

Кибертерроризм – дестабилизирующий фактор и угроза национальной безопасности

Игорь СВИРИДОВ

Геополитическая поляризация мира привела к тому, что киберпространство превратилось в полноценный театр военных действий. