Научная статья

УДК 343
EDN: FAFWRA

КИБЕРТЕРРОРИЗМ КАК СОВРЕМЕННАЯ УГРОЗА КОЛЛЕКТИВНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина Владимировна Семёнова[1], Наталья Ивановна Карчевская[2]
[1, 2] Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии, Санкт-Петербург, Россия
[1] 9053202867@mail.ru
[2] karcheva68@mail.ru

Аннотация. В статье рассматриваются актуальные вопросы, связанные с уровнем общественной опасности киберпреступлений и кибертерроризма, в частности, проблемой противодействия кибертерроризму как преступлению против безопасности Российской Федерации. Влияние информационно-коммуникационных технологий многогранно и противоречиво, что и привело к появлению новых видов преступлений: компьютерной преступности и кибертерроризму. Кибертерроризм представляет собой незаконные действия, угрожающие государственной безопасности, личности и обществу.

Ключевые слова: киберпреступность, терроризм, кибертерроризм, информационная безопасность, национальная безопасность, информационно-коммуникационные технологии

Для цитирования: Семёнова И.В., Карчевская Н.И. Кибертерроризм как современная угроза коллективной информационной безопасности // Вестник Санкт-Петербургского военного института войск национальной гвардии. 2023. № 4 (25). С. 30–37. URL: https://vestnik-spvi.ru/2023/12/004.pdf. EDN: FAFWRA.

Original article

CYBERTERRORISM AS A MODERN THREAT TO COLLECTIVE INFORMATION SECURITY

Irina V. Semyonova[1], Natalya I. Karchevskaya[2]
[1, 2] Saint-Petersburg Military Order of Zhukov Institute of the National Guard Troops, Saint-Petersburg, Russia
[1] 9053202867@mail.ru
[2] karcheva68@mail.ru

Abstract. The article discusses current issues related to the level of public danger of cybercrime and cyberterrorism, in particular, the problem of countering cyberterrorism as a crime against the security of the Russian Federation. The influence of information and communication technologies is multifaceted and contradictory, which has led to the emergence of new types of crimes – computer crime and cyber terrorism. Cyberterrorism is illegal actions that threaten state security, individuals and society.

Keywords: cybercrime, terrorism, cyberterrorism, information security, national security, information and communication technologies

For citation: Semyonova I.V., Karchevskaya N.I. Cyberterrorism as a modern threat to collective information security. Vestnik Sankt-Peterburgskogo voennogo instituta vojsk nacional'noj gvardii. 2023;4(25): 30–37. (In Russ.). Available from: https://vestnik-spvi.ru/2023/12/004.pdf. EDN: FAFWRA.

Введение

Сложно представить современный мир без использования информационных технологий как совокупности методов, производственных и программно-технологических [1] средств, объединенных в технологическую цепочку и обеспечивающих сбор, хранение, обработку, вывод и распространение информации. Именно информационные технологии позволяют снижать трудоемкость процессов использования информационных ресурсов. Закономерно, что современные инфротехнологии породили такое новое явление, как компьютерная преступность и её разновидность – компьютерный террор [19]. Следовательно, киберпреступность и кибертерроризм можно рассматривать как новые методы преступной деятельности, опирающиеся на современные средства связи и информатики.

Несмотря на то, что цифровые технологии приносят значительные экономические и социальные выгоды большей части населения мира, такие проблемы, как отсутствие глобальной системы управления технологиями и небезопасность киберпространства, представляют значительный риск.

Основные положения

Анализ статистических данных позволяет говорить о том, что количество кибератак, которым подвергаются пользователи интернет-ресурсов, постоянно растет. По данным Бюро специальных технических мероприятий МВД России, количество компьютерных преступлений в России по сравнению с прошлым (2022) годом выросло в полтора раза, в связи с чем вопрос формирования системы информационной безопасности является на сегодняшний день, по мнению авторов, одной из приоритетных задач, стоящих перед правоохранительными органами Российской Федерации[1].

