АКТУАЛЬНЫЕ ПРОБЛЕМЫ ГОСУДАРСТВА И ПРАВА
2023. Т. 7. № 4
http://journals.tsutmb.ru/current-issues-of-the-state-and-law/

AKTUAL'NYE PROBLEMY GOSUDARSTVA I PRAVA =
= CURRENT ISSUES OF THE STATE AND LAW
2023, vol. 7, no. 4
http://journals.tsutmb.ru/current-issues-of-the-state-and-law-eng/
ISSN 2587-9340 (Print) ISSN 2782-3334 (Online)

НАУЧНАЯ СТАТЬЯ
УДК 343.9:004
https://doi.org/10.20310/2587-9340-2023-7-4-601-609
Шифр научной специальности 5.1.4

Экстремизм и терроризм в сети Интернет как преступления в сфере компьютерной информации мирового масштаба

© ПОПОВА Елена Альбертовна
кандидат юридических наук, доцент, заведующая кафедрой уголовного права и процесса Института права и национальной безопасности, ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина», Российская Федерация, 392000, г. Тамбов, ул. Интернациональная, 33, https://orcid.org/0000-0002-6903-1775, elenap2672@yandex.ru
© КУЗНЕЦОВА Ирина Сергеевна
секретарь судебного заседания, Тамбовский областной суд, Российская Федерация, 392000, г. Тамбов, ул. Коммунальная, 8, https://orcid.org/0009-0006-4301-1967, irinakis_is15@mail.ru

Аннотация
В современных условиях информатизации население сталкивается с проблемами, имеющими разный характер, а также различные формы проявлений. Рассмотрена проблема, у которой всеобщий характер, которая в мировом масштабе представляет собой распространение идеологии терроризма и экстремизма. На данный момент мировое сообщество прилагает огромные силы, чтобы разработать новейшие способы и средства борьбы с рассматриваемыми особо тяжкими преступлениями, такими как экстремизм и терроризм, их последствия являются жестокими и иногда даже непоправимыми. При изучении вопросов, связанных с экстремизмом и терроризмом в Интернете, применялись известные теоретические методы: дедукция и индукция, анализ и синтез. Использование формально-юридического метода частного права позволило исследовать и провести оценку текстов нормативных правовых актов. Целью исследования является анализ общей характеристики экстремизма и терроризма в сети Интернет как противоправного деяния, совершенного в сфере компьютерной информации, мирового масштаба, а также выявление и разрешение наиболее актуальных и спорных вопросов как в теоретическом, так и в практическом плане применительно к рассматриваемой проблеме. Сегодня террористы и экстремисты все чаще используют сферу телекоммуникаций и компьютерной информации для реализации своих преступных намерений. Отметим, что преступления экстремистской и террористической направленности, совершаемые именно с использованием сферы компьютерной информации, несут глобальные угрозы, являются очень опасными, серьезными не только для российского общества и государства, но и в целом для мирового сообщества. Ущерб, который наносится данными видами преступлений, растет с геометрической прогрессией.

Ключевые слова
информация, информационное общество, компьютерная информация, сфера телекоммуникаций, сеть Интернет, терроризм, экстремизм, преступления в сфере компьютерной информации, противодействие

Для цитирования
Попова Е.А., Кузнецова И.С. Экстремизм и терроризм в сети Интернет как преступления в сфере компьютерной информации мирового масштаба // Актуальные проблемы государства и права. 2023. Т. 7. № 4. С. 601-609. https://doi.org/10.20310/2587-9340-2023-7-4-601-609

ORIGINAL ARTICLE
https://doi.org/10.20310/2587-9340-2023-7-4-601-609

Extremism and terrorism on the Internet as crimes in the field of computer information on a global scale

© Elena A. POPOVA,
PhD (Law), Associate Professor, Head of Criminal Law and Procedure Department, Law and National Security Institute, Derzhavin Tambov State University, 33 Internatsionalnaya St., Tambov, 392000, Russian Federation, https://orcid.org/0000-0002-6903-1775, elenap2672@yandex.ru
© Irina S. KUZNETSOVA
Court Secretary, Tambov Regional Court, 8 Kommunalnaya St., Tambov, 392000, Russian Federation, https://orcid.org/0009-0006-4301-1967, irinakis_is15@mail.ru

