ГОСУДАРСТВО И ПРАВО, 2023, № 1, с. 79–91
STATE AND LAW, 2023, No. 1, pp. 79–91

КИБЕРТЕРРОРИЗМ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И КВАЛИФИКАЦИЯ

© 2023 г. В. В. Красинский[1, *], В. В. Машко[2, **]

[1]Главное управление региональной безопасности Московской области, г. Красногорск
[2]Российский государственный гуманитарный университет, г. Москва

**E-mail: krasinskijvv@fedsfm.ru*
***E-mail: kmbiai@yandex.ru*

Поступила в редакцию 23.05.2022 г.

Аннотация. В статье рассматривается проблема кибертеррористических посягательств на информационные ресурсы и информационную инфраструктуру. Авторы дают криминологическую характеристику различных видов кибертерроризма и предлагают варианты квалификации преступлений кибертеррористического характера. На основе зарубежного опыта обосновываются различные модели и актуальные направления противодействия кибертерроризму.

Ключевые слова: кибертерроризм, виды кибертерроризма, информационные ресурсы, информационная инфраструктура, информационные технологии, киберпространство, кибератаки, кибербезопасность, противодействие кибертерроризму, модели противодействия кибертерроризму.

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

DOI: 10.31857/S102694520024122-5

CYBERTERRORISM: CRIMINOLOGICAL CHARACTERISTICS AND QUALIFICATION

© 2023 V. V. Krasinsky[1, *], V. V. Mashko[2, **]

[1]Main Department of Regional Security of the Moscow Region, Krasnogorsk
[2]Russian State University for the Humanities, Moscow

**E-mail: krasinskijvv@fedsfm.ru*
***E-mail: kmbiai@yandex.ru*

Received 23.05.2022

Abstract. The article addresses the problem of the problem of cyberterrorist attacks on information resources and information infrastructure. Authors gives a criminological description of various types of cyberterrorism and offers options for qualifying crimes of a cyberterrorist nature. Based on foreign experience, various models and main directions of countering cyberterrorism are substantiated.

Key words: cyberterrorism, types of cyberterrorism, information resources, information infrastructure, information technology, cyberspace, cyberattacks, cybersecurity, countering cyberterrorism, models of countering cyberterrorism.

For citation: *Krasinsky, V.V., Mashko, V.V. (2023).* Cyberterrorism: criminological characteristics and qualification // Gosudarstvo i pravo=State and Law, No. 1, pp. 79–91.

В последние годы значительно актуализировались угрозы, связанные с попытками террористических структур использовать современные технологии для несанкционированного доступа и уничтожения информации, деструктивного воздействия на информационные ресурсы и информационную инфраструктуру различных государств, в том числе Российской Федерации. Такое положение привело к формированию нового вида преступной деятельности – кибертерроризма.

Актуальность изучения кибертерроризма определяется: широким внедрением в различные секторы государственного управления и экономики информационных технологий, уязвимостью оборудования, инфраструктуры и программного обеспечения перед киберугрозами; высокой степенью общественной опасности террористических кибератак[1]; развитием рынка хакерских услуг и потребителей кибертеррористических сервисов в даркнете; совершенствованием уровня организации и тактики террористической деятельности; усилением межгосударственного противоборства в киберпространстве[2] и использованием кибертерроризма как инструмента борьбы с недружественными государствами и военными противниками.

Примечательно, что возможность использования кибертерроризма в качестве компонента информационной войны была отмечена исследователями еще в начале XXI в.[3]

Террористическими структурами кибертерроризм рассматривается главным образом как элемент брендирования и поддержания репутации успешной организационной структуры. При этом большинство террористических организаций используют возможности сети Интернет не для осуществления кибертеррористических атак, а для распространения своей джихадистской идеологии, «теологического» обоснования террористических действий, размещения инструкций для подготовки и осуществления террористических актов, вербовочной деятельности и т.п.[4] В силу этого политики многих государств недооценивают угрозы, исходящие от кибертерроризма, и не уделяют должного внимания вопросам совершенствования механизмов противодействия данному явлению[5]. И это, несмотря на то что по характеру своего психологического воздействия на население кибертеррористические атаки сопоставимы с последствиями совершения традиционных актов терроризма. В частности, в серии исследований, касающихся явлений кибертерроризма, группа психологов во главе с Мишелем Гроссом эмпирически измерила последствия воздействия кибертерроризма в контролируемых экспериментальных условиях. Их ключевым выводом стало то, что воздействие кибертерроризма вызывает значительные негативные эмоции и когнитивные реакции (восприятие угрозы) на уровне, эквивалентном уровню обычных террористических актов, и усиливает у людей чувство уязвимости, тревоги, а также подрывает авторитет действующей власти[6].

Многие государства столкнулись с угрозами кибертерроризма в период существования квазигосударственного образования МТО «Исламское государство» на территории Сирии и Ирака.

Так, одним из первых хакеров ИГИЛ был Джунаид Хуссейн, представлявший группировку «Кибер-халифат». В марте 2015 г. указанная группировка опубликовала в свободном доступе списки военнослужащих армии США с призывами к нападениям на них и членов их семей.

В апреле 2016 г. МТО «Исламское государство» объявило о создании «Объединенной кибер-армии» («Объединенный кибер-халифат»), которая включала четыре хакерские группы, ранее действовавшие самостоятельно: «Кибер-армия Халифата», «Армия Сыновей Халифата», «Призраки Халифата» и «Команда электронной безопасности Калашникова».

В июне 2016 г. в Telegram был распространен список с личными данными более 4600 человек. Список сопровождался инструкцией: «Волки Исламского государства, список “смерти” очень важен. Убейте их немедленно. Кибер-армия Халифата, Объединенный кибер-халифат, Исламское государство»[7].

---

[1] Кибератаки – непреднамеренный или несанкционированный доступ, использование, манипулирование, прерывание или уничтожение с помощью электронных устройств, процессов и инфраструктуры обработки информации.

[2] Под киберпространством понимается область информационной среды, включающая взаимозависимую совокупность информационно-технической инфраструктуры, в том числе информационные и телекоммуникационные сети и компьютерные системы, предназначенные для хранения, обработки, модификации и обмена данными.

[3] См.: *Taylor R.W., Caeti T.J., Loper D.K. et al.* Digital Crime and Digital Terrorism. Pearson / Prentice Hall, 2006. P. 20.

[4] См.: *Tesauro L.* The Role Al Qaeda Plays in Cyberterrorism [Электронный ресурс]. – Режим доступа: URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (дата обращения: 25.12.2021).

[5] См.: *Saurabh Ranjan Srivastava and Sachin Dube.* Cyberattacks, Cybercrime and Cyberterrorism // Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications // Information Resources Management Association (USA). 2020. P. 931–963.

