Дата поступления рукописи в редакцию: 15.07.2026 г.
Дата принятия рукописи в печать: 11.07.2026 г.

DOI: 10.24412/2782-3849-2026-7-58-61

ЯЦЕНКО Сергей Васильевич,

доцент кафедры судебно-экспертной и оперативно-розыскной деятельности факультета подготовки криминалистов Санкт-Петербургской академии Следственного комитета, кандидат юридических наук, доцент,

e-mail: mail@law-books.ru

КОРЧАГИН Андрей Анатольевич,

ФГБОУ ВО «Кубанский государственный аграрный университет имени И.Т. Трубилина», доцент, доктор юридических наук,

e-mail: mail@law-books.ru

К ВОПРОСУ О КИБЕРТЕРРОРИЗМЕ КАК СОВРЕМЕННОЙ УГРОЗЕ БЕЗОПАСНОСТИ ГОСУДАРСТВА: ЗНАЧЕНИЕ И МАСШТАБЫ ПРОБЛЕМ ПРОТИВОДЕЙСТВИЯ

Аннотация. *Автор в своей научной статье проводит комплексный анализ существующих угроз, реализуемых в информационном пространстве связанных с кибертерроризмом и иными видами преступлений, с помощью цифровых технологий, проблемах противодействия данным проявлениям и способах их решения.*

Ключевые слова: *правоохранительные органы, кибертерроризм, противодействие, цифровые технологии, общество, безопасность, государство*

YATSENKO Sergey Vasilyevich,

Associate Professor, Department of Forensic and Operational-Investigative Activities, Faculty of Forensic Science Training St. Petersburg Academy of the Investigative Committee Candidate of Law, Associate Professor

KORCHAGIN Andrey Anatolyevich,

Federal State Budgetary Educational Institution of Higher Education "Kuban State Agrarian University named after I.T. Trubilin" Associate Professor, Doctor of Law

ON CYBERTERRORISM AS A MODERN THREAT TO STATE SECURITY: THE SIGNIFICANCE AND SCOPE OF COUNTERMEASURES

Annotation. *In this research article, the author provides a comprehensive analysis of existing threats implemented in the information space related to cyberterrorism and other crimes using digital technologies, the challenges of countering these phenomena, and solutions.*

Key words: *law enforcement, cyberterrorism, countermeasures, digital technologies, society, security, state*

В современных условиях тотальной оцифровки экономики и социальной сферы активно внедряются цифровые и инновационные решения, способствуя формированию глобального единого информационного пространства.

Современная жизнь практически немыслима без интернет-соединения, которое обеспечивает доступ к госуслугам, коммерческим платформам и базам данных. Наряду с очевидными преимуществами технологического прогресса, повсеместное использование Сети сопряжено с рисками: ростом объема фейковых новостей и оскорблений, а также угрозами хищения персональных сведений и банковских средств.

Деяния, совершаемые в глобальной компьютерной сети, представляют собой правонарушения, использующие новейшие информационно-технические ресурсы, которые активно применяются террористами и соответствующими организациями.

Распространение интернета привело к выходу террористической деятельности за рамки

национальных границ, что породило феномен «кибертерроризма», где главным инструментом выступают цифровые технологии.

Данный вид преступности представляет серьезную угрозу национальной безопасности государств.

Причины актуальности интернет-преступлений кроются в высокой степени анонимности таких действий, широкой аудитории, низкой правовой и цифровой культуре населения, трудностях идентификации злоумышленников и блокировки их ресурсов, а также в неспособности эффективно реагировать на особенности современного информационно-коммуникационного кризиса.

Увеличение числа интернет-преступлений и правонарушений, совершаемых с использованием современных информационных технологий, усиливается под влиянием сложной внешнеполитической конъюнктуры.

Эта обстановка отличается нестабильностью и рисками, обусловленными активной деятельностью запрещенной в РФ террористической группировки «ИГИЛ», которая через различные цифровые площадки проводит вербовку молодежи в свои незаконные вооруженные структуры.

Также негативное воздействие оказывают рост нелегального трафика наркотиков и психотропных препаратов, введение экономических санкций против России и напряженная ситуация на Украине.

Прежде чем анализировать ключевые проблемы борьбы с киберпреступностью, целесообразно определить основные категории правонарушений в цифровой среде. В наиболее общем виде все подобные деяния делятся на две большие группы: насильственные и ненасильственные.