Abstract
In modern conditions of informatization, the population is faced with problems of a different nature, as well as various forms of manifestation. The problem is considered, which has a universal character, which on a global scale represents the spread of the ideology of terrorism and extremism. At the moment, the world community is making enormous efforts to develop the latest methods and means of combating these particularly serious crimes, such as extremism and terrorism, their consequences are cruel and sometimes even irreparable. When studying issues related to extremism and terrorism on the Internet, well-known theoretical methods were used: deduction and induction, analysis and synthesis. The use of the formal legal method of private law made it possible to study and evaluate the texts of regulatory legal acts. The purpose of study is to analyze the general characteristics of extremism and terrorism on the Internet as an illegal act committed in the field of computer information on a global scale, as well as to identify and resolve the most pressing and controversial issues, both theoretically and practically, in relation to the problem under consideration. Today, terrorists and extremists are increasingly using the sphere of telecommunications and computer information to realize their criminal intentions. Let us note that extremist and terrorist crimes committed specifically using the sphere of computer information pose global threats, are very dangerous and serious not only for Russian society and the state, but also for the world community in general. The damage caused by these types of crimes is growing exponentially.

Keywords
information, information society, computer information, telecommunications sector, Internet, terrorism, extremism, crimes in the field of computer information, counteraction

For citation
Popova, E.A., & Kuznetsova, I.S. (2023). Extremism and terrorism on the Internet as crimes in the field of computer information on a global scale. *Aktual'nye problemy gosudarstva i prava = Current Issues of the State and Law*, vol. 7, no. 4, pp. 601-609 (In Russ., abstract in Eng.) https://doi.org/10.20310/2587-9340-2023-7-4-601-609

Введение

Сегодня, в XXI веке, в период информационного общества цифровая информация имеет особую, уникальную ценность как социальную, так и экономическую, правовую. Веком энергетики был назван многими учеными XX век, в то время как XXI столетие стали называть веком информационных ресурсов. Согласно известному афоризму немецкого банкира Натана Ротшильда: «кто владеет информацией – тот владеет миром». Отметим, что эта фраза в полной мере отражает суть нашей эпохи, где доступ к информации и умение правильно ее использовать становятся основой успеха и профессионального роста.

Научно-технический прогресс привел к появлению фундаментальных технологических инноваций, которые практически незаменимы для современного человека. Массовое внедрение этих технологий привело к появлению информационных ресурсов. Сегодня информация имеет определенную реальную цену и стала особо ценным товаром в связи с развитием и совершенствованием технологий. Все это так же является стимулом появления и развития новых форм преступлений, в первую очередь, конечно, компьютерных.

Безусловно, на данный момент информация, которая хранится в электронном виде, является базой материального благосостояния достаточно многих людей, с помощью нее разрабатываются системы государственной безопасности, движутся вперед без нее открытия в современной науке.

Компьютерная информация играет значительную роль во всех общественных сферах общества, поэтому сегодня особо актуально охранять частные, общественные и государственные интересы в сфере информационных технологий.

По данным Генеральной прокуратуры Российской Федерации, за последние «пять лет количество преступлений, связанных с компьютерной информацией, увеличилось более чем в 11 раз, а удельный вес в общей структуре преступности вырос с 2 до 25 %. Большая часть преступлений в сфере компьютерной информации совершается с использованием сети Интернет (почти 58 % от всех преступлений) или при помощи средств мобильной связи (42 %). Также среди способов совершения компьютерных преступлений фигурируют расчетные (пластиковые) карты, компьютерная техника, программные средства» [1, с. 489].

Все это обусловливает актуальность данной темы и предопределяет необходимость детального рассмотрения теоретических и практических аспектов предмета заявленного исследования.