В числе главных негативных аспектов кибертеррористических атак, совершаемых террористическими организациями, следует назвать рост международной напряженности, подрыв доверия между государствами, провоцирующих возникновение глобальных экономических и политических кризисов. Кибертерроризм сегодня отнесен к числу главных угроз мировому сообществу, противодействие которому выступает одной из актуальных задач государств в обеспечении национальной безопасности [18].

Доктрина информационной безопасности Российской Федерации обращает внимание на то, что террористические и экстремистские группировки применяют методы манипулирования людьми, группами и общественным мнением с целью разжигания межнациональной и социальной розни, возбуждения вражды и ненависти по национальному и религиозному признакам, распространения экстремистских принципов. Кроме того, эти организации со злым умыслом создают средства поражающего воздействия на объекты критической информационной инфраструктуры[2].

Как уже было отмечено, развитие информационных технологий привело к тому, что они закономерно стали применяться в преступной деятельности. Изучение оперативной обстановки, связанной со сдерживанием, выявлением и пресечением компьютерных преступлений, показывает, что в информационно-телекоммуникационной сети Интернет наблюдается тенденция к изменению видов преступной деятельности в сфере информационных технологий и электронной коммерции [11].

Прежде чем характеризовать кибертерроризм как современную угрозу коллективной информационной безопасности, необходимо разобраться с толкованием самого термина «кибертерроризм», поскольку в научной литературе существуют различные точки зрения по данному вопросу [2, 9, 15, 16].

Чаще всего киберэкстремизм представляется как форма экстремистской деятельности в информационном пространстве. Таким образом, речь идет непосредственно о криминальном использовании технологий приема, обработки, передачи, хранения и распространения информационных сообщений экстремистского характера, содержащей оскорбления в адрес каких-либо социальных (прежде всего, этнических и религиозных) групп, призывы к насилию над ними [12].

[1] В 2022 году в России было зафиксировано около 510 тыс. преступлений с использованием информационных технологий против 10 тыс. в 2014-м. Таким образом, речь идет о более чем 50-кратном росте числа ИТ-преступлений. Такие цифры 22 мая 2023 года озвучил представитель криминалистического центра Следственного комитета Темирлан Салихов // Киберпреступность и киберконфликты: Россия // https://www.tadviser.ru/index.php (дата обращения: 23.10.2023).

[2] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание Законодательства Российской Федерации. 2016. № 50. Ст. 7074.

Кроме того, следует обратить внимание на тот факт, что толкование кибертерроризма необходимо осуществлять как минимум с двух позиций: технологической и диалектической. Технологический подход предполагает, что в этом случае кибертерроризм следует понимать, как «использование информационных технологий террористическими группами и отдельными лицами. Это может включать использование информационных технологий для организации и выполнения атак против сетей, компьютерных систем и телекоммуникационных инфраструктур, а также для обмена информацией или угроз в электронном виде. Взлом компьютерных систем, ввод вирусов для уязвимых сетей, разрушение веб-сайтов и прочие действия, которые могут причинить вред компьютерным технологиям»[3]. Диалектический подход позволяет дефинировать кибертерроризм, как «умышленную разрушительную деятельность, или угрозы, реализуемые посредством применения компьютеров и/или сетей, с намерением причинить вред или дальнейшие социальные, идеологические, религиозные, политические последствия либо запугать любое лицо в целях содействия таким целям» [12].

Разночтение и неточность в понятиях, возникающие вследствие отсутствия единого подхода к трактовкам и формулировкам, крайне затрудняют определение их истинного уровня опасности киберпреступлений, когда данное явление пытаются использовать в правоприменительной практике при количественном учете и классификации новых видов киберпреступлений [4].

Для обеспечения правовых основ безопасности информационно-коммуникационных технологий, как минимум, в каждом отдельном государстве на национальном уровне необходимо систематизировать и упорядочить нормативные правовые документы, регламентирующие деятельность в данной области. Для успешности результатов данной работы следует определить необходимые критерии, формирующие информационную безопасность (например, «защита источников информации»; «борьба с киберпреступностью»; «борьба с кибертерроризмом»; «информационное обеспечение реализации государственной политики»; «защита киберпространства»; «обеспечение безопасности инфраструктуры передачи данных и связи» и т. д.), а также четко сформулировать и упорядочить термины, используемые в нормативных правовых документах. Таким образом, для достижения гармонии и единообразия лексических форм терминология правовых актов, созданных в одной и той же области, не должна существенно различаться, и, кроме того, должна быть обеспечена устойчивая согласованность используемых понятийных и терминологических принципов[4].

