Научная статья
УДК 343.34
https://doi.org/10.36511/2078-5356-2024-1-187-192

Правовое регулирование киберэкстремизма и кибертерроризма: проблемы и перспективы

Мельник Святослав Сергеевич
Московский государственный институт международных отношений (Университет) Министерства иностранных дел Российской Федерации, Москва, Россия, big-benac@yandex.ru, ORCID: 0000-0001-5771-9743

Аннотация. Статья посвящена комплексному анализу кибертерроризма и киберэкстремизма как наиболее опасным социальным явлениям, получившим широкое распространение в связи с развитием информационных технологий, особенно в сфере информационно-коммуникационной сети «Интернет». Автором исследованы теоретические концепции осмысления кибертерроризма как правовой дефиниции, рассмотрены исторические особенности развития этого явления, выявлены различные подходы в правовом регулировании кибертерроризма в Индии, Нигерии и Филиппинах. Предложено собственное определение киберэкстремизма, которое основывается на компиляции конститутивных признаков кибертерроризма (как самостоятельного явления) и экстремизма. Особое внимание уделяется полисистемности правового регулирования борьбы с киберэкстремизмом и кибертерроризмом (универсальный уровень правового регулирования, региональный уровень правового регулирования и национальный). Исследование зарубежного опыта правового регулирования позволило сместить акцент с универсального уровня международно-правового регулирования на региональный, что в существенной степени повлияет на региональную структуру безопасности. В ходе исследования сделан вывод, что наиболее перспективным направлением регионального сотрудничества в борьбе с киберэкстремизмом для Российской Федерации будет Шанхайская организация сотрудничества (далее — ШОС). Это связано с тем, что ШОС единственная международная организация, которая имеет конвенционное регулирование противодействия экстремизму как таковому. Расширение сотрудничества является целесообразным, поскольку киберэкстремизм представляет собой определенную форму экстремизма, а также с учетом опыта Республики Индия как государства – члена ШОС, которое имеет соответствующее национальное законодательство, направленное на противодействие кибертерроризму.

Ключевые слова: кибертерроризм, киберэкстремизм, киберпреступность, Шанхайская организация сотрудничества, сепаратизм, объекты критической инфраструктуры, кибербезопасность

Для цитирования: Мельник С. С. Правовое регулирование киберэкстремизма и кибертерроризма: проблемы и перспективы // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 1 (65). С. 187–192. https://doi.org/10.36511/2078-5356-2024-1-187-192.

Original article

Legal regulation of cyberextremism and cyberterrorism: challenges and opportunities

Svyatoslav S. Melnik
Moscow State Institute of International Relations (University) Ministry of Foreign Affairs, Moscow, Russian Federation, big-benac@yandex.ru, ORCID: 0000-0001-5771-9743

Abstract. The article is devoted to a comprehensive analysis of cyberterrorism and cyberextremism as the most dangerous social phenomena that have become widespread due to the development of information technologies, especially in the field of the Internet information and telecommunications network. The author investigates the theoretical concepts of understanding cyberterrorism as a legal definition, examines the historical features of the development of this phenomenon, identifies various approaches in the legal regulation of cyberterrorism in India, Nigeria and the Philippines. The author offers his own definition of cyberextremism, which is based on the compilation of constitutive features of cyberterrorism (as an self-determined phenomenon) and extremism. Particular attention is paid to the polysystem of legal regulation of the fight against cyberextremism and cyberterrorism (universal level of legal regulation, regional level of legal regulation and national legal regulation). The study of overseas experience of legal regulation allowed to shift the focus from the universal level of international legal regulation to the regional one, which will significantly affect the regional security structure. In the course of the study, the author came to the conclusion that the most promising area of regional cooperation in the fight against cyberextremism for the Russian Federation will be the Shanghai Cooperation Organization (further — SCO). This is due to the fact that the SCO is the only international organization that has a conventional regulation of extremism per se. The expansion of cooperation is appropriate given the fact that cyber extremism is a certain form of extremism, as well as the experience of the Republic of India as a SCO member state, which has relevant national legislation aimed at countering cyberterrorism.

Keywords: cyberterrorism, cyberextremism, cybercrime, Shanghai Cooperation Organization, separatism, critical infrastructure facilities, cybersecurity

For citation: Melnik S. S. Legal regulation of Cyberextremism and Cyberterrorism: challenges and opportunities. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 1 (65), pp. 187–192. (In Russ.). https://doi.org/10.36511/2078-5356-2024-1-187-192.

