период 2023 и 2024 годов» и понимается как пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур, на основе норм регулирования, механизмов организации, управления и использования[12].

Рассматривая доктринальные толкования исследуемого термина, Ю.Г. Дремова под сетевым информационным пространством понимает структурный элемент глобального информационного пространства, ограниченный рамками коммуникации [6]. Л.А. Бураева выделяет его в качестве вида кибертерроризма, основанного исключительно на организационно-коммуникационных целях [16]. Е.С. Лапин полагает, что данное сетевое информационное пространство является социально-технологической средой специфической формы взаимодействия, в которой возможно осуществление и преступной деятельности [8].

Несмотря на многообразие используемой терминологии (сетевое информационно-электронное пространство [18], пространство сетевых платформ [19], информационно-электронное пространство [16], сетевое пространство [4], социально-сетевое пространство [7]), они используются в качестве синонимов понятий ИТС, сеть Интернет.

Полагаем, что понятие сетевого информационного пространства является родовым понятием электронных ИТС и сети Интернет. Она не ограничивается только одной сетью и может включать в себя:

– «закрытые» сети Darknet (даркнет), «Шелковый путь» (Silk Road), «Гидра» («Hydra»);

– корпоративные сети (Enterprise Network), относящиеся к типам Интранет (Intranet) или Экстранет (Extranet);

– сети оборонных или военных ведомств [1];

– автоматизированные информационные системы правоохранительных органов, обеспечивающие их сетевое взаимодействие (ИСОД, ЕИТКС);

– сети специального назначения (ГАС «Правосудие», ГАС «Выборы»);

– сети связи (5G);

– сети, основанные на технологии 2IP, функционирующие посредством полной децентрализации пиринговых сетей, то есть каждый из пользователей является и сервером, и клиентом. Такая система устойчива к влиянию со стороны правоохранительных органов, поскольку получить доступ в одноранговую сеть с ограниченным доступом практически невозможно [15].

Полагаем, что под **сетевым информационным пространством** необходимо понимать совокупность глобальных (GAN – Global Area Network), региональных (MAN – Metropolitan Area Network, локальных (LAN – Local Area Network) и иных информационно-телекоммуникационных сетей, связывающих или способных связывать информационные системы посредством использования комплексов

[11] Информационное письмо Банка России от 18.01.2023 № ИН-08-12/6 «О национальной оценке рисков ОД и ФТ» // СПС «КонсультантПлюс».

[12] Приказ Минстроя России от 07.02.2022 № 76/пр (ред. от 06.10.2022) «Об утверждении ведомственной программы цифровой трансформации Министерства строительства и жилищно-коммунального хозяйства Российской Федерации на очередной финансовый 2022 год и плановый период 2023 и 2024 годов» // СПС «КонсультантПлюс».

сетевых протоколов, главной целью которого является предоставление возможности реализации различных форм и видов коммуникации.

Элементы сетевого информационного пространства включают в себя:

– социальные сети (ВКонтакте, Одноклассники, Мой Мир@mail.ru, Twitter);

– мессенджеры (Telegram, Whatsapp, Viber, Skype);

– блоги, которые могут быть личными, коллективными и корпоративными;

– аудио- и видеоподкасты;

– специализированные социальные интернет-хранилища или медиахранилища (например, видеохостинг YouTube);

– интернет-форумы (веб-конференции), чаты и видеочаты;

– технологии потокового мультимедиа (радио и телевидения);

– электронную или голосовую почты;

– вебинары;

– IP-телефонию;

– файлобменные сети и «облачные» технологии, хранящие противоправную информацию с целью ее последующего распространения (Google Drive, Яндекс Диск, Norton Zone, OneDrive)

– SMS-сервисы и др.