На основании анализа и обобщения российских и зарубежных источников можно заключить, что кибертерроризм – это преднамеренная, идеологически и политически мотивированная преступная деятельность, осуществляемая в киберпространстве посредством цифровых технологий и направленная против информации, компьютерных систем, компьютерных программ и баз данных, а также объектов критической информационной инфраструктуры, которая создает угрозу жизни или здоровью людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения и органов власти, достижения преступных намерений, провокации военного конфликта [5, 10, 14]. При этом террористические кибератаки могут быть направлены на объекты, как виртуальной среды, так и реальной действительности [17, 6].

По мнению авторов, необходимо обратить внимание на то обстоятельство, что так называемый «обычный» террор применяется для совершения «традиционных» террористических актов, привычными для понимания обычных граждан, видов оружия и механизмов, с помощью которых приводят в действие взрывные устройства. Напротив, киберпреступники используют «нетрадиционное» оружие, под которым понимается информационное оружие, и, в первую очередь, его современная форма – всемир-

[3] Роскомнадзор. Публичный доклад 2016. URL: https://rkn.gov.ru/docs/doc_1646.pdf (дата обращения: 23.10.2023).

[4] Постановление № 7-6 Парламентской Ассамблеи Организации Договора о коллективной безопасности «О проекте Рекомендаций по сближению и гармонизации национального законодательства государств-членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности» (Вместе с <Примерным перечнем опасных правонарушений, затрагивающих национальные интересы>) (Принято в г. Санкт-Петербурге 27.11.2014) // https://paodkb.org/documents/postanovlenie-soveta-parlamentskoy-assamblei-organizatsii-dogovora-o-0f1c9ce9-d286-457d-a825-6be775310f80// (дата обращения: 23.10.2023).

ная информационная компьютерная сеть – Интернет [7]. Таким образом, современные достижения техники используются с целью негласного получения доступа к информации, с возможностью проводить различного рода манипуляции с ней [3].

Необходимо понимать, что в процессе противостояния «обычному» терроризму следует использовать комплексный подход борьбы, сочетающий культурные начала с политическими, экономическими, правовыми и социальными мерами.

Гораздо сложнее складывается обстановка в рамках борьбы с «новым» терроризмом. Как уже отмечалось, использование информационных технологий сегодня, привело к появлению кибертерроризма, способного с помощью манипуляций компьютерными системами вносить хаос в современную жизнь. Однако следует знать, что на сегодняшний день существует типология правонарушений, которая может помочь выстроить единый механизм анализа и оценки состояния, а также прогресса киберпреступности. Кроме того, это позволит предложить практические рекомендации противодействия и пути международного сотрудничества в этой области [8].

Всемирная паутина Интернет играет важную роль в распространении экстремистского и иного противоправного мышления в современных условиях. Электронные средства массовой информации (особенно неофициальные, нелегальные) являются удобным и эффективным инструментом для распространения разнообразных радикальных взглядов. На наш взгляд, кибертерроризм следует характеризовать как одну из разновидностей терроризма, характеризующуюся использованием цифровых технологий и вредоносных программ, с помощью которых преступники получают незаконный доступ к компьютерным системам для достижения своих противоправных целей.

Кроме того, по мнению авторов, следует четко определить методы кибертерроризма, которые можно охарактеризовать, как несанкционированное проникновение в целевую систему или захват контроля над ней путем взлома, в том числе путем получения или похищения идентификационных данных, которые могут быть использованы для входа в систему (расширения прав пользователя); использование языка программирования или набора команд для обнаружения и использования уязвимостей в программных приложениях; распространение компьютерных вирусов, корректирующих и уничтожающих данные или затрудняющих работу компьютерных систем; внедрение в программу вирусов – вредоносных программ, которые при определенных обстоятельствах (временных или информационных) запускаются (активизируются) для выполнения злонамеренных операций (как правило, несанкционированного доступа к данным, искажения или уничтожения).