[6] См.: *Canetti D., Gross M., Waismel-Manor I. et al.* How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks // Cyberpsychology, Behavior, and Social Networking. 2017. Vol. 20. No. 2. P. 72–77.

[7] “Killing Lists” – The Evolution of Cyber Terrorism? [Электронный ресурс]. – Режим доступа: URL: https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism#gsc.tab=0 (дата обращения: 25.12.2021).

Наиболее известными хакерскими группами, аффилированными с МТО «Аль-Каида», являются: «Альянс Аль-Каиды Онлайн» (ответвление хакерской группы "GForce Pakistan", которая 17 октября 2001 г. нарушила функционирование веб-сервера Национального управления океанических и атмосферных исследований (NOAA)) и «Электронная Аль-Каида» (хакерская группа, которая специализируется на DDoS-атаках и похищениях данных)[8].

Следует отметить, что многие кибератаки, организованные структурами Аль-Каиды, оказались нерезультативными (в их числе DDoS-атака на веб-сайт Ватикана, кибератаки на финансовые учреждения США, фондовую биржу и системы SCADA, а также попытка провести DDoS-атаки 11 ноября 2017 г.).

Как справедливо отмечает бывший аналитик ЦРУ, в настоящее время директор Инициативы Атлантического совета по стратегическому прогнозированию Мэтью Берроуз, кибертерроризм несет в себе важную символическую функцию: он позволяет террористам наносить урон инфраструктуре, которую они считают символом ненавистной им западной цивилизации[9].

О масштабах и остроте угроз кибертерроризма свидетельствуют и социологические исследования. Так, согласно данным опроса Института Гэллапа, 82% респондентов рассматривают кибертерроризм как главную угрозу[10].

Несмотря на то что самому термину «кибертерроризм» уже более 40 лет[11], среди ученых, политиков и практиков нет единого мнения относительно того, что представляет собой кибертерроризм. Сформировалось два основных подхода к трактовке кибертерроризма.

Сторонники «узкого» понимания кибертерроризма рассматривают его как политически или идеологически мотивированное посягательство на информационные системы и использование IT-технологий с целью устрашения органов власти и населения или нанесения ущерба жизненно важным объектам инфраструктуры[12].

Так, Уилсон под кибертерроризмом понимает политически мотивированное использование компьютеров в качестве оружия (или целей) субнациональными группами или тайными агентами, стремящимися повлиять на аудиторию или заставить правительство изменить свою политику[13].

Сулейман Озерен полагает, что кибертерроризм можно просто определить как принуждение других к политическим действиям с использованием компьютерных ресурсов в киберпространстве[14].

В.А. Голубев под кибертерроризмом понимает преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта[15]. Ю.В. Гаврилов и Л.В. Смирнов в качестве кибертерроризма рассматривают оказание противоправного воздействия на информационные системы, совершенное в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности[16].

Эксперты НАТО определяют кибертерроризм как «кибератаку с использованием компьютера или коммуникационных сетей с целью вызвать разрушения, страх или запугать общество ради достижения собственных идеологических целей»[17].

---

[8] См.: *Holt T.J., Bossler A.M., Seigfried-Spellar K.C.* Cybercrime and digital forensics. NY, 2017.

[9] См.: *Charlton C.* Armchar warriors. Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem [Электронный ресурс]. – Режим доступа: URL: https://www.thesun.co.uk/news/2643688/cyber-terrorism-attacks-threat-level-isis-facebook-energy (дата обращения: 25.12.2021).

[10] См.: *Choi J.* 8 in 10 say cyberterrorism is top potential threat: Gallup [Электронный ресурс]. – Режим доступа: URL: https://thehill.com/policy/cybersecurity/544274-8-in-10-say-cyberterrorism-is-top-potential-threat-gallup (дата обращения: 25.12.2021).

[11] В 1980-х годах Барри К. Коллин, старший научный сотрудник Института безопасности и разведки в Калифорнии, впервые ввел в научный оборот словосочетание "cyber terror" («кибертеррор»), определив его как «конвергенцию кибернетики и терроризма».

[12] См.: *Fowler M.* Cyber terrorism: Sci-Fi fantasy or legitimate threat? [Электронный ресурс]. – Режим доступа: URL: https://thehill.com/opinion/cybersecurity/578868-cyber-terrorism-sci-fi-fantasy-or-legitimate-threat (дата обращения: 24.12.2021); *Саркисян А.Ж.* Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий // Росс. следователь. 2019. № 3. С. 54–59.

[13] См.: *Wilson C.* Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report RJ32114 (Washington, D.C.: Library of Congress, Congressional Research Service, 17 October 2003). P. 4.

[14] См.: *Ozeren S.* Global Response to Cyberterrorism and Cybercrime: a Matrix for International Cooperation and Vulnerability Assessment: Dissertation Prepared for the Degree of Doctor of Philosophy. University of North Texas, 2005. P. 7.

[15] См.: *Голубев В.А.* Кибертерроризм – угроза национальной безопасности [Электронный ресурс]. URL: www.crime-research.ru

[16] См.: *Гаврилов Ю.В., Смирнов Л.В.* Современный терроризм: сущность, типология, проблемы противодействия. М., 2003.

[17] Responses to Cyber Terrorism / NATO Science for Peace and Security Series / Centre of Excellence Defence Against Terrorism, Ankara, Turkey. 2008.

Последователи «широкого» определения кибертерроризма указывают, что кибертерроризмом может считаться любое использование террористами интернет-технологий, любая форма онлайн-активности в киберпространстве, способная причинить вред или нести угрозу его причинения.

Так, В.А. Васенин под кибертерроризмом понимает совокупность противоправных действий, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач[18].

Широкое толкование понятия «кибертерроризм» дает Национальная конференция законодательных собраний штатов США (NCSL). Под кибертерроризмом NCSL понимает использование информационных технологий террористическими группами и отдельными лицами для достижения своих целей[19].

По мнению криминолога Марджи Бритц, кибертерроризм – это «преднамеренное, методологическое, идеологически мотивированное распространение информации, облегчение коммуникации или атака на физические цели, цифровую информацию, компьютерные системы и / или компьютерные программы, которые предназначены для нанесения социального, финансового, физического или психологического вреда невоюющим объектам и аудиториям с целью воздействия на идеологические, политические или социальные изменения; или любое использование цифровой связи или информации, которая облегчает такие действия прямо или косвенно»[20].

Следует отметить, что большинство исследователей и экспертов-аналитиков в сфере безопасности придерживаются «узкого» понимания кибертерроризма[21].

«Широкое» понимание кибертерроризма, как правило, связано с ошибочным отождествлением кибертерроризма с другими видами террористической и преступной деятельности.

Так, сбор средств с использованием сети Интернет является самостоятельным видом терроризма – финансированием террористической деятельности.