Результаты исследования

Преступления, совершаемые с использованием электронно-вычислительных машин и имеющие глобальное измерение, получили правильную и обоснованную оценку международного сообщества, что нашло свое отражение в Конвенции о киберпреступности. Конвенция является одним из основных и ключевых документов в области борьбы с компьютерными преступлениями. Конвенция была принята Советом Европы в Будапеште в 2001 г. Документ подписали не только европейские страны, но и Аргентина, Япония, а также США.

Важность и значимость вышеуказанной Конвенции неоднократно отмечались в научных работах, и здесь ее также следует подчеркнуть. Во-первых, Конвенция предусматривает такие компьютерные преступления, как:

– преступления против неразглашения и открытости компьютерных систем и данных;

– преступления, связанные с использованием компьютеров (компьютерный подлог, компьютерное мошенничество);

– «преступления, связанные с содержанием данных (детская порнография);

– преступления, связанные с нарушением авторского права и смежных прав;

– преступления, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем» [2, с. 171].

Во-вторых, такая Конвенция ставит достаточно важные и существенные процессуальные вопросы, вопросы взаимодействия правоохранительных органов государств, а также вопросы юрисдикции, которые определяются определенной характеристикой государства, в том числе территориальной.

До настоящего времени Российская Федерация не стала участником Конвенции. Считается, что статья 32 Конвенции «противоречит российскому законодательству и нарушает суверенитет государства» [3, с. 39], поскольку в ней говорится, что такие действия могут быть предприняты без своевременного уведомления и без согласия стороны, против которой предпринимаются действия.

Выделим, что понимается под компьютерными преступлениями. Конечно, это, в первую очередь, противоправное деяние, где компьютер является или объектом, против которого совершается преступление, или инструментом, используемый для совершения преступных действий. Также это такие преступления, которые совершаются с использованием компьютерной информации, где компьютерная информация – предмет и (или) средство совершения направленных против закона действий.

Согласно действующему Уголовному кодексу РФ преступлениями в сфере компьютерной информации являются преступления, совершаемые в области обработки информации и нарушения информационной безопасности.

Глава 28 УК РФ содержит нормы, регламентирующие ответственность за преступления в сфере компьютерной информации. Включение данной главы в действующий кодифицированный уголовный закон обусловлено коренными изменениями общественных отношений в Российской Федерации и формированием открытого информационного общества. Очевидная опасность данных преступлений обусловлена тем, что компьютеры и другие современные устройства, а также хранимая и передаваемая с их помощью информация соприкасаются со всеми сферами жизни современного общества.

Интересно отметить, что большая часть преступлений, предусмотренных главой 28 УК РФ, зарегистрирована по статье 272 УК РФ. Удельный вес данного преступления среди иных преступлений в сфере информационных технологий составляет 83,8 %. Затем идет состав преступления, предусматривающий уголовную ответственность по статье 273 УК РФ. На него приходится 15,4 % от всех преступлений в киберпространстве. Если обратиться к статье 274 УК РФ, то следует подчеркнуть, что этот процент незначителен, и подобные преступления совершаются редко. В данном случае проблема не в том, что рассматриваемые действия не совершаются, напротив, существует множество трудностей с их квалификацией.

Как уже отмечалось выше, развитие современных информационных технологий и распространение компьютеризации коренным образом изменили криминальную среду не только на национальном, но и на глобальном уровне. Из-за отсутствия надлежащего и профессионального социального регулирования Интернет сегодня безнаказанно используется преступниками как место совершения не только традиционных преступлений, таких как кражи, но и более сложных, замаскированных и завуалированных хищений, таких как продажа конфиденциальной информации и вымогательство, а также многих иных видов преступлений.

Следует отметить, что особую опасность представляет экстремизм в Интернете и его крайняя предельная форма – терроризм, то есть поведение, нарушающее работу информационных систем и выводящее их из строя, «создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решения государственными органами, а также угроза совершения вышеуказанных действий в тех же целях» [4, с. 59].

Сегодня российская наука не содержит единого мнения по поводу определения понятия «кибертерроризм». Так, кибертерроризм – это совокупность общественно опасных действий в виртуальном пространстве, которые создают угрозу безопасности личности, общества, государства.