Например, запрещено использовать такие программы, как «троянский конь», позволяющие доставлять данные на удаленные компьютеры или выполнять вредоносные действия без ведома владельца зараженной системы. Также не допускается создание помех и препятствий для обмена информацией в сетях путем нарушения работы серверов и сайтов с помощью DoS/DDoS-атак[5].

Очевидно, что государственные органы все чаше вынуждены задаваться вопросами кибербезопасности.

В качестве примера следует обратить внимание на то, что с целью обеспечения кибербезопасности, на законодательном уровне было закреплено требование о подготовке специалистов по отдельным направлениям противодействия терроризму (например, по идеологии терроризма, ядерному, химическому, биологическому и кибертерроризму), однако, данное положение не было эффективно реализовано[6].

Российской Федерацией предпринимаются меры по предотвращению оттока кадров данной сферы деятельности (например, предоставление льгот и особых условий), но стоит заметить, что эти меры вряд ли можно считать успешными в отношении тех, кто работает в государственном секторе, а не в частных компаниях. Тем не менее для решения проблемы кибертерроризма стоит обратить внимание и на работу, которая ведется в рамках международного сотрудничества. Так, например, в

[5] Постановление № 51-24 Межпарламентской Ассамблеи государств-участников СНГ «О Рекомендательных типологиях новых преступлений, совершаемых с использованием информационных технологий» (Принято в г. Санкт-Петербурге 27.11.2020) // http://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendatcii_mpa_sng/vspomogatelnie_pravovie_akti_i_zakonoproektnie_predlozheniya (дата обращения: 23.10.2023).

[6] Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 05.10.2009) // https://www.consultant.ru/document/cons_doc_LAW_92779/ (дата обращения: 23.10.2023).

рамках этого сотрудничества государства, входящие в ОДКБ, разрабатывают меры по борьбе с кибертерроризмом и совершенствуют нормативное правовое регулирование в этой области, поскольку непосредственно расширяется спектр угроз информбезопасности, включая их характер и интенсивность, и, кроме того, увеличиваются количество и частота попыток иностранных государств получать конфиденциальную информацию о состоянии обеспечения национальной информбезопасности[7].

В качестве мер по укреплению способности бороться с терроризмом и трансграничной преступной деятельностью, по мнению авторов, следует обратить внимание и на борьбу с поддержкой распространения терроризма и трансграничной преступной деятельности, в частности, по вопросам организационно-правовой деятельности государственных органов. На наш взгляд, именно деятельность всех соответствующих государственных органов, направленных на реализацию правовых предписаний, особая ответственность в деятельности правоохранительных органов, в вопросах и процессе противостояния кибертерроризму и финансированию террористической деятельности, возможна путем установления прочной связи между учебными центрами, разработки соответствующих программ и мероприятий (например, таких как курсы повышения квалификации, встречи с квалифицированными специалистами-практиками и научно-практические семинары) [20].

Следует отметить, что с целью разработки квалифицированных методов борьбы (противостояния) с IT-преступлениями осуществляется анализ экономики внедрения информационных технологий; сбор, сортировка и проверка индивидуальных данных; разработка приложений, обеспечивающих безопасное и надежное хранение и передачу данных; обучение программам машинного обучения; разработка решений в области искусственного интеллекта; создание и применение блокчейн-решений; консультирование по вопросам интернет-безопасности.

Необходимо обратить внимание, насколько остро стоит проблема обеспечения безопасности в цифровой сфере [13]. В связи с попытками решения данной проблемы осуществляется сбор, систематизация и верификация передачи данных; согласованная борьба с организованной киберпреступностью и кибертерроризмом (перенос реальных методов в виртуальный мир); контроль за системой «электронного государства»; создается новый двусторонний канал взаимодействия между правительством и гражданами, требующий постоянной модерации и контроля за ходом общения; обеспечение непрерывности работы (в случае сбоев в работе ИТ; ликвидация цифровой безграмотности среди населения и его обучение в области IT-технологий; создание облачных систем хранения информации; манипулирование массивами данных; формулирование норм хранения данных; оперирование формулами шифрования; создание средств представления данных; оценка опасности ИТ-систем; создание машин семантического поиска и перевода; обеспечение взаимодействия компьютера и человека).