Распространение с помощью информационно-коммуникационных сетей и интернет-мессенджеров направленной информации с целью формирования сочувствия террористам и их идеям, дальнейшего вовлечения в террористическую деятельность представляет собой пропаганду терроризма.

Использование информационных сетей и компьютерных технологий для планирования и координации террористической деятельности выступает элементом организации любой современной террористической деятельности.

Все эти признаки составов квалифицируются как преступления, не имеющие специфической киберокраски.

Такой же методологической ошибкой является механическое перенесение определения «терроризм» на любую противоправную деятельность в киберпространстве, так как оно не позволяет провести грань между кибертерроризмом и хактивизмом. В то же время возникает отождествление понятия киберпреступности и кибертерроризма.

Отличительным признаком кибертерроризма служит политический или идеологический мотив. При наличии экономической, корыстной мотивации кибератака квалифицируется как общеуголовное преступление.

Неверно относить к кибертерроризму размещение в Сети любой устрашающей население информации.

Любой шок-контент носит устрашающий характер. При этом он чаще всего никак не связан с терроризмом. Террористическая пропаганда также не является кибертерроризмом, поскольку отсутствуют посягательства на критически важные и потенциально опасные объекты инфраструктуры и информационные сети. Пропаганда терроризма направлена на рекрутирование и вербовку новых сторонников, на расширение социальной базы и спонсорской поддержки терроризма.

По этой же причине искажение объективной информации, распространение фейков в целях воздействия на принятие решения органами власти или международными организациями является пропагандой, а не кибертерроризмом.

Не может рассматриваться как кибертерроризм раскрытие информации ограниченного доступа с персональными данными военнослужащих или сотрудников правоохранительных органов, а также призывами нападения на них. Данные деяния образуют совокупность составов преступлений, предусмотренных ст. 137 «Нарушение

---

[18] См.: *Васенин В.А.* Информационная безопасность и компьютерный терроризм [Электронный ресурс]. URL: www.crime-research.ru

[19] См.: Cyberterrorism / National Conference of State Legislatures [Электронный ресурс]. – Режим доступа: URL: http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm (дата обращения: 12.04.2022).

[20] *Holt T.J., Bossler A.M., Seigfried-Spellar K.C.* Op. cit.

[21] Узкий подход к кибертерроризму закреплен в разделе 3.11 Национальной стратегии кибербезопасности Великобритании 2016–2021 гг.

неприкосновенности частной жизни» и ч. 2 ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» УК РФ.

Атаки кибертеррористов нацелены на вывод из строя критически важных и потенциально опасных объектов инфраструктуры, автоматизированных систем управления и информационных сетей или создание условий для техногенных аварий и катастроф.

В первую очередь речь идет о посягательствах на объекты здравоохранения, транспорта, связи, кредитно-финансовую систему, топливно-энергетический комплекс, ядерно опасные объекты, объекты оборонно-промышленного комплекса, ракетно-космическую промышленность, горнодобывающую промышленность, металлургию, химическую промышленность.

Первая известная компьютерная атака на систему промышленной автоматизации произошла в 1982 г. Это была атака на советский газопровод в Сибири. В результате вмешательства произошел взрыв мощностью до 3 кт. Был причинен значительный ущерб газотранспортной системе.

В 1993 г. террористы в Литве угрожали взорвать Игналинскую АЭС с помощью «трояна».

В 2010 г. вирусом Stuxnet были заражены ядерные объекты Ирана.

В результате кибератаки 23 декабря 2015 г. на украинские электрораспределительные предприятия «Прикарпатьеоблэнерго» и «Киевоблэнерго» была нарушена работа более 50 подстанций в распределительных сетях. Без электричества осталось более 220 тыс. жителей. Атака была осуществлена с использованием вредоносной программы BlackEnergy3.

В 2016 г. совершена кибератака на атомную станцию Gundremmingen в Германии. Для заражения промышленного сегмента использовалось «классическое» вредоносное программное обеспечение. Преступниками была заражена система визуализации загрузки топливных радиоактивных элементов станции. Критические элементы объекта не пострадали.

В 2017 г. произошла целевая атака на энергетический комплекс США (Wolf Creek Generating Station). Использовались вредоносное программное обеспечение, «фишинг», «watering-hole-атаки».

В феврале 2021 г. проведена атака хакеров на станцию очистки воды в г. Олдсмаре (США, штат Флорида), в ходе которой предпринята попытка повысить концентрацию гидроксида натрия в воде более чем в 100 раз, что чуть не привело к отравлению водоснабжения целого города.

На примере описанных актов кибертерроризма видно, что террористические кибератаки долгое время не являлись распространенными. Значительно больший общественный резонанс и ответную реакцию властей вызывали действия хакеров-вымогателей. Так, только в 2020 г. в ответ на действия подобных группировок 40 штатов США приняли более 280 законопроектов и резолюций, связанных с кибербезопасностью[22], а после кибератак, совершенных в 2021 г. на Colonial Pipeline и SolarWinds, ведущие производители программного обеспечения и органы правопорядка образовали международную группу по защите от интернет-вымогательства – *Ransomware Task Force*, в которую вошли компании Microsoft и Amazon, а также ФБР и Британское агентство по борьбе с организованной преступностью.

Вместе с тем отмечается заметная активизация актов кибертерроризма недружественных России государств в связи с проведением специальной военной операции на Украине.

Кроме того, «кибервойну» Российской Федерации объявил ряд хакерских группировок, включая Anonymous, а масштабным кибератакам регулярно подвергаются российские интернет-провайдеры и правительственные сайты, в том числе Роскомнадзора, Пенсионного фонда России, Федеральной антимонопольной службы и информационные ресурсы Крыма, а также крупные российские компании: «Газпром», «Лукойл», «Норникель» и «Яндекс».

Определять сущность кибертерроризма и разрабатывать его формулировку следует, прежде всего отталкиваясь от его характерных черт. К числу таковых можно отнести: 1) политический или идеологический мотив; 2) желание создать атмосферу страха в обществе; 3) наличие действий, создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступлении иных тяжких последствий (или угроза совершения таких действий) для отраслевой или национальной экономики, правопорядка, обороноспособности и безопасности государства, его внешне- и внутриполитическим интересам; 4) использование информационно-телекоммуникационных технологий.

Основной целью кибертеррористов выступает вывод из строя информационно-технологической части инфраструктуры или применение данной инфраструктуры для создания условий, которые могут привести к техногенным авариям и катастрофам, а также устрашению населения.

[22] См.: *Keren L.G. Snider, Ryan Shandler, Shay Zandani, Daphna Canetti.* Cyberattacks, cyber threats, and attitudestoward cybersecurity policies // Journal of Cybersecurity. 2021. Vol. 7. Issue 1.

Важной отличительной характеристикой кибертерроризма в сравнении с традиционным терроризмом является цифровой аспект кибертерроризма.