XXI век зачастую называют цифровым, так как произошел качественный скачок в развитии информационно-коммуникационных технологий. Безусловно, это не могло не коснуться преступности в широком смысле этого слова. Данное социальное явление давно изучается психологами, социологами, юристами, и все склонны считать, что преступления будут вечным спутником любого общества в любой точке земного шара (основная криминологическая аксиома гласит: «Никто не знает, почему преступления совершаются, но они совершались и будут совершаться»). С развитием технологий преступники стали совершенствовать свои навыки, активно осваивая новые инструменты (социальные сети, криптовалюту, мессенджеры и др.).

Эти же возможности появились и у террористов, которые все чаще используют информационно-коммуникационную сеть «Интернет» в своих целях, в том числе для продвижения крайних экстремистских взглядов, возникла проблема «цифрового терроризма», который в некоторых источниках употребляется как синоним терминов «кибертерроризм» и «киберэкстремизм». Все это в очередной раз поставило весь цивилизованный мир перед проблемой обеспечения кибербезопасности как отдельных стран, так и международных организаций (ЕС, СЕ, ЕАЭС, ШОС и пр.).

В 2021 году Центром стратегических и международных исследований (*Center for Strategic and International Studies*) было выявлено 118 кибератак, которые можно квалифицировать как акты кибертерроризма. Они были направлены на государственные учреждения, крупные *IT*-компании (*information technologies company*), предприятия оборонно-промышленного комплекса, а также имели своей целью совершение преступлений в сфере экономики, ущерб от которых превысил 1 млн долларов США. Среди них были кибератаки на крупнейшие китайские *gaming*-компании (разработка видеоигр), объекты критической инфраструктуры — система водоснабжения в городе Олдсмар, Флорида; Национальное агентство по атомной энергии Польши, Министерство здравоохранения Польши и ряд других [1].

На данный момент нет общепризнанного определения кибертерроризма или киберэкстремизма, появление последнего связывают и

вовсе с началом 2000-х. Термин «кибертерроризм» впервые был использован сотрудником Калифорнийского института безопасности и разведки Барри К. Коллином в середине 1980-х годов [2]. Предложенное им определение исходило из конвергенции кибернетики и терроризма. После этого в различных источниках появились свои варианты толкования, стали добавляться юрисдикционные особенности, признаки конкретных правовых семей, юридико-технических средств и культурологических факторов. Например, Габриэль Вейманн под кибертерроризмом понимает особую сферу соприкосновения киберпространства и терроризма. К нему он относит: незаконные кибератаки или угрозы совершения таких атак на информационные сети, которые совершаются с целью запугивания или принуждения правительства или его народа для достижения политических целей. По мнению этого исследователя, такая квалификация возможна лишь в том случае, если результатом станут серьезные последствия, которые, как минимум, будут вселять страх в население. Атаки на объекты критической инфраструктуры следует квалифицировать в зависимости от причиненного вреда [2]. При этом установление качественных характеристик такого понятия, как «страх», не так однозначно. Как известно, отличительной чертой уголовного законодательства является его определенность и точность, что в данном определении этим требованиям не соответствует.

Наиболее удачным с точки зрения системного подхода к толкованию дефиниции является определение, предложенное Дж. Плотнеком и Д. Слеем, которые, выделив такие признаки понятия, как актор, мотив, намерение, используемые средства, эффект, цель, предположили, что это умышленная атака или угроза таковой со стороны негосударственных субъектов с намерением использовать киберпространство для того, чтобы возникли реальные последствия, с целью вызвать страх или принудить гражданских, государственных или негосударственных субъектов к выполнению социальных или идеологических целей. К числу реальных последствий кибертерроризма авторы относят физические, психосоциальные, политические, экономические, экологические и др., которые происходят за пределами киберпространства [3]. Особую роль они отводят субъектному составу, что необходимо для разграничения, например, с такими понятиями, как «кибервойна» и «кибертерроризм».

Вопрос о последствиях остается дискуссионным, так как с ним связана конструкция объективной стороны преступления, что в значительной степени влияет на квалификацию и требует дальнейшего анализа. Разграничение с киберэкстремизмом можно провести на основе цели, что будет выражаться в распространении крайних взглядов, а также идеологии разделения по принципу «свой–чужой», остальные же признаки будут аналогичными уже указанным выше.