Кибертерроризм – это серьезная проблема всего человечества, ее можно даже сравнить с самыми разрушительными, уничтожающими видами современного оружия – бактериологическим, ядерным, химическим. Интересно отметить, что в этой области мировой опыт констатирует уязвимость, незащищенность государств, ведь у терроризма в сети Интернет нет каких-либо государственных границ. Террорист в виртуальном пространстве способен угрожать таким информационным системам, которые расположены в любой точке мира.

Можно привести примеры преступлений такой направленности в мировой истории. Например, «в 1996 г. против дипломатических представительств Шри-Ланки одна из террористических организаций провела сетевую атаку; в 2004 г. электронные ресурсы правительства Южной Кореи были подвергнуты массированной атаке; в 2005–2006 гг. было зафиксировано более 2 млн кибернападений на информационные ресурсы органов государственной власти, в том числе свыше 300 тыс. атак на интернет-представительство Президента РФ» [5, с. 120].

Интересно отметить, что кибертеракты могут быть совершены с помощью множества различных приемов:

– доступ к информации, представляющей собой разновидность конфиденциальной, банковской или личной информации, угроза разглашения такой информации третьим лицам либо передачи ее в свободный и широкий доступ;

– вмешательство в работу или повреждение различных физических элементов информационного пространства – использование вредоносных программ, нарушающих работу электросетей, создающих помехи или выводящих из строя аппаратуру;

– дезинформация и захват средств массовой информации для демонстрации силы террористических организаций и передачи их требований;

– уничтожение или активное подавление линий связи, неправильная адресация, перегрузка узлов коммуникации;

– проведение информационно-психологических операций и т. п.;

– кража либо ликвидация программ, данных информационных ресурсов посредством взлома систем защиты, разработки и внедрения вирусов и т. п.;

– влияние на информацию и программное обеспечение» [6, с. 171].

Подчеркнем, что террористы в киберпространстве имеют определенное финансирование и материальную поддержку. Безусловно, это делается с определенными целями. Например, можно выделить, в чем же состоится интерес финансирования кибертерроризма транснациональными корпорациями. Ответ достаточно прост: данным способом корпорации устраняются конкурентов, а также производят изменения в так называемом инвестиционном климате государств, где они непосредственно осуществляют свою деятельность.

Также интерес материальной поддержки кибертеррористов есть у отдельных государств, которые таким образом решают конкретные политические проблемы на различных уровнях, как на мировом, так и на локальном.

Мотивы преступника, занимающегося кибертеррористической деятельностью, также можно определить. Они практические не меняются и бывают либо финансовыми, либо политическими. Террористы в виртуальном пространстве достаточно грамотные люди, поэтому, безусловно, осознают факт серьезной зависимости государственных инфраструктур от информационно-телекоммуникационных сетей и пользуются этим в своих преступных целях. К примеру, «в статье Мохаммеда бен Ахмада ас-Салима «39 способов служить и участвовать в джихаде» вводится понятия «электронный джихад», который рассматривается как один из способов дестабилизации западных государств» [7, с. 48].

Эффективность противодействия кибертерроризму затрудняется, ведь он с каждым годом становится привлекательнее для преступников и имеет всемирные сетевые масштабы. Также подчеркнем, что дешевле и проще получить средства для совершения таких противоправных деяний, чем приобрести традиционное классическое оружие.

Н.В. Григорьев считает, что «в отличие от традиционных форм терроризма, компьютерный обладает более высокой степенью анонимности и в то же время устраняет необходимость в территориальной близости к цели» [8, с. 7], что, безусловно, делает его более популярным, ведь тогда уменьшается возможность захватить или уничтожить преступника во время атаки.

Последствия такого терроризма для огромного количества людей имеют глобальный характер. Стоит согласиться с мнением Фрэнка Барнаби, который пишет, «…что компьютерный террорист с ноутбуком в состоянии причинить больше вреда, чем террорист, вооруженный бомбами и иными видами традиционного оружия» [9, с. 171].