Динамика и масштабы кибертерроризма зависят от уровня развития информационно-телекоммуникационной инфраструктуры.

Криминологическая характеристика кибертерроризма связана с его особенностями.

Акты кибертерроризма носят трансграничный характер. Преступник может находиться в одной стране, совершать преступление в другой, наносить вред третьему государству. При этом зараженные сети могут охватывать тысячи компьютеров, находящихся в десятках стран.

Кибератаки могут затрагивать различные значимые для государства объекты и наносить значительный вред экономической безопасности, правопорядку, обороноспособности и безопасности государства.

В отличие от традиционных терактов кибератаки не требуют приобретения оружия и взрывчатых веществ. Наиболее распространенными способами кибертеррористической деятельности выступают дефейс сайтов, DDoS-атаки, распространение вирусов и программируемых криптов.

Кибератаки можно проводить удаленно и относительно анонимно.

Себестоимость кибератак позволяет рассматривать их как сравнительно недорогое и эффективное средство террористической деятельности.

Кибертерроризм может осуществляться путем как самостоятельных действий квалифицированных террористов-одиночек и технически подготовленных групп, так и вербовки и использования хакеров или сотрудников критически важных и потенциально опасных объектов (т.н. внутренние нарушители). Наиболее опасными и подготовленными являются акты государственного кибертерроризма, которые планируются, осуществляются, спонсируются и курируются недружественными государствами (спецслужбами и используемыми ими организациями).

Разнообразие организационных форм, программных средств и задействованной в кибератаках инфраструктуры позволяет вести речь о классификации кибертерроризма.

Эксперты различают несколько видов (типов) кибертерроризма: простой, структурированный и комплексный.

Для простого типа кибертерроризма характерны взломы отдельных систем, использование чужих программ и одиночный характер деятельности террориста.

Структурированный кибертерроризм сочетает атаки нескольких систем, создание собственных программ и наличие группы лиц с разделением ролей.

Комплексному кибертерроризму присущи массовые скоординированные атаки, способность к преодолению разнородных средств защиты, а также высокий уровень организации кибертеррористической деятельности (планирование, координация, контроль, обучение).

Как отмечалось, субъектами кибертерроризма могут выступать отдельные террористы, группы граждан с разделением ролей, террористические организации, спецслужбы и используемые ими организации недружественных государств.

Только спецслужбы и курируемые ими организации способны обеспечить высокий уровень организации и широкомасштабный характер кибертеррористической деятельности. Яркими примерами государственного кибертерроризма можно считать кибератаки спецслужб США на объекты критической информационной инфраструктуры Российской Федерации в марте 2021 г. под предлогом реагирования на «российские хакерские атаки» или кибероперации Украины и государств – участников НАТО в период проведения специальной военной операции на территории Украины.

Объектом кибертерроризма является общественная безопасность. Рассмотрение в качестве объекта преступления компьютерных систем необоснованно заужает сферу правового регулирования и уголовно-правового воздействия.

В широком смысле предметом кибертерроризма является информационная инфраструктура, в узком смысле – информация; объекты информатизации; информационные системы; сайты / аккаунты; сети связи; информационные технологии; деятельность по формированию и обработке информации, развитию и использованию информационных технологий, обеспечению информационной безопасности.

С объективной стороны кибертерроризм характеризуется: несанкционированным доступом; уничтожением информации, программ, ресурсов; созданием ботнетов; разрушением сетей и аппаратных средств; перезагрузкой узлов коммуникаций.

Представляется, что признаки объективной стороны кибертерроризма должны отвечать двум условиям: 1) связь с нанесением ущерба критически важным и потенциально опасным объектам, объектам обеспечения жизнедеятельности населения; 2) создание опасности причинения значительного вреда жизни, здоровью или имуществу неопределенного круга лиц, отраслевой или национальной экономике, правопорядку, обороноспособности

и безопасности государства, внешне- и внутриполитическим интересам государства.

За основу оценки возможного ущерба можно взять определенные ст. 7 Федерального закона от 12 июля 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»[23] критерии: социальную значимость (возможность причинения вреда жизни или здоровью людей, прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, прекращения доступа к государственной услуге для ее получателей); политическую значимость (возможность причинения ущерба интересам государства в вопросах внутренней и внешней политики); экономическую значимость (возможность причинения прямого или косвенного ущерба субъектам критической информационной инфраструктуры и (или) государственному бюджету); экологическую значимость (возможность неблагоприятного воздействия на окружающую среду); значимость объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка).

С субъективной стороны акты кибертерроризма совершаются умышленно. Не может деликтоспособный субъект неосознанно удалять, изменять, повреждать, блокировать, перехватывать данные информационных систем, создавать зараженную сеть, причинять вред критически важному или потенциально опасному объекту и при этом не предвидеть возможность наступления общественно опасных последствий своих действий.

Рассматривая акты кибертерроризма, необходимо затронуть вопросы квалификации данного преступления.

Для эффективного применения уголовного законодательства в целях противодействия кибертерроризму необходима его четкая квалификация – установление точного соответствия между признаками совершенного деяния и признаками состава преступления, предусмотренного уголовно-правовой нормой.

Как справедливо отмечает В.П. Кашепов, «правильная и точная квалификация преступлений: обеспечивает соблюдение законности при осуществлении правосудия; выражает социально-политическую и юридическую оценку совершенного деяния; гарантирует права и законные интересы обвиняемого, способствуя индивидуализации уголовной ответственности; предопределяет законное и обоснованное применение институтов и норм Общей части уголовного законодательства, регламентирующего освобождение от уголовной ответственности и наказания, погашение судимости; обусловливает процессуальный порядок расследования преступлений; позволяет правильно охарактеризовать состояние, структуру и динамику преступности и выработать эффективные меры борьбы с ней»[24].

Квалификация кибертерроризма как классического компьютерного преступления является некорректной и значительно снижает как степень общественной опасности, так и возможный размер наказания. Так, максимальная санкция по ст. 274^1 УК РФ предусматривает до десяти лет лишения свободы, по ст. 272, 273 УК РФ – до семи лет, а по ст. 274 УК РФ – до пяти лет лишения свободы. При этом максимальное наказание по ч. 3 ст. 205 УК РФ составляет до двадцати лет лишения свободы или пожизненное лишение свободы.

В юридической литературе вопросы квалификации кибертерроризма предлагается рассматривать в виде двух вариантов:

введение квалифицирующего состава в конструкцию ст. 205 УК РФ (теракт: с использованием информационных сетей; с использованием вредоносных программ; с получением неправомерного доступа к компьютерной информации конфиденциального характера либо к сведениям, содержащим государственную тайну)[25];

внесение изменений в ст. 272–274^1 УК РФ[26].