Наиболее часто преступными террористическими и экстремисткими формированиями используются:

– месседжер «Signal», позволяющий лицам обмениваться информацией с абонентами путем отправки текстового или звукового сообщения;

– месседжеры «Wickr», «Threema», обеспечивающие мгновенное удаление информации как на самом мобильном устройстве, так и на серверах сети;

– мобильные приложения «SureSpot», «Kik»;

– технологии потокового мультимедиа Al-Hayat Media Center, The Al-Furqan Institute for Media Production, The Al-I'tisam Media Foundation, занимающиеся распространением текстовой, аудио- и видеопродукции;

– технологии связи CryptoPhone и BlackPhone, направленные на обеспечение конфиденциальности обмена информацией, предоставляют возможность вести переговоры и без доступа к сети за счет использования bluetooth [12].

В целях предотвращения преступлений, совершаемых террористическими и экстремистскими преступными формированиями в сетевом информационном пространстве, возникла необходимость в применении средств уголовно-правового противодействия.

С принятием ППВС №37 от 15 декабря 2022 года законодатель в п. 20 обращает внимание на то, что преступление квалифицируется как совершенное с использованием электронных или ИТС, 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.

Следовательно, любое общественно-опасное деяние, которое было совершено с использованием ИТС, может быть отнесено к данной группе и квалифицировано с их использованием, что, в свою очередь, влечет нарушение принципов законности, обоснованности и справедливости.

Законодатель, пытаясь обособить группу преступлений, совершаемых с использованием ИТС, не учел, что большинство преступлений может быть совершено с использованием элементов сетевого информационного пространства. В целях разрешения данного противоречия предлагается дифференцировать использование сетевого информационного пространства по характеру его применения:

1) Сетевое информационное пространство как вспомогательное средство совершения преступления. Такое использование не создает даже отдалённой угрозы на объект посягательства и не образует этапа осуществления единого преступления. Как правило, оно носит информационный характер (например, использование мобильного телефона для уточнения места встречи для совершения террористического акта, создание аккаунта в социальных сетях для последующей вербовки лиц в террористические и экстремистке организации, покупка компьютера с целью осуществления последующих преступлений).

2) Сетевое информационное пространство как условие совершения преступления. Использование элементов сетевого информационного пространства предполагает, что они могут выступать

в качестве орудия или средства совершения преступления либо относиться к иному умышленному созданию условий для совершения преступления при выполнении приготовительных действий. Такие деяния должны быть квалифицированы по ч. 1 ст. 30 УК РФ. В данном случае технологические системы создают возможность для последующего совершения посягательства. Например, изучение места предполагаемого совершения преступления путем использования мессенджеров или социальных сетей для установления контакта с лицами, знающими данную местность, составление плана с использованием GPS связи.

Рассматриваемые выше деяния находятся за пределами приготавливаемого преступления. Соответственно, они не являются факультативными признаками объективной стороны состава преступления и не должны учитываться при его уголовно-правовой оценке.

3) Сетевое информационное пространство как инструмент совершения преступления. Оно предполагает использование элементов сетевого информационного пространства для начала или продолжения выполнения объективной стороны совершения преступлений.

Данные общественно-опасные деяния можно разделить по цели использования:

1. *Преступления экстремистского и террористического характера с использованием сетевого информационного пространства, направленные на* обеспе*чение деятельности преступных экстремистских и террористических формирований.* Например, финансирование экстремистской или террористической деятельности; иное содействие в совершении преступлений.

2. *Преступления экстремистского и террористического характера с использованием сетевого информационного пространства, направленные на информационно-психологическое воздействие.* Например, размещение в социальных сетях, мессенджерах, YouTube-каналах, Интернет и иных ресурсах материалов, возбуждающих ненависть либо вражду, создание платформ по прохождению обучения в целях осуществления террористической деятельности.

3. *Преступления экстремистского и террористического характера с использованием сетевого информационного пространства, направленные на нарушение целостности компьютерной информации:*

– неправомерный доступ к личному кабинету пользователя на портале государственных услуг для последующего использования его персональных данных в целях осуществления террористической или экстремисткой деятельности;

– рассылка в сетевых платформах компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации;

– осуществление неправомерного доступа к ИТС в целях распространения недостоверной информации о совершаемых преступлениях;

– воздействие на операторов ИТС в целях совершения ими перечисленных выше действий [17].