Помимо теоретических вариаций осмысления, в некоторых странах предпринимались попытки внедрения практических мер по борьбе с кибертерроризмом, как с отдельной категорией преступлений. Например, само понимание проблемы появилось достаточно давно, в конце 1990-х годов, в США [4]. Уже тогда возникла реальная угроза для нормального функционирования основных государственных институтов. В 1997 году был подготовлен отчет Комиссии по защите критически важных объектов, в своем роде уникальный, так как именно в нем впервые были установлены сферы, представляющие особое значение для самого существования государства. К их числу отнесены: обмен информацией, энергетика, банки и финансы, движение товаров и службы экстренного реагирования. В этом же отчете поднимается вопрос о соответствии уголовного законодательства тем вызовам и угрозам, которые несет в себе киберпреступность (*Adequacy of Criminal Law and Procedure for Infrastructure Assurance*). В частности отмечалось, что для эффективного уголовно-правового предотвращения киберпреступлений необходимы не только усилия на федеральном уровне, но также на уровне штатов, местного самоуправления и международном уровнях [5]. Актуальность этих выводов до сих пор не утрачена. Особо необходимо обратить внимание и на порядок расположения мер по противодействию киберпреступности. Приоритет отдается именно национальному уровню в полисистемном правовом регулировании. Однако в случае с актами кибертерроризма и киберэкстремизма участие как компетентных органов, так и государств в международных правоохранительных организациях является необходимым условием обеспечения международной безопасности. Кибертерроризм «стирает» рамки между государствами, разрушая институты, имеющие конститутивное значение как для конкретного государства и общества, так и для поддержания международного правопорядка. Это обусловлено тем, что такие атаки могут совершаться на несколько стран одновременно или же на интеграционные образования, что

существенно затрудняет расследование и сотрудничество в этой области.

Одной из актуальных проблем, связанных с киберэкстремизмом и кибетерроризмом, является установление юрисдикции в отношении атак, направленных на объекты критической инфраструктуры государства. Представляется, что решение именно этого вопроса требует некоторого отступления от известных доктринальных позиций в отношении уголовной и международной уголовной юрисдикции.

Например, Пол Стоктон и Мишель Голдман (Юридический факультет Йельского университета) обращают внимание на то, что теории понимания юрисдикции, которые разрабатывались в Гарвардском университете в 1930-х, 1950-х и 1980-х годах, не могли предвидеть появление у террористов возможности совершать атаки на различные государственные институты с территории других стран, что стало возможным благодаря информационно-коммуникационной сети «Интернет» [6].

В этой связи одним из возможных вариантов разрешения юрисдикционного вопроса является расширение экстерриториального действия закона в отношении кибертерроризма и киберэкстремизма, что требует консенсуса в рамках международного сообщества. Для этого необходимо построение структуры международного сотрудничества на основе, прежде всего, универсального международного договора, в котором будет определено само понятие этих явлений и установлены обязательства по привлечению к уголовной ответственности за их совершение. При этом региональное сотрудничество, даже если оно обеспечено соответствующими международными договорами регионального характера, может выступать лишь промежуточным этапом в процессе становления универсальной системы противодействия кибертерроризму.

Однако на сегодняшний день установление юрисдикции в отношении таких преступлений сопряжено с проблемами, поскольку в законодательстве лишь отдельных стран предусмотрена уголовная ответственность за кибертерроризм.

Так, уже установлена уголовная ответственность за совершение кибертерроризма в Нигерии, где статьей 18 *Закона о киберпреступности (2015)* установлено, что любое лицо, которое получает доступ к компьютеру или компьютерной системе в целях осуществления террористической деятельности, совершает преступление, за которое устанавливается наказание в виде пожизненного лишения свободы [7]. Такое определение не раз подвергалось критике по большей части из-за отсутствия развернутой характеристики качественных признаков деяния. Обращалось внимание на необходимость уточнения целей, способов и мотивов совершения такого противоправного деяния, так как отсутствие адекватного определения его понятия, вне всяких сомнений, создает проблемы для уголовно-правового преследования нарушителей [8].

В Индии *Закон об информационных технологиях 2000 года* также предусматривает ответственность за совершение кибертерроризма. Статья 66*F* устанавливает, что любое лицо, которое угрожает единству, целостности и безопасности Индии или вселяет страх в людей (либо определенную его часть) путем: попытки проникновения к компьютерной системе без соответствующего доступа, ограничения доступа к компьютерной системе или использования программы или набора команд, искажающих или разрушающих информацию, обрабатываемую компьютером или передаваемую по сети, несет уголовную ответственность и влечет за собой наказание вплоть до пожизненного лишения свободы [9].

Интересен в этом плане и опыт Филиппин, где в 2012 году появилась идея создания *Великой хартии вольностей за свободу интернета на Филиппинах*. Данный акт так и не был принят, но тем не менее он содержал определение этого термина, в 2022 году была попытка возобновить соответствующую дискуссию. Так как разработкой законопроекта занимались сенаторы и специалисты в области обеспечения кибербезопасности, взгляд на возможный подход к правовому закреплению остается актуальным. В главе II проекта Хартии дается следующее определение кибертерроризму: «Это нарушение Закона о безопасности личности 2007 года, совершенное посредством или с использованием Интернета, или информационно-коммуникационных технологий» [10]. Таким образом, дается общая характеристика способа совершения преступления с отсылкой на специальный нормативный правовой акт.