Представляется, что правильнее было бы введение самостоятельного состава «Акт кибертерроризма» в Уголовный кодекс РФ или дополнение ст. 205 «Террористический акт» УК РФ особым квалифицированным составом. Как уже отмечалось, вариант с изменением составов компьютерных преступлений не соответствует степени тяжести кибертерроризма и мерам наказания.

На практике встречаются факты совершения преступлений кибертеррористического характера лицами, признанными невменяемыми или не достигшими возраста уголовной ответственности. Данные обстоятельства не влияют на общественную опасность и противоправность совершенных деяний. Вместе с тем установленные в этих случаях правоохранительными органами лица субъектами

[23] См.: СЗ РФ. 2017. № 31 (ч. I), ст. 4736.

[24] *Кашепов В.П.* Переквалификация преступных деяний при изменении уголовного закона // Журнал росс. права. 2014. № 4. С. 8.

[25] См.: *Чекунов И.Г.* Киберпреступность: понятие и классификация // Росс. следователь. 2012. № 2. С. 37–44; *Соломатина Е.С.* Перспективы развития законодательства в сфере борьбы с кибертерроризмом // Закон и право. 2009. № 1. С. 47, 48.

[26] См.: *Капитонова Е.А.* Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2. С. 29–44.

преступлений не являются и уголовной ответственности не подлежат.

Можно предположить ситуацию, когда хакер или специалист IT-подразделения критически важного объекта под воздействием побоев, истязаний, незаконного лишения свободы или угроз применения насилия совершает акт кибертерроризма.

Преступность или непреступность подобного деяния зависит от того, сохраняло ли такое лицо способность руководить своими действиями. Если оно было незаконно лишено свободы, не имело возможности воспользоваться средствами связи, находилось под постоянным наблюдением террористов, обстоятельства позволяют рассматривать эту ситуацию как неспособность руководить своими действиями.

Если лицо сохраняло возможность руководить своими действиями (могло связаться с правоохранительными органами, проинформировать руководство объекта инфраструктуры о подготовке террористической атаки, предупредить коллег для принятия мер или др. способами избежать опасности), деяние будет считаться непреступным, только если физическое или психическое принуждение создавало состояние крайней необходимости и не были превышены ее пределы. Сложно предположить такую вероятность даже в теории.

Можно привести следующий пример. Для того чтобы избежать побоев или угрозы причинения вреда здоровью, лицо, по указанию группы террористов, осуществило несанкционированный доступ к информационным системам военного госпиталя, отключило автоматизированные системы управления медицинским оборудованием операционных, а также систему хранения донорской крови, что привело к гибели нескольких военнослужащих в операционных, порче донорской крови и ее компонентов. Очевидно, что причиненный вред гораздо значительней, чем вред предотвращенный. Думается, что физическое или психическое принуждение при сохранении возможности руководить действиями (волевой момент) можно рассматривать только как смягчающее обстоятельство.

Учитывая тяжесть состава кибертерроризма, в соответствии с ч. 2 ст. 75 УК РФ возможные основания освобождения от уголовной ответственности должны быть специально предусмотрены в соответствующей статье Особенной части УК РФ. Принимая во внимание террористический характер акта кибертерроризма, в ст. 78 УК РФ необходимо закрепить неприменение сроков давности по данному составу преступления.

В качестве смягчающего наказание обстоятельства также можно рассматривать явку с повинной, активное способствование раскрытию и расследованию преступления, изобличению и уголовному преследованию других соучастников акта кибертерроризма.

Значительный интерес представляют вопросы противодействия кибертерроризму, которые можно рассмотреть на примере национальных моделей противодействия кибертерроризму в США, Великобритании, Канаде, ФРГ, Франции, Индии, КНР и Российской Федерации.

Первая развитая система противодействия кибертерроризму сформировалась в США.

В конце 1990-х годов основными полномочиями в области кибербезопасности[27] было наделено ФБР, которое в тот период осуществляло противодействие киберугрозам криминального характера. После террористической атаки 11 сентября 2001 г. вопросы кибербезопасности стали рассматриваться сквозь призму борьбы с терроризмом. Основным приоритетом стала защита критически важных объектов инфраструктуры.

В 2002 г. в ФБР создан киберотдел, в 2003 г. учреждено Агентство по кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности США.

В 2003 г. опубликована Национальная стратегия кибербезопасности, в которой сделан акцент на превентивные действия, что потребовало усиления полномочий спецслужб и совершенствования государственного контроля информационной сферы.

Завершающим этапом формирования централизованной системы противодействия кибертерроризму стало создание в 2009 г. Киберкомандования США (USCYBERCOM). После создания киберкомандования ответственность за безопасность гражданской информационно-телекоммуникационной инфраструктуры была возложена на Министерство внутренней безопасности, а вопросы защиты военных информационных сетей переданы Киберкомандованию[28].

В 2011 г. утверждена Стратегия Министерства обороны США по действиям в киберпространстве[29]. Киберпространство стало официально рас-

[27] В рекомендации Международного союза Электросвязи X.1205 МСЭТ кибербезопасность определена как «набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя».

[28] См.: *Шариков П.А.* Эволюция американской политики кибербезопасности // Мировая экономика и международные отношения. 2019. Т. 63. № 10. С. 51–58.

[29] См.: Department of Defence. Strategy for Operating in Cyberspace. Washington. DC.US Department of Defence. 2011.

сматриваться как самостоятельный театр военных действий, а кибератаки приравнены к виду боевых действий.

В 2017 г. принят исполнительный указ Президента США «Об укреплении кибербезопасности федеральных сетей и критической инфраструктуры», который стал правовой и методической основой для развития подразделений кибербезопасности федеральных структур исполнительной власти Соединенных Штатов Америки.

В сентябре 2018 г. опубликована Национальная киберстратегия США. В документе заявлено, что «США вовлечены в продолжительное соперничество со стратегическими противниками, несостоявшимися государствами, террористами и криминальными сетями, которые развивают новые и эффективные кибервооружения»[30]. Провозглашена цель использовать наступательный киберпотенциал в интересах национальной безопасности.

В декабре 2020 г. в США принят Закон о кибербезопасности Интернета ("Internet of Things Cybersecurity Improvement Act"), который устанавливает требования к безопасности для оборудования сети Интернет, приобретаемого федеральным правительством. Кроме того, начиная с 2021 г. федеральное правительство значительно усилило взаимодействие с частным сектором в вопросах выявления киберугроз и обеспечения кибербезопасности США[31].

Традиционно схожий подход в США к обеспечению кибербезопасности и противодействию кибертерроризму заложен в британской модели.

В 2011 г. в Великобритании была разработана первая пятилетняя Национальная стратегия кибербезопасности, одним из направлений реализации которой определено противодействие кибертерроризму. Первоначально система противодействия кибертерроризму носила децентрализованный характер и включала Центр защиты национальной инфраструктуры (CPNI), Группу быстрого реагирования на инциденты в области компьютерной безопасности (CERT-UK) и Центр оценки киберугроз (CCA).