В силу повышенной общественной опасности приготовительных действий к тяжкому или особо тяжкому преступлениям, использование сетевого информационного пространства как инструмента совершения преступления должно признаваться одним из вариантов проявления объективной стороны конкретного оконченного или неоконченного преступления и быть учтено при его уголовно-правовой квалификации. Например, если лицо осуществило неправомерный доступ к компьютерной информации и затем распространило с чужого аккаунта информацию, призывающую к совершению экстремисткой или террористической деятельности, содеянное должно быть квалифицировано в совокупность со статьями главы 28 УК РФ.

Приведенный нами анализ дает основание подвести следующие итоги:

1) Под сетевым информационным пространством необходимо понимать совокупность глобальных (GAN – Global Area Network), региональных (MAN – Metropolitan Area Network, локальных (LAN – Local Area Network) и иных информационно-телекоммуникационных сетей, связывающих или способных связывать информационные системы посредством использования комплексов сетевых протоколов, главной целью которого является предоставление возможности реализации различных форм и видов коммуникации.

2) При совершении преступления с использованием сетевого информационного пространства характер использования сетевого информационного пространства выступает в качестве методологической основы дифференциации и индивидуализации уголовной ответственности и наказания. Предлагаем разграничивать использование элементов сетевого информационного пространства на: а) вспомогательное средство совершения преступления, б) условие совершения преступления, в) инструмент (орудие или средство) совершения преступления.

3) С учетом повышенной общественной опасности рассматриваемых преступлений, совершаемых в сетевом информационном пространстве, полагаем возможным: а) внести квалифицирующий признак «с использованием компьютерной информации либо с использованием электронных, информационно-телекоммуникационных сетей, включая сеть Интернет, в отдельные статьи УК РФ, предусматривающие уголовную ответственность за совершение преступлений террористического характера (ст. ст. 205, 205^1, 205^3, 205^4, 205^5 УК РФ) и экстремистского характера (ст. ст. 282^1, 282^2, 282^3, 282^4 УК РФ), где он будет учтен как отягчающий признак, либо б) дополнить ст. 63 УК РФ «Обстоятельства, отягчающие наказание» признаком «совершение преступления с использованием компьютерной информации или информационно-телекоммуникационных сетей, включая сеть Интернет.

СПИСОК ЛИТЕРАТУРЫ

1. Are there any global network other than the Internet? Network Engineering Stack Exchange. URL: https://networkengineering.stackexchange.com/questions/25362/are-there-any-global-network-other-than-the-internet
2. Pre-print of the chapter Jason R.C.: «The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations» by Jason R.C. Nurse and Maria Bada, due to appear in The Oxford Handbook of Cyberpsychology (2018/19). Ed. by Alison Attrill-Smith, Chris Fullwood, Melanie Keep, and Daria J. Kuss. 2019. 7 Jan. URL: http://rxiv.org> pdf/1901.01914.pdf
3. Алексеев Г.В., Антонов Я.В., Атнашев В.Р. и др. Экстремизм в современном мире: моногр. / Федеральное государственное бюджетное образовательное учреждение высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Северо-Западный институт управления / под общ. ред. А.И. Бастрыкина. СПб.: ИПЦ СЗИУ РАНХиГС, 2018. С. 93.
4. Булгаков А.Э. Политические лидеры в социальных сетях: прозрачность ответственности // Конституционное и муниципальное право. 2023. № 5. С. 32–40.
5. Варвара Кошечкина. По соцсетям разошелся фейк про подготовку волны терактов в России. lenta.ru: 21.10.2022. URL: https://lenta.ru/news/2022/10/21/fake_terakt/
6. Дрёмова Ю.Г. Национальные инновационные системы: учебное пособие для вузов. М.: Издательство Юрайт, 2023. 180 с. URL: https://urait.ru/bcode/520392
7. Зотов В.В., Кривоухов А.А., Васильева И.Н. Социально-сетевое взаимодействие в сети Интернет: к определению феномена медиа // Коммуникология. 2022. Т. 10, № 4. С. 13–22.
8. Лапин Е.С. Теория оперативно-розыскной деятельности: учебник и практикум для вузов. 7-е изд., перераб. и доп. М.: Юрайт, 2023. 439 с. URL: https://urait.ru/bcode/514974.
9. Лунеев В.В. Курс мировой и российской криминологии. Особенная часть: учебник для вузов. М.: Юрайт, 2023. 872 с. URL: https://urait.ru/bcode/531634.
10. Любовь Ширижик. Российский подросток попал под следствие ФСБ за обучение навыкам терактов. lenta.ru: 14.06.2023. URL: https://lenta.ru/news/2023/06/14/teeennn/
11. Нечевин Д.К., Баранов В.В. Противодействие экстремизму в глобальной компьютерной сети Интернет: история и современность // Административное право и процесс. 2022. № 2. С. 26–33.
12. Пащенко И.В. Идеология террористических сообществ в сети Интернет: технологии распространения и специфика противодействия // Caucasian Science Bridge. 2018.1(2). С.12–24.
13. Поляков В.В. Групповая форма совершения преступлений как один из признаков высокотехнологичной преступности // Российский юридический журнал. 2023. № 1. С. 117–126.
14. Серебренникова А.В., Лебедев М.В. Уголовно-правовая характеристика террористического акта // Актуальные проблемы российского права. 2020. № 2 (111). URL: https://cyberleninka.ru/article/n/ugolovno-pravovaya-harakteristika-terroristicheskogo-akta
15. Смушкин А.Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 3. С. 102–111.
16. Степанов О.А. Международные правовые аспекты противодействия высокотехнологичному терроризму // Современное право. № 2. 2003.
17. Степанов О.А. Противодействие кибертерроризму в цифровую эпоху: монография. М.: Издательство Юрайт, 2023. 103 с. URL: https://urait.ru/bcode/519031
18. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. М.: ИЗиСП, КОНТРАКТ, 2019. 212 с.
19. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы / М.В. Самсонова, Е.Г. Стрельцова, А.В. Чайкина и др.; отв. ред. Е.Г. Стрельцова. М.: Инфотропик Медиа, 2022. 336 с.

Поступила в редакцию 18.08.2023

Зварыгин Валерий Евгеньевич, кандидат юридических наук, доцент,
заведующий кафедрой уголовного права и криминологии
E-mail: valzvar2022@mail.ru

Ахатова Алия Махмутовна, ассистент кафедры уголовного права и криминологии
E-mail: ahatova.aliya3@mail.ru

ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 4)

V.E. Zvarygin, A.M. Akhatova
CRIMES OF EXTREMIST AND TERRORIST NATURE WITH THE USE OF NETWORK INFORMATION SPACE

DOI: 10.35634/2412-9593-2023-33-5-864-871

The possibilities of cross-border dissemination of information in the network information space are increasingly being used by criminal terrorist and extremist organizations. The purpose of such activities is to undermine sovereignty, political and social stability, forcibly change the constitutional system, and violate the territorial integrity of the Russian Federation. The main difference of such crimes is their focus on digital technologies as a means of communication. The article gives the author's definition of the concept of a network information space, which is understood as a set of global (GAN – Global Area Network), regional (MAN – Metropolitan Area Network), local (LAN - Local Area Network) and other information and telecommunication networks connecting or capable of connecting information systems through the use of network protocol complexes, the main purpose of which is to provide an opportunity to implement various forms and types of communication. The problem of applying court clarifications is considered. The authors offer their own list of extremist and terrorist crimes committed using the network information space. The conclusion is made about the need for a gradual contribution to the criminal code, supplemented by the addition of a qualifying sign «committing a crime using computer information or electronic or ITS, including the Internet» or supplement Art. 63 of the Criminal Code of the Russian Federation as appropriate.

Keywords: extremism, terrorism, network information space, digital information, telecommunication network, Internet, criminal law, qualification of crimes, cross-border nature of a crime, social danger.

Received 18.08.2023

Zvarygin V. E., Candidate of Law, Associate Professor, Head of the Department of Criminal Law and Criminology
E-mail: valzvar2022@mail.ru

Akhatova A.M., assistant of the Department of Criminal Law and Criminology
E-mail: ahatova.aliya3@mail.ru

Udmurt State University
Universitetskaya st., 1/4, Izhevsk, Russia, 426034