Нельзя не согласиться с мнением Токолова А. В., что разработка высокотехнологичных цифровых механизмов противодействия кибертерроризму и объединение усилий государств всего мира является первоочередной задачей на современном этапе. Международному сообществу следует выработать единые для всех стран правила игры в сфере цифровых технологий, универсальный и общий для всех международный стандарт, который будет максимально учитывать интересы каждой страны. Должна быть улучшена трансграничная система обмена данными о киберугрозах. Вместе с тем меры безопасности не должны приниматься в ущерб технологическому прогрессу и инновациям. Свобода общения и коммуникаций, а также беспрепятственный обмен опытом и идеями в цифровую эпоху должны быть законодательно гарантированы [17].

Следует заметить, что опасности, которые таят в себе новые информационно-технологические разработки, вовсе не означают, что нельзя двигаться вперед по пути научно-технического прогресса. Кроме того, как принято считать, разнообразие – это приправа к жизни. Множество разнообразных впечатлений помогают людям стать всесторонне развитыми, открывают глаза на красоту и сложность окружающего нас мира. Эксперименты с чем-то незнакомым и еще не изведанным

[7] Постановление № 14-7.1 Парламентской Ассамблеи Организации Договора о коллективной безопасности «О проекте модельного закона ОДКБ "Об информационной безопасности"» (Принято в г. Москве 29.11.2021 // https://paodkb.org/events/ assambleya-prinyala-modelnyy-zakon-ob-informatsionnoy-bezopasnosti / (дата обращения: 23.10.2023).

могут стать захватывающим приключением. Диверсификация деятельности приносит новое удовольствие и помогает оценить разнообразие перспектив. Пробуя что-то новое, мы можем получить столь необходимый отдых от повседневной рутины.

Знакомство с различными видами деятельности может быть очень полезным. Знакомство с незнакомыми вещами может стать увлекательным путешествием и открыть множество перспектив. Разнообразие повседневных привычек может принести новое наслаждение и дать возможность отдохнуть от обыденности. Однако не следует забывать о правилах пользования чем-то новым и, по всей видимости, неизбежным. Важно, чтобы это новое не причинило неприятностей и не привело к непоправимым последствиям.

Заключение

Подводя итог вышесказанному, следует отметить, что рождение информационной эпохи ставит перед законодателями множество серьезных задач, некоторыми из которых являются: распознавание граждан и их личностей, обеспечение безопасности данных, решение вопросов юрисдикции в цифровой сфере, налогообложение цифровой торговли, борьба с киберпреступностью и кибертерроризмом. Государство должно быть гибким в политике разработки новых нормативных установок, что, в свою очередь, должно способствовать укреплению доверия в осуществлении онлайновых сделок и помогать находить баланс между экономическим прогрессом и сохранением конфиденциальности данных.

Список источников

1. Амирова Д. К. Кибертерроризм как современная угроза безопасности граждан / Д. К. Амирова, Р. И. Габдрахманова // Ученые записки Казанского юридического института МВД России. 2021. Т. 6. № 2 (12). С. 126–131.

2. Бычков В. В. Квалификация преступлений террористического характера, связанных с незаконным оборотом ядерных материалов и радиоактивных веществ / В. В. Бычков, В. Б. Вехов // Расследование преступлений: проблемы и пути их решения. 2019. № 3 (25). С. 49–54.

3. Вехов В. Б. Проблемы борьбы с кибертерроризмом / В. Б. Вехов, С. А. Ковалев // Правопорядок: история, теория, практика. 2018. № 1 (16). С. 89–93.

4. Витвицкая С. С. Киберпреступления: понятие, классификация, международное противодействие / С. С. Витвицкая, А. А. Витвицкий, Ю. И. Исакова // Правовой порядок и правовые ценности, 2023. Т. 1. № 1 С. 18–27.

5. Гасанов А. М. Понятие и признаки киберпреступлений / А. М. Гасанов, Я. Ю. Меженина // Colloquiumjournal. 2019. № 16-7 (40). С. 137–138.