В Национальной стратегии кибербезопасности 2016–2021 гг. закрепили смешанную, государственно-коммерческую модель противодействия кибертерроризму. Головной координирующей и методической структурой стал Национальный центр кибербезопасности (NCSC) (учрежден в 2016 г.). Для защиты от кибератак в Вооруженных силах создан Военный центр операций по кибербезопасности.

Канадская модель строится на Стратегии создания безопасного киберпространства для всех канадцев. Ключевым органом является Центр реагирования на киберинциденты, который ведет мониторинг и оказывает консультативную помощь субъектам критической инфраструктуры в обнаружении, предупреждении и пресечении киберугроз. Информационно-пропагандистскую деятельность о потенциальных рисках и мерах безопасности в киберпространстве (программа Get Cyber Safe) осуществляет Служба общественной безопасности Канады[32].

В ФРГ центральная роль в обеспечении кибербезопасности и противодействии кибертерроризму отведена Министерству внутренних дел. При МВД действует Национальный ситуационный центр кибербезопасности, Национальный центр киберзащиты Германии, Центр по борьбе с киберпреступностью федеральной полиции.

Для проведения военных кибероперациий в бундесвере организованы киберкомандование Вооруженных сил ФРГ, группы по реагированию на инциденты в сфере кибербезопасности, отделы киберзащиты.

В 2021 г. принята Стратегия кибербезопасности Германии на 2021–2026 гг. Предусмотрено усиление кибербезопасности органов государственной власти, критической инфраструктуры и экономики, компаний малого и среднего бизнеса и граждан. В Стратегии закреплены новые полномочия государственных органов, в том числе возможность доступа следственных органов к результатам мониторинга телекоммуникационных сетей, проведения онлайн-обысков, расширены полномочия по взаимодействию полиции с подразделениями киберзащиты при расследовании киберпреступлений.

На федеральном, региональном и муниципальном уровнях реализуются совместные проекты в сфере кибербезопасности.

В отличие от англосаксонских стран Франция не считает кибербезопасность и противодействие кибертерроризму прерогативой спецслужб.

В 2009 г. было создано Национальное агентство безопасности информационных систем (ANSSI). Данный орган, находящийся в прямом подчинении премьер-министра Франции, отвечает за безопасность национальных информационных систем, а также координацию деятельности по

[30] National Cyber Strategy of the United States of America. Sept. 2018 [Электронный ресурс]. – Режим доступа: URL: www.whitehouse.gov/the-press-office/2017/08/18/statement-donald-j-trump-elevation-cyber-command (дата обращения: 14.05.2022).

[31] См.: Executive Order on Improving the Nation's Cybersecurity [Электронный ресурс]. – Режим доступа: URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (дата обращения: 14.05.2022).

[32] См.: *Гришин С.Е.* Формирование культуры кибербезопасности в обществе – актуальная задача современности // Вестник Саратовского гос. соц.-экон. ун-та. 2011. № 4. С. 170–173.

обеспечению кибербезопасности как в государственном, так и в частном секторе.

В 2011 г. в качестве реакции на серию кибератак на Минфин Франции была разработана первая национальная киберстратегия «Оборона и безопасность информационных систем: Стратегия Франции». Основные идеи данного документа получили развитие в Национальной стратегии цифровой безопасности Франции 2015 г. и Стратегическом обзоре по кибероборонe 2018 г.

Французский законодатель дифференцирует подходы к оборонительным и наступательным кибероперациям. При этом Франция, как и США, оставляет за собой право использования наступательных кибероперациий и в качестве самостоятельного инструмента, и в поддержку действий Вооруженных сил Французской Республики[33].

Национальные органы в сфере кибербезопасности и противодействия кибертерроризму взаимодействуют с уполномоченными структурами ЕС – Европейским центром по борьбе с киберпреступностью и Европейским агентством по безопасности сети и информации.

Помимо этого, государства Европы периодически проводят совместные мероприятия в сети Интернет, направленные на блокирование ресурсов террористических структур. Так, 21 ноября 2019 г. под эгидой Европола прошел День борьбы с террористической онлайн-пропагандой ИГИЛ, в рамках которого девять интернет-компаний, считающихся лидерами в своих областях, в том числе Google, Telegram, Twitter, Instagram, осуществили при координирующей роли европейского полицейского агентства одно из самых масштабных за историю функционирования сети Интернет удалений страниц, использовавшихся сторонниками террористических и экстремистских структур[34].

В Индии разработка программных документов в сфере кибербезопасности началась в 2013 г. после разоблачений Э. Сноудена. Департаментом электроники и информационных технологий была подготовлена Национальная политика в области кибербезопасности. В спецслужбах Индии, включая аппарат советника по безопасности, внешнюю разведку, военную разведку, контрразведку и МВД, были сформированы подразделения, занимающиеся кибероперациями.

В 2018 г. учреждено Оборонное киберагентство (Defence Cyber Agency), которое по своему функционалу является киберкомандованием[35].

В КНР большое влияние на государственную политику в сфере кибербезопасности и противодействия кибертерроризму оказывает Коммунистическая партия Китая (КПК). Координирующую роль играет Центральный комитет по кибербезопасности и информатизации КПК.

Китайская система кибербезопасности и противодействия кибертерроризму охватывает не только техническую безопасность, но и необъемлющий контроль национальной информационной инфраструктуры. Для защиты информационных систем от кибератак и вирусов эффективно применяется «Золотой щит» – система фильтрации интернет-контента.

Российская система противодействия кибертерроризму возникла в 2013 г. Указом Президента РФ была образована Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы ГосСОПКА[36].

Задачами ГосСОПКА были определены: прогнозирование ситуации в области обеспечения информационной безопасности; обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, других субъектов, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак; установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Обеспечение и контроль функционирования ГосСОПКА осуществляет ФСБ России. Для обеспечения координации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты создан Национальный координационный центр по компьютерным инцидентам.

В 2017 г. принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической

[33] См.: *Чихачев А.* Франция: киберреспублика на марше. URL: http://russiancouncil.ru/analytics-and-comments/analytics/frantsiya-kiberrespublika-na-marshe

[34] См.: Referral Action Day Against Islamic State Online Terrorist Propaganda, Europol, 22 November 2019 [Электронный ресурс]. – Режим доступа: URL: https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda (дата обращения: 14.05.2022).

[35] См.: *Куприянов А.* Индия в эпоху кибервойн. URL: http://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn

[36] См.: Указ Президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СЗ РФ. 2013. № 3, ст. 178; Указ Президента РФ от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СЗ РФ. 2017. № 52 (ч. I), ст. 8112.

информационной инфраструктуры Российской Федерации»[37].