Аудитория пользователей сети Интернет за год увеличилась на 5,1 % (+6 млн человек) и теперь составляет 124 млн человек, это 85 % населения Российской Федерации. На основании данных показателей можно выделить, что террористы в киберпространстве могут оказывать прямое или косвенное воздействие на огромное количество российского населения.

Сегодня в России проводится ряд организационных мер по борьбе с терроризмом в сети Интернет. В 2013 г. ФСБ РФ были делегированы полномочия по созданию государственного механизма по обнаружению, предупреждению и ликвидации атак в российском виртуальном пространстве.

В 2016 г. была утверждена Доктрина информационной безопасности РФ, получившая дальнейшее развитие с принятием Стратегии развития информационного общества в РФ на 2017–2030 гг.

«Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере»[1].

«Стратегия определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов»[2].

Статья 280 Уголовного кодекса РФ предусматривает ответственность за открытые призывы к осуществлению экстремистской деятельности. Вторая часть этой статьи предусматривает аналогичные действия, совершенные с использованием информационно-коммуникационных сетей, в том числе средств массовой информации и Интернета.

Согласно пункту 1 статьи 1 Федерального закона «О противодействии экстремистской деятельности» экстремистской деятельностью признаются «публичные призывы к совершению преступлений по мотивам политической ненависти или вражды, либо по мотивам ненависти или вражды в отношении к какой-либо социальной группы»[3].

Одной из основных угроз национальной безопасности Российской Федерации является экстремистская деятельность националистических, радикальных социальных, религиозных, этнических и иных организаций и групп, направленная на «нарушение единства и территориальной целостности Российской Федерации»[4], дестабилизацию политической и социальной обстановки в стране.

Экстремизм в цифровом пространстве – это «форма экстремистской деятельности физических и юридических лиц по незаконному созданию, хранению и массовому распространению» [10, с. 60] экстремистской информации в информационно-коммуникационной сети Интернет. Отметим, что распространению экстремизма в виртуальном пространстве содействует достаточно низкая цена создания, применения сетевых ресурсов, ведь для человека, хорошо владеющего навыками программирования, не создаст каких-либо трудностей разработать сайт, открыть аккаунт, группу в социальной сети.

Приведем пример из судебной практики. *Антонов Д.В. зарегистрировался на сайте в сети Интернет, создав учетную запись пользователя, то есть ему была предоставлена возможность публиковать в ней разного рода графические, текстовые, видеоматериалы, аудиоматериалы, а также примечания, так называемые комментарии к ним.*

Воспользовавшись указанной возможностью, Антонов Д.В., испытывая чувство ненависти к представителям ФСИН России, имея прямой умысел на открытое обращение к неопределенному кругу лиц с призывом к осуществлению экстремистской деятельности посредством сети Интернет, 16 апреля 2020 г. по адресу своего места жительства вошел в открытую информационно-коммуникационную сеть Интернет, являющуюся общим и широко распространенным ресурсом социальных сетей, с помощью мобильного телефона, принадлежащего ему, разместил комментарии в группе к видеозаписи, содержащей призыв к насильственным действиям в отношении сотрудников ФСИН России[5].

Подчеркнем, что сегодня увеличилась эффективность, результативность работы правоохранительных органов в направлении обнаружения преступлений, связанных с

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 9.05.2017 № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

[3] О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3031.

[4] Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года: Указ Президента РФ от 29.05.2020 № 344 // Собрание законодательства Российской Федерации. 2020. № 22. Ст. 3475.

[5] Приговор № 1-310/2020 от 27.07.2020 по делу № 1-310/2020. Доступ из интернет-ресурса «Судебные и нормативные акты РФ (СудАкт)» (дата обращения: 20.04.2023).

экстремистской деятельностью. Их количество возросло более чем на четверть (1057, +26,9 %). Две трети (62,5 %) преступлений совершены с использованием сети Интернета (в 2020 г. – 56,8 %). Также в соответствии с анализом результатов деятельности правоохранительных органов отметим, что при совершении преступлений данной направленности активно используются социальные сети и мессенджеры. На такую статистику также повлиял рост числа преступлений по статье 280 УК РФ. Так, зарегистрировано 486 таких деяний. Количество фактов организации деятельности экстремистских организаций также возросло почти на треть – 278. В 2021 г. количество преступлений террористической направленности с использованием сети Интернет выросло на треть – 576[6].

На сегодняшний момент государство активно предпринимает меры для предупреждения преступлений в сфере компьютерной информации. Данные меры нельзя назвать предотвращающими рассматриваемый вид преступных посягательств, а, наоборот, это больше контрмеры в ответ на уже совершенные преступные посягательства. Следует подчеркнуть, что современный преступник в виртуальном пространстве значительно быстрее, ловчее осваивает данные, инициативнее, динамичнее изучает и затем применяет в своей противоправной деятельности новейшие технические разработки.

Заключение

Под преступностью в сфере компьютерной информации понимаются деяния, совершаемые в виртуальном пространстве, включая неправомерное вмешательство в функционирование компьютеров, компьютерных программ и компьютерных сетей, несанкционированное изменение компьютерных данных и иные противоправные общественно опасные деяния, совершаемые с использованием компьютеров, компьютерных сетей и программ.

Компьютерные преступления имеют широкий масштаб незаконных, противоправных деяний, начиная от мошенничества, кражи личной информации и заканчивая преступлениями на почве ненависти и распространение наркотиков. Ежегодное увеличение компьютерных преступлений вызвано доходностью, минимальностью риска. Количество киберугроз, безусловно, росло, растет и будет расти, поэтому такую проблему следует поставить в приоритет каждому человеку, организациям и в целом государствам. На основании прогнозов к 2025 г. ущерб от компьютерных преступлений, который получит мировая экономика, может составить до $10 трлн.

Подчеркнем, что привлечь преступника к уголовной ответственности за различные действия в сети Интернет довольно сложно, ведь характер таких действий может быть многообразным, при этом в УК РФ отсутствует какая-либо иерархия тяжести совершенных лицом деяний.

В настоящее время потенциал экстремизма и терроризма в Сети огромен, в первую очередь, он используется как способ решения проблем экономического, политического, социального характеров. Часто определенные экстремисты, террористы либо группа экстремистов, террористов заявляют конкретные угрозы о выведении из строя, дестабилизации объектов жизнеобеспечения людей, предприятий, жилого фонда и т. д. Очевидно, что такие общественно опасные действия даже без выдвижения, к примеру, каких-либо политических требований, способны очень резко и серьезно нарушить спокойную обстановку в стране, стать так называемым спусковым крючком для организации различного рода несанкционированных, неразрешенных массовых выступлений, что неминуемо может привести к существенному снижению уровня как жизни населения, так и законности, легитимности государственной власти в стране.

[6] Количество экстремистских преступлений в РФ выросло более чем на четверть в 2021 г. // ТАСС. URL: https://tass.ru/obschestvo/14478143?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 20.04.2023).

Список источников

1. *Стяжкина С.А.* Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ) // Вестник Удмуртского университета. Серия «Экономика и право». 2021. № 3. С. 489-496. https://doi.org/10.35634/2412-9593-2021-31-3-489-496, https://elibrary.ru/cjnjmw
2. *Чернякова А.В.* Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 168-179. https://elibrary.ru/yxrbdf
3. *Атнашев В.Р.* Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3 (29). С. 37-42. https://elibrary.ru/avhdyz
4. *Ищенко Е.П.* Виртуальный криминал. М.: Проспект, 2014. 228 с.
5. *Геворгян Е.М.* Кибертерроризм как угроза информационной безопасности Российской Федерации // Скиф. Вопросы студенческой науки. 2021. № 6 (58). С. 118-122. https://elibrary.ru/puppdf
6. *Моторина Т.С., Шамсудинова В.В.* Кибертерроризм как угроза информационной безопасности Российской Федерации // Научные исследования XXI века. 2020. № 3 (5). С. 168-172. https://elibrary.ru/bbmfgg
7. *Серебренникова А.В.* Кибертерроризм: причины и условия // Colloquium-Journal. 2021. № 17 (104). С. 47-49. https://doi.org/10.24412/2520-6990-2021-17104-47-49, https://elibrary.ru/tjrxhe
8. *Григорьев Н.В.* Влияние кибертерроризма на молодежную среду // Вестник национального антитеррористического комитета. 2017. № 2. С. 5-8.
9. *Малик Е.Н.* Кибертерроризм как мировая угроза: вызовы и меры борьбы // Вестник Прикамского социального института. 2020. № 1 (85). С. 169-173. https://elibrary.ru/qqjhod
10. *Бутенко А.С.* Экстремизм в сети Интернет: понятие и сущность // Юристъ-Правоведъ. 2019. № 2 (89). С. 57-61. https://elibrary.ru/pxvdkl