Ключевым аспектом противодействия кибертерроризму и киберэкстремизму является как национальное, так и международно-правовое регулирование. Косвенно это подтверждается полисистемностью мер противодействия киберпреступности, указанных в отчетах США. Выработка необходимого нормативного регулирования должна учитывать особенности юридической техники соответствующего государства. А также теоретическую базу, которая

была выработана за последние 30 лет, так как угроза кибертерроризма и киберэкстремизма не эфемерна, а вполне реальна. В данной ситуации необходимо опережать события, формируя необходимые институциональные механизмы в рамках различных межгосударственных образований. В этом контексте необходимо обратить внимание на уже имеющийся опыт региональных организаций, в частности ШОС. Именно в рамках этой международной организации впервые на договорном уровне были предложены меры по противодействию экстремизму [11]. И этот опыт может и должен быть использован для эффективной борьбы с терроризмом и экстремизмом в информационно-телекоммуникационной сети «Интернет».

На наш взгляд, принятие универсального международного договора является одним из возможных вариантов разрешения существующих проблем в организации и противодействии киберпреступности в широком смысле слова, и, в частности, с кибертерроризмом и киберэкстремизмом. Однако последнее обстоятельство пока еще не находит широкой поддержки и консенсуса. Об этом свидетельствует, например то, что, если во внесенном Российской Федерацией 30 июля 2021 года на рассмотрение проекте Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях [12] имелись проектируемые статьи 20 (Преступления, связанные с террористической деятельностью) и 21 (Преступления, связанные с экстремистской деятельностью), то в текущем ее проекте эти нормы оказались в числе исключенных [13].

В таких условиях именно региональная структура безопасности может заложить фундамент для дальнейшего расширения нормативного регулирования противодействия кибертерроризму и киберэкстремизму.

Таким образом, можно сделать вывод о том, что проблема правового регулирования противодействия кибертерроризму и киберэкстремизму требует особого внимания со стороны мирового сообщества. Выработка мер, направленных на противодействие таким противоправным деяниям, должна учитывать уже существующие теоретические подходы к правовому регулированию данной категории преступлений, так как они наиболее адекватно отражают ту модель нормативного закрепления, которая позволит наиболее эффективно противодействовать кибертерроризму. Для отечественной науки уголовного права важным является субъектный состав и наличие последствий, здесь необходим взвешенный, сбалансированный подход, как например в Республике Индия. Из рассмотренных в статье подходов к нормативному регулированию в отдельных странах именно индийское законодательство отражает единство теории и практики борьбы с терроризмом и экстремизмом в киберпространстве. Помимо этого, Индия является одним из государств-членов ШОС, использование уже известных юридических средств воздействия на преступность в существенной степени облегчит гармонизацию законодательства внутри интеграционного образования, что также является безусловным преимуществом. Вместе с тем, конечно же, проблема терроризма и экстремизма является глобальной для всего мирового сообщества. Необходимо прилагать усилия всех субъектов международного права для ограничения распространения экстремистской идеологии, однако этот процесс требует времени и дополнительных усилий со стороны ряда международных организаций. Наиболее эффективным на данном этапе будет использование комплекса мер, которые вырабатываются на региональном уровне [14].

Список источников

1. What is cyberterrorism? 2022. URL: https://www.techtarget.com/searchsecurity/definition/cyberterrorism#:~:text=The%20U.S.%20Federal%20Bureau%20of,subnational%20groups%20or%20clandestine%20agents.%22 (дата обращения: 23.05.2023).

2. Plotnek J., Slay, J., "Cyber Terrorism: A Homogenized Taxonomy and Definition" (2021). Computers & Security, Volume 102.

3. Cyberterrorism How Real Is the Threat? Gabriel Weimann. URL: https://www.usip.org/sites/default/files/sr119.pdf (дата обращения: 23.05.2023).

4. Cyber Terrorism. Why it exists, why it doesn't, and why it will. Stefan Soesanto. 2020. URL: https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/ (дата обращения: 23.05.2023).

5. The Report of the President's Commission on Critical Infrastructure Protection. URL: https://sgp.fas.org/library/pccip.pdf (дата обращения: 23.05.2023).