В указанном Федеральном законе определены силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, определены значимые объекты критической информационной инфраструктуры и требования по обеспечению их безопасности, закреплены права и обязанности субъектов критической информационной инфраструктуры, порядок категорирования, оценки и государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Российская система противодействия кибертерроризму помимо специализированных государственных и координирующих органов включает известные компании, занимающие лидирующие позиции в рассматриваемой сфере («Лаборатория Касперского», «Информзащита», «Инфосистемы Джет», «Ростелеком-Солар», “Positive Technologies”, “Group-IB” и др.).

Анализ национальных киберстратегий позволяет выделить кибертерроризм в качестве самостоятельного элемента киберпреступности, фокусирует внимание на важной роли кибербезопасности в системе доктринальных документов, регламентирующих вопросы национальной безопасности, подчеркивает сходство основных направлений обеспечения кибербезопасности и противодействия кибертерроризму.

Выводы

Кибертерроризм представляет собой новый вид террористической деятельности, связанный с политически мотивированным деструктивным воздействием на информационные системы, автоматизированные системы управления и информационные сети для нанесения ущерба объектам жизнедеятельности населения, отраслевой или национальной экономике, правопорядку, обороноспособности и безопасности государства, внешне- и внутриполитическим интересам государства.

Кибертерроризм может осуществляться как путем самостоятельных действий террористов-одиночек и отдельных групп, так и путем вербовки и целевого использования хакеров или сотрудников критически важных и потенциально опасных объектов. Наиболее опасными являются акты государственного кибертерроризма, которые курируются спецслужбами и организациями иностранных государств.

Квалификация актов кибертерроризма как классического компьютерного преступления значительно снижает степень общественной опасности и возможный размер наказания. Актуальным является введение самостоятельного состава «Акт кибертерроризма» в Уголовный кодекс РФ или закрепление дополнительного квалифицирующего состава в конструкции ст. 205 «Террористический акт» УК РФ. Принимая во внимание террористический характер природы кибертерроризма, в ст. 78 УК РФ необходимо закрепить неприменение сроков давности по данному составу.

Сравнительный анализ существующих национальных киберстратегий указывает на ряд общих подходов. Большинство государств понимают кибербезопасность как элемент национальной безопасности. Кибероперации рассматриваются как инструмент борьбы с недружественными государствами и военными противниками. Констатируется значимость национального оборудования и программного обеспечения для полноценной защиты информационной безопасности.

Исходя из зарубежного и российского опыта, можно выделить несколько актуальных направлений противодействия кибертерроризму: анализ киберугроз и компьютерных инцидентов; анализ сведений об уязвимостях программного обеспечения и оборудования; мониторинг защищенности информационных ресурсов; развертывание системы верификации и фильтрации электронных сообщений; организация эшелонированной антивирусной защиты, блокировка вредоносных доменов и IP-адресов; разработка программных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; автоматизированная защита государственных цифровых услуг; обучение сотрудников обнаружению, предупреждению и ликвидации последствий целевых компьютерных атак.

СПИСОК ЛИТЕРАТУРЫ

1. *Васенин В.А.* Информационная безопасность и компьютерный терроризм [Электронный ресурс]. URL: www. crime-research.ru
2. *Гаврилов Ю.В., Смирнов Л.В.* Современный терроризм: сущность, типология, проблемы противодействия. М., 2003.
3. *Голубев В.А.* Кибертерроризм – угроза национальной безопасности [Электронный ресурс]. URL: www.crime-research.ru
4. *Гришин С.Е.* Формирование культуры кибербезопасности в обществе – актуальная задача современности // Вестник Саратовского гос. соц.-экон. ун-та. 2011. № 4. С. 170–173.
5. *Капитонова Е.А.* Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2. С. 29–44.

[37] См.: СЗ РФ. 2017. № 31 (ч. I), ст. 4736.

6. *Кашепов В.П.* Переквалификация преступных деяний при изменении уголовного закона // Журнал росс. права. 2014. № 4. С. 8.

7. *Куприянов А.* Индия в эпоху кибервойн. URL: http://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn

8. *Саркисян А.Ж.* Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий // Росс. следователь. 2019. № 3. С. 54–59.

9. *Соломатина Е.С.* Перспективы развития законодательства в сфере борьбы с кибертерроризмом // Закон и право. 2009. № 1. С. 47, 48.

10. *Чекунов И.Г.* Киберпреступность: понятие и классификация // Росс. следователь. 2012. № 2. С. 37–44.

11. *Чихачев А.* Франция: киберреспублика на марше. URL: http://russiancouncil.ru/analytics-and-comments/analytics/frantsiya-kiberrespublika-na-marshe

12. *Шариков П.А.* Эволюция американской политики кибербезопасности // Мировая экономика и международные отношения. 2019. Т. 63. № 10. С. 51–58.

13. *Canetti D., Gross M., Waismel-Manor I. et al.* How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks // Cyberpsychology, Behavior, and Social Networking. 2017. Vol. 20. No. 2. P. 72–77.

14. *Charlton C.* Armchar warriors. Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem [Электронный ресурс]. – Режим доступа: URL: https://www.thesun.co.uk/news/2643688/cyber-terrorism-attacks-threat-level-isis-facebook-energy (дата обращения: 25.12.2021).

15. *Choi J.* 8 in 10 say cyberterrorism is top potential threat: Gallup [Электронный ресурс]. – Режим доступа: URL: https://thehill.com/policy/cybersecurity/544274-8-in-10-say-cyberterrorism-is-top-potential-threat-gallup (дата обращения: 25.12.2021).

16. Cyberterrorism / National Conference of State Legislatures [Электронный ресурс]. – Режим доступа: URL: http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm (дата обращения: 12.04.2022).

17. *Fowler M.* Cyber terrorism: Sci-Fi fantasy or legitimate threat? [Электронный ресурс]. – Режим доступа: URL: https://thehill.com/opinion/cybersecurity/578868-cyber-terrorism-sci-fi-fantasy-or-legitimate-threat (дата обращения: 24.12.2021).

18. *Holt T.J., Bossler A.M., Seigfried-Spellar K.C.* Cybercrime and digital forensics. NY, 2017.

19. *Keren L.G. Snider, Ryan Shandler, Shay Zandani, Daphna Canetti.* Cyberattacks, cyber threats, and attitudestoward cybersecurity policies // Journal of Cybersecurity. 2021. Vol. 7. Issue 1.

20. "Killing Lists" – The Evolution of Cyber Terrorism? [Электронный ресурс]. – Режим доступа: URL: https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism#gsc.tab=0 (дата обращения: 25.12.2021).

21. *Ozeren S.* Global Response to Cyberterrorism and Cybercrime: a Matrix for International Cooperation and Vulnerability Assessment: Dissertation Prepared for the Degree of Doctor of Philosophy. University of North Texas, 2005. P. 7.