References

1. Styazhkina S.A. (2021). Criminal-legal features of the qualification of violations of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunications networks (article 274 of the criminal code of the Russian Federation). *Vestnik Udmurtskogo universiteta. Seriya «Ekonomika i pravo» = Bulletin of Udmurt University. Series Economics and Law*, no. 3, pp. 489-496. (In Russ.) https://doi.org/10.35634/2412-9593-2021-31-3-489-496, https://elibrary.ru/cjnjmw
2. Chernyakova A.V. (2018). International and foreign experience of criminal law counteraction to thefts committed by using computer information. *Yuridicheskaya nauka i pravookhranitel'naya praktika = Legal Science and Law Enforcement Practice*, no. 4 (46), pp. 168-179. (In Russ.) https://elibrary.ru/yxrbdf
3. Atnashev V.R. (2019). International cooperation on cybercrime and cyberterrorism. *Evraziiskaya integratsiya: ekonomika, pravo, politika = Eurasian Integration: Economics, Law, Politics*, no. 3 (29), pp. 37-42. (In Russ.) https://elibrary.ru/avhdyz
4. Ishchenko E.P. (2014). *Virtual'nyi criminal* [Virtual Crime]. Moscow, Prospekt Publ., 228 p. (In Russ.)
5. Gevorgyan E.M. (2021). Cyber terrorism as a national safety's threat of Russian Federation. *Skif. Voprosy studencheskoi nauki = Sciff. Questions of Student Science*, no. 6 (58), pp. 118-122. (In Russ.) https://elibrary.ru/puppdf
6. Motorina T.S., Shamsudinova V.V. (2020). Cyber terrorism as a national safety's threat of Russian Federation. *Nauchnye issledovaniya XXI veka* [Scientific Research of the 21st Century], no. 3 (5), pp. 168-172. (In Russ.) https://elibrary.ru/bbmfgg
7. Serebrennikova A.V. (2021). Cyber terrorism: causes and conditions. *Colloquium-Journal*, no. 17 (104), pp. 47-49. (In Russ.) https://doi.org/10.24412/2520-6990-2021-17104-47-49, https://elibrary.ru/tjrxhe
8. Grigor'ev N.V. (2017). Vliyanie kiberterrorizma na molodezhnuyu sredu [The impact of cyberterrorism on youth]. *Vestnik natsional'nogo antiterroristicheskogo komiteta = Herald of the National Antiterrorism Committee*, no. 2, pp. 5-8. (In Russ.)
9. Malik E.N. (2020). Cyberterrorism as a world threat: challenges and measures of struggle. *Vestnik Prikamskogo sotsial'nogo institute = Bulletin of Prikamsky Social Institute*, no. 1 (85), pp. 169-173. (In Russ.) https://elibrary.ru/qqjhod

10. Butenko A.S. (2019). Extremism on the Internet: the concept and the essence. *Yurist"-Pravoved"* [Jurist-Lawyer], no. 2 (89), pp. 57-61. (In Russ.) https://elibrary.ru/pxvdkl

Авторы заявляют об отсутствии конфликта интересов. / Authors declare no conflict of interests.

Поступила в редакцию / Received 14.08.2023
Поступила после рецензирования / Revised 09.11.2023
Принята к публикации / Accepted 17.11.2023