К насильственным преступлениям относятся угрозы физического насилия, кибersталкинг (преследование), а также проявления киберэкстремизма и кибертерроризма.

В группу ненасильственных входят кибермошенничество, шантаж в сети, хищение цифровых активов, нелегальный оборот запрещенных веществ, организация азартных игр через интернет и легализация денежных средств, полученных преступным путем, с использованием электронных платежей.

Простота доступа к информационному пространству существенно затрудняет борьбу с преступлениями, связанными с незаконным оборотом наркотиков и психотропных веществ, а также с пропагандой деструктивных религиозных и политических идей. Подобные правонарушения массово охватывают молодежную среду, нанося серьезный ущерб национальным интересам государства.

С технологической стороны кибертерроризм представляет собой террористическую активность, осуществляемую через применение информационных технологий.

Кибертеррористы используют широкий арсенал цифровых инструментов: от атак на компьютерные сети и коммуникации до распространения террористического контента в электронной форме.

Ущерб технологической инфраструктуре причиняется незаконными действиями, такими как внедрение вредоносного ПО в уязвимые системы или атаки на веб-ресурсы.

С диалектической точки зрения кибертерроризм определяется как умышленная разрушительная деятельность, направленная на нанесение идеологического, религиозного или социального вреда с использованием информационных средств

Кибертерроризм является составной частью киберконфликтов, которые представляют собой реальную опасность для национальной безопасности и требуют безотлагательного вмешательства со стороны государства.

Противодействие таким угрозам должно опираться на нормы международного права.

Как следует из вышесказанного, в научной среде существует множество трактовок понятия «кибертерроризм», отличающихся широким охватом.

Современные тенденции постиндустриального этапа развития общества порождают ряд существенных противоречий.

Цифровизация и информатизация, стимулируя прогрессивные изменения, одновременно генерируют новые риски, в том числе затрагивающие систему национальной безопасности.

В современных условиях правоохранительные органы испытывают значительные трудности, обусловленные скрытностью киберпреступной деятельности, масштабами воздействия в интернете, серьезным искажением данных и низким уровнем цифровой и правовой культуры граждан.

Для обеспечения безопасности данных применяются четыре ключевых направления:

физическая защита, заключающаяся в создании материальных преград для несанкционированного доступа к данным;

правовая защита, опирающаяся на совершенствование нормативно-правовой базы;

техническая защита, направленная на охрану информационных ресурсов с использованием некриптографических методов;

криптографическая защита,

обеспечивающая безопасность данных посредством их шифрования.

Тем не менее, наряду с позитивными процессами, такими как развитие гражданского общества и рост политической активности, наблюдаются и деструктивные тенденции.

Яркими примерами служат распространение терроризма, активизация террористических группировок, а также деятельность киберпреступников, чьи действия носят террористический характер.

Кибертерроризм представляет собой серьезную угрозу информационной безопасности государства и выступает новым элементом в системе национальных и международных рисков.

Анализ статистических данных и мирового опыта противодействия киберпреступности показывает, что уровень интернет-преступности в России в настоящее время остается высоким. Это обусловлено рядом следующих факторов:

недостаточная правовая урегулированность процедур эксплуатации информационных ресурсов и несовершенство нормативно-правовой базы в сфере противодействия киберпреступности;

трудности, возникающие при проведении расследований киберинцидентов и установлении личностей виновных лиц;

стремительное развитие киберпространства, появление инновационных методов осуществления хакерских атак, а также возникновение новых форм и

видов противоправных действий, реализуемых через информационные платформы;

отсутствие единого комплексного подхода и методологии в сфере борьбы с киберпреступностью.

На фоне тотальной цифровизации политической, экономической и государственной сфер риски, связанные с киберэкстремизмом и кибертерроризмом, стремительно нарастают.

В последнее время террористические и экстремистские группировки всё чаще публично заявляют о намерениях уничтожить или парализовать функционирование стратегически значимых объектов, причем такие угрозы нередко переходят в плоскость реальных действий.

Подобные инциденты вызывают резкую дестабилизацию политического климата и ставят под удар национальную безопасность страны, что в свою очередь ведет к существенной утрате обществом доверия к властным структурам.