22. Responses to Cyber Terrorism / NATO Science for Peace and Security Series / Centre of Excellence Defence Against Terrorism, Ankara, Turkey. 2008.

23. *Taylor R.W., Caeti T.J., Loper D.K. et al.* Digital Crime and Digital Terrorism. Pearson / Prentice Hall, 2006. P. 20.

24. *Tesauro L.* The Role Al Qaeda Plays in Cyberterrorism [Электронный ресурс]. – Режим доступа: URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (дата обращения: 25.12.2021).

25. *Saurabh Ranjan Srivastava and Sachin Dube.* Cyberattacks, Cybercrime and Cyberterrorism // Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications // Information Resources Management Association (USA). 2020. P. 931–963.

26. *Wilson C.* Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report RJ32114 (Washington, D.C.: Library of Congress, Congressional Research Service, 17 October 2003). P. 4.

REFERENCES

1. *Vasenin V.A.* Information security and computer terrorism [Electronic resource]. URL: www. crime-research.ru (in Russ.).

2. *Gavrilov Yu. V., Smirnov L.V.* Modern terrorism: essence, typology, problems of counteraction. M., 2003 (in Russ.).

3. *Golubev V.A.* Cyberterrorism – a threat to national security [Electronic resource]. URL: www.crime-research.ru (in Russ.).

4. *Grishin S.E.* The formation of a cybersecurity culture in society is an urgent task of our time // Herald of the Saratov State Socio-Economic University. 2011. No. 4. P. 170–173 (in Russ.).

5. *Kapitonova E.A.* Features of cyberterrorism as a new kind of terrorist act // News of higher educational institutions. Volga Region. Social sciences. 2015. No. 2. P. 29–44 (in Russ.).

6. *Kashepov V.P.* Retraining of criminal acts when changing the criminal law // Journal of Russian law. 2014. No. 4. P. 8 (in Russ.).

7. *Kupriyanov A.* India in the era of cyberwar. URL: http://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn (in Russ.).

8. *Sarkisyan A.J.* Criminological characteristics of crimes committed in the field of information and communication technologies // Russ. Investigator. 2019. No. 3. P. 54–59 (in Russ.).

9. *Solomatina E.S.* Prospects for the development of legislation in the field of combating cyberterrorism // Law and Law. 2009. No. 1. P. 47, 48 (in Russ.).

10. *Chekunov I.G.* Cybercrime: concept and classification // Russ. Investigator. 2012. No. 2. P. 37–44 (in Russ.).

11. *Chikhachev A.* France: Cyber Republic on the march. URL: http://russiancouncil.ru/analytics-and-comments/analytics/frantsiya-kiberrespublika-na-marshe (in Russ.).

12. *Sharikov P.A.* Evolution of American cybersecurity policy // World economy and international relations. 2019. Vol. 63. No. 10. P. 51–58 (in Russ.).

13. *Canetti D., Gross M., Waismel-Manor I. et al.* How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks // Cyberpsychology, Behavior, and Social Networking. 2017. Vol. 20. No. 2. P. 72–77.

14. *Charlton C.* Armchar warriors. Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem [Electronic resource]. – Access mode: URL: https://www.thesun.co.uk/news/2643688/cyber-terrorism-attacks-threat-level-isis-facebook-energy (accessed: 25.12.2021).

15. *Choi J.* 8 in 10 say cyberterrorism is top potential threat: Gallup [Electronic resource].– Access mode: URL: https://thehill.com/policy/cybersecurity/544274-8-in-10-say-cyberterrorism-is-top-potential-threat-gallup (accessed: 25.12.2021).

16. Cyberterrorism / National Conference of State Legislatures [Electronic resource]. – Access mode: URL: http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm (accessed: 12.04.2022).

17. *Fowler M.* Cyber terrorism: Sci-Fi fantasy or legitimate threat? [Electronic resource]. – Access mode: URL: https://thehill.com/opinion/cybersecurity/578868-cyber-terrorism-sci-fi-fantasy-or-legitimate-threat (accessed: 24.12.2021).

18. *Holt T.J., Bossler A.M., Seigfried-Spellar K.C.* Cybercrime and digital forensics. NY, 2017.

19. *Keren L.G. Snider, Ryan Shandler, Shay Zandani, Daphna Canetti.* Cyberattacks, cyber threats, and attitudestoward cybersecurity policies // Journal of Cybersecurity. 2021. Vol. 7. Issue 1.

20. "Killing Lists" – The Evolution of Cyber Terrorism? [Electronic resource]. – Access mode: URL: https://www.ict.org.il/Article/1793/killing-lists-the-evolution-of-cyber-terrorism#gsc.tab=0 (accessed: 25.12.2021).

21. *Ozeren S.* Global Response to Cyberterrorism and Cybercrime: A Matrix for International Cooperation and Vulnerability Assessment: Dissertation Prepared for the Degree of Doctor of Philosophy. University of North Texas, 2005. P. 7.

22. Responses to Cyber Terrorism / NATO Science for Peace and Security Series / Centre of Excellence Defence Against Terrorism, Ankara, Turkey. 2008.

23. *Taylor R.W., Caeti T.J., Loper D.K. et al.* Digital Crime and Digital Terrorism. Pearson / Prentice Hall, 2006. P. 20.

24. *Tesauro L.* The Role Al Qaeda Plays in Cyberterrorism [Electronic resource]. – Access mode: URL: https://smallwarsjournal.com/jrnl/art/role-al-qaeda-plays-cyberterrorism (accessed: 25.12.2021).

25. *Saurabh Ranjan Srivastava and Sachin Dube.* Cyberattacks, Cybercrime and Cyberterrorism // Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications // Information Resources Management Association (USA). 2020. P. 931–963.

26. *Wilson C.* Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress, CRS Report RJ32114 (Washington, D.C.: Library of Congress, Congressional Research Service, 17 October 2003). P. 4.

Сведения об авторах

КРАСИНСКИЙ Владислав Вячеславович –
доктор юридических наук, заместитель начальника управления противодействия экстремизму и терроризму Главного управления региональной безопасности Московской области; 143407 Московская область, г. Красногорск, бульвар Строителей, д. 1

МАШКО Владислав Валерьевич –
кандидат исторических наук, доцент кафедры международной безопасности Российского государственного гуманитарного университета; 125993 г. Москва, Миусская площадь, д. 6

Author's information

KRASINSKY Vladislav V. –
Doctor of Law, Associate Professor, Deputy Head of the Department of Counteraction to Extremism and Terrorism of the Main Department of Regional Security of the Moscow Region; 1 Stroiteley boulevard, 143407 Moscow Region, Krasnogorsk, Russia

MASHKO Vladislav V. –
Candidate of Historical Sciences, Associate Professor of the Department of International Security of the Russian State University for the Humanities; 6 Miusskaya square, 125993, Moscow, Russia