6. Гедгафов М. М. Развитие кибертерроризма в условиях глобализации информационного пространства // Образование и право. 2021. № 6. С. 304–308.

7. Жуков А. З. Пути совершенствования методов по противодействию кибертерроризму в Российской Федерации // Пробелы в российском законодательстве. 2020. Т. 13. № 4. С. 67–70.

8. Карамова Э. И. К вопросу о кибертерроризме в глобализирующемся мире / Э. И. Карамова, С. М. Фомин // Социально-политические науки. 2016. № 3. С. 154–155.

9. Красинский В. В. Кибертерроризм: криминологическая характеристика и квалификация / В. В. Красинский, В. В. Машко // Государство и право. 2023. № 1. С. 79–91.

10. Кучерков И. А. О понятии «киберпреступление» в законодательстве и научной доктрине // Юридическая наука. 2019. № 10. С. 78–81.

11. Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В. С. Овчинского. М. : ИНФРА-М, 2021. 630 с.

12. Панталева Н. С. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности / Н. С. Панталева, Н. П. Пархитько // Юридическая наука. 2019. № 3. С. 47–50.

13. Полякова Т. А. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде / Т. А. Полякова, А. В. Минбалеев, И. С. Бойченко // Вестник Академии права и управления. 2018. № 3 (52). С. 32–36.

14. Рябинин К. Ю. Понятие и признаки киберпреступлений // Colloquium-journal. 2020. № 5–8 (57). С. 46–48.

15. Семенова И. В. Кибертерроризм как дестабилизирующий фактор, источник которого расположен вне сети / И. В. Семенова, С. И. Захарцев // Юридическая наука: история и современность. 2023. № 2. С. 79–87.

16. Семенова И. В. Понятие «кибертерроризм»: теоретико-правовой подход // Военное право. 2022. № 2 (72). С. 73–77.
17. Токолов А. В. Блокчейн-технология в обеспечении кибербезопасности государства // Вестник Московского университета МВД России. 2019. № 5. С. 221–225.
18. Хамурзов А.Т. Кибертерроризм: новые вызовы и меры противодействия // Юридические исследования. 2021. № 3 (2). С. 74–77.
19. Ханов Т. А. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений / Т. А. Ханов, А. Ж. Нуркеев // Известия Алтайского государственного университета. 2017. № 6 (98). С. 105–111.
20. Ширинова А. А. Кибертерроризм, как болезнь современной интернет-сети. Пути противодействиям / А. А. Ширинова, И. А. Семенцова // Уголовное законодательство России: основные проблемы применения и направления совершенствования: сборник материалов I Международной научно-практической конференции. 2019. С. 19–21.