6. Paul N. Stockton, Michele Golabek-Goldman PROSECUTING CYBERTERRORISTS: APPLYING TRADITIONAL JURISDICTIONAL FRAMEWORKS TO A MODERN THREAT. URL: https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf (дата обращения: 10.07.2023).

7. CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT 2015. URL: https://lawpadi.com/wp-content/

uploads/2015/08/CyberCrime_ProhibitionPreventionetc_Act_2015.pdf (дата обращения: 10.07.2023).

8. Marcus Araromi. Cyber-Terrorism under the Nigerian Law: A New Form of Threat or an Old Threat in a New Skin? URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3286617 (дата обращения: 10.07.2023).

9. THE INFORMATION TECHNOLOGY ACT 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 10.07.2023).

10. The Magna Carta for Philippine Internet Freedom. Legacy.senate.gov.ph.. URL: http://legacy.senate.gov.ph/lisdata/1446312119!.pdf (дата обращения: 20.12.2021).

11. Волеводз А. Г., Ализаде В. А. Международно-правовые подходы к противодействию экстремизму: материально-правовые и процессуальные аспекты // Международное уголовное право и международная юстиция. 2018. № 6. С. 7–11.

12. Письмо Временного поверенного в делах Постоянного представительства Российской Федерации при Организации Объединенных Наций от 30 июля 2021 года на имя Генерального секретаря // Документ ООН A/75/980, August 10, 2021.

13. Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях: записка Председателя: пересмотренный текст конвенции // Документ ООН A/AC.291/22/Rev.1, 6 November 2023.

14. Xue Y., & Makengo B. M. (2021). Twenty Years of the Shanghai Cooperation Organization: Achievements, Challenges and Prospects. Open Journal of Social Sciences, 9, 184–200.

References

1. What is cyberterrorism? 2022. URL: https://www.techtarget.com/searchsecurity/definition/cyberterrorism#:~:text=The%20U.S.%20Federal%20Bureau%20of,subnational%20groups%20or%20clandestine%20agents.%22 (accessed 23.05.2023).

2. Plotnek J., Slay, J., "Cyber Terrorism: A Homogenized Taxonomy and Definition" (2021). Computers & Security, Volume 102.

3. Cyberterrorism How Real Is the Threat? Gabriel Weimann. URL: https://www.usip.org/sites/default/files/sr119.pdf (accessed 23.05.2023).

4. Cyber Terrorism. Why it exists, why it doesn't, and why it will. Stefan Soesanto. 2020. URL: https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/ (accessed 23.05.2023).

5. The Report of the President's Commission on Critical Infrastructure Protection. URL: https://sgp.fas.org/library/pccip.pdf (accessed 23.05.2023).

6. Paul N. Stockton, Michele Golabek-Goldman PROSECUTING CYBERTERRORISTS: APPLYING TRADITIONAL JURISDICTIONAL FRAMEWORKS TO A MODERN THREAT. URL: https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf (accessed 07.10.2023).

7. CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT 2015. URL: https://lawpadi.com/wp-content/uploads/2015/08/CyberCrime_ProhibitionPreventionetc_Act_2015.pdf (accessed 10.07.2023).

8. Marcus Araromi. Cyber-Terrorism under the Nigerian Law: A New Form of Threat or an Old Threat in a New Skin? URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3286617 (accessed 07.10.2023).

9. THE INFORMATION TECHNOLOGY ACT 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (accessed 07.10.2023).

10. The Magna Carta for Philippine Internet Freedom. Legacy.senate.gov.ph. URL: http://legacy.senate.gov.ph/lisdata/1446312119!.pdf (accessed 20.12.2021).

11. Volevodz A. G., Alizade V. A. International legal approaches to countering extremism: substantive and procedural aspects. *International criminal law and international justice*, 2018, no. 6, pp. 7–11. (In Russ.)

12. Letter from the Charge d'Affaires of the Permanent Mission of the Russian Federation to the United Nations of July 30, 2021 addressed to the Secretary General. UN Document A/75/980, August 10, 2021. (In Russ.)

13. Ad Hoc Committee on the Development of a Comprehensive International Convention against the Use of Information and Communication Technologies for Criminal Purposes: note by the Chairman: revised Text of the Convention. UN Document A/AC.291/22/Rev.1, 6 November, 2023. (In Russ.)

14. Xue Y., & Makengo B. M. (2021). Twenty Years of the Shanghai Cooperation Organization: Achievements, Challenges and Prospects. Open Journal of Social Sciences, 9, 184–200.

Статья поступила в редакцию 11.07.2023; одобрена после рецензирования 25.12.2023; принята к публикации 05.03.2024.

The article was submitted 11.07.2023; approved after reviewing 25.12.2023; accepted for publication 05.03.2024.