Параллельно усиливается опасность применения информационных технологий для вывода из строя ключевых элементов государственной инфраструктуры с целью запугивания руководства страны.

Завершая анализ проведенного исследования, следует подчеркнуть, что преступления, совершаемые в цифровом пространстве с использованием современных информационных технологий, приобретают массовый масштаб и несут серьезную угрозу для всего человечества.

Также важно наладить системное и бесперебойное сотрудничество с развитыми странами для обмена опытом в активной борьбе с киберпреступниками, а также согласования и разработки совместных методов совершенствования борьбы с киберпреступлениями.

Представители правоохранительных органов и других служб обязаны постоянно повышать свои навыки и умения в борьбе с киберпреступлениями на современном уровне.

Такой вид преступления, как терроризм, проявляющийся в киберпространстве, представляет собой одно из самых опасных явлений в современном обществе, нося деструктивный характер для всего человечества.

Обеспечение безопасности национального информационного пространства - процесс сложный, требующий комплексного, многоаспектного подхода, но вполне подлежащий реализации.

Учитывая масштабность проблематики и её глобальную значимость, целесообразно разбить комплексную дилемму на отдельные составляющие для их последовательного решения.

Государству следует задействовать специализированные административные и технологические механизмы.

Ключевым аспектом является законодательное закрепление уголовной ответственности за финансирование террористической деятельности.

Параллельно требуется усилить оперативный обмен данными, направленными на предотвращение киберпреступлений.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (с изм. от 29 июля 2017 г. № 250-ФЗ) // Собрание законодательства РФ. - 1996. - № 25. - ст. 2954.

[2] Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» // СЗ РФ. – 2011. – № 27. – ст. 3872.

[3] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. – 2006. – № 31. – ст. 3448. 8.

[4] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. –

2016. – № 50. – ст. 7074.

[5] Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие / А. В. Аносов. – М.: Академия управления МВД России, 2019. – 208 с.

[6] Артамонов В.А. Кибербезопасность в условиях цифровой трансформации социума / В.А. Артамонов // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 1. – С.777-784.

[7] Ахриева М.М. Киберпреступность в условиях современной экономики / М.М. Ахриева // Международный журнал гуманитарных и естественных наук. – 2021. – № 8-2 (59). – С.80-82.

[8] Малышева Ю.Ю. Проблемы квалификации обмана как способа совершения мошенничества с использованием электронных средств платежа // Мониторинг правоприменения. 2018. № 4 (29). С. 31-33.

[9] Третьякова Е.И. Способы совершения мошенничества с использованием электронных средств платежа // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 1. С. 169-176.

References:

[1] Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on July 29, 2017 No. 250-FZ)//Collection of Legislation of the Russian Federation. - 1996. - № 25. - Art. 2954.

[2] Federal Law of 27.06.2011 No. 161-FZ “On the National Payment System “//NW RF. – 2011. – № 27. - Art. 3872.

[3] Federal Law of 27.07.2006 No. 149-FZ “On Information, Information Technologies and Information Protection “//NW RF. – 2006. – № 31. - Art. 3448. 8.

[4] Decree of the President of the Russian Federation of 05.12.2016 No. 646 “On Approval of the Information Security Doctrine of the Russian Federation “//NW of the Russian Federation. – 2016. – № 50. - Art. 7074.

[5] A.V. Anosov. Activities of the internal affairs bodies to combat crimes committed using information, communication and high technologies: study. manual/A.V. Anosov. - M.: Academy of Management of the Ministry of Internal Affairs of Russia, 2019. - 208 s.

[6] Artamonov V.A. Cybersecurity in the context of digital transformation of society/V.A. Artamonov//Greater Eurasia: development, security, cooperation. – 2022. – № 1. - С.777-784.

[7] Akhrieva M.M. Cybercrime in the modern economy/M.M. Akhrieva//International Journal of Humanities and Natural Sciences. – 2021. – № 8-2 (59). - S.80-82.

[8] Malysheva Yu. Yu. Problems of qualification of deception as a method of committing fraud using electronic means of payment//Monitoring of law enforcement. 2018. № 4 (29). S. 31-33.

[9] Tretyakova E.I. Methods of committing fraud using electronic means of payment//Izvestia Tula State University. Economic and legal sciences. 2020. № 1. S. 169-176.