References

1. Amirova D. K., Gabdrahmanova R. I. Kiberterrorizm kak sovremennaya ugroza bezopasnosti grazhdan. In: Uchenye zapiski Kazanskogo yuridicheskogo instituta MVD Rossii. 2021. Vol. 6;2 (12): 126–131. (In Russ.).
2. Bychkov V. V., Vekhov V. B. Kvalifikaciya prestuplenij terroristicheskogo haraktera, svyazannyh s nezakonnym oborotom yadernyh materialov i radioaktivnyh veshchestv. In: Rassledovanie prestuplenij: problemy i puti ih resheniya. 2019;3 (25): 49–54. (In Russ.).
3. Vekhov V. B., Kovalev S. A. Problemy bor'by s kiberterrorizmom. In: Pravoporyadok: istoriya, teoriya, praktika. 2018;1 (16): 89–93. (In Russ.).
4. Vitvickaya S. S., Vitvickij A. A., Isakova Yu. I. Kiberprestupleniya: ponyatie, klassifikaciya, mezhdunarodnoe protivodejstvi. In: Pravovoj poryadok i pravovye cennosti, 2023. Vol. 1;1: 18–27.
5. Gasanov A. M., Mezhenina Ya. Yu. Ponyatie i priznaki kiberprestuplenij. In: Colloquiumjournal. 2019;16-7 (40): 137–138. (In Russ.).
6. Gedgafov M. M. Razvitie kiberterrorizma v usloviyah globalizacii informacionnogo prostranstva. In: Obrazovanie i pravo. 2021;6: 304–308. (In Russ.).
7. Zhukov A. Z. Puti sovershenstvovaniya metodov po protivodejstviyu kiberterrorizmu v Rossijskoj Federacii. In: Probely v rossijskom zakonodatel'stve. 2020. Vol. 13;4: 67–70. (In Russ.).
8. Karamova E. I., Fomin S. M. K voprosu o kiberterrorizme v globaliziruyushchemsya mire. In: Social'no-politicheskie nauki. 2016;3: 154–155. (In Russ.).
9. Krasinskij V. V., Mashko V. V. Kiberterrorizm: kriminologicheskaya harakteristika i kvalifikaciya. In: Gosudarstvo i pravo. 2023:1: 79–91. (In Russ.).
10. Kucherkov I. A. O ponyatii «kiberprestuplenie» v zakonodatel'stve i nauchnoj doctrine. In: Yuridicheskaya nauka. 2019;10: 78–81. (In Russ.).
11. Ovchinskogo V. S. (eds.) Operativno-rozysknaya deyatel'nost' v cifrovom mire: sbornik nauchnyh trudov. Moscow: INFRA-M, 2021. (In Russ.).
12. Pantaleva N. S., Parhit'ko N. P. Kiberterrorizm i kiberekstremizm kak sovremennye ugrozy nacional'noj i mezhdunarodnoj bezopasnosti. In: Yuridicheskaya nauka. 2019;3: 47–50. (In Russ.).
13. Polyakova T. A., Minbaleev A. V., Bojchenko I. S. Problemy pravovogo obespecheniya informacionnoj bezopasnosti v processe ispol'zovaniya cifrovyh tekhnologij v global'noj cifrovoj srede. In: Vestnik Akademii prava i upravleniya. 2018;3 (52): 32–36 (In Russ.).
14. Ryabinin K. Yu. Ponyatie i priznaki kiberprestuplenij. In: Colloquium-journal. 2020;5–8 (57): 46–48. (In Russ.).
15. Semenova I. V., Zaharcev S. I. Kiberterrorizm kak destabiliziruyushchij faktor, istochnik kotorogo raspolozhen vne seti. In: Yuridicheskaya nauka: istoriya i sovremennost'. 2023;2: 79–87. (In Russ.).
16. Semenova I. V. Ponyatie «kiberterrorizm»: teoretiko-pravovoj podhod. In: Voennoe pravo. 2022;2 (72): 73–77. (In Russ.).
17. Tokolov A. V. Blokchejn-tekhnologiya v obespechenii kiberbezopasnosti gosudarstva. In: Vestnik Moskovskogo universiteta MVD Rossii. 2019;5: 221–225. (In Russ.).
18. Hamurzov A.T. Kiberterrorizm: novye vyzovy i mery protivodejstviya. In: Yuridicheskie issledovaniya. 2021;3 (2): 74–77. (In Russ.).
19. Hanov T. A., Nurkeev A. Zh. Sovremennye podhody k opredeleniyu komp'yuternoj prestupnosti i osobennosti komp'yuternyh prestuplenij. In: Izvestiya Altajskogo gosudarstvennogo universiteta. 2017;6 (98): 105–111. (In Russ.).

20. Shirinova A. A., Semencova I. A. Kiberterrorizm, kak bolezn' sovremennoj internet-seti. Puti protivodejstviyam. In: Ugolovnoe zakonodatel'stvo Rossii: osnovnye problemy primeneniya i napravleniya sovershenstvovaniya. 2019: 19–21. (In Russ.).

Информация об авторах

И. В. Семёнова – кандидат юридических наук
Н. И. Карчевская – кандидат юридических наук, доцент

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 27.11.2023;
одобрена после рецензирования 01.12.2023;
принята к публикации 25.12.2023.

Information about the authors

I. V. Semyonova – Candidate of Sciences (Law)
N. I. Karchevskaya – Candidate of Sciences (Law), Docent

Contribution of the authors: the authors contributed equally to this article.
The authors declare no conflicts of interests.

The article was submitted 27.11.2023;
approved after reviewing 01.12.2023;
accepted for publication 25.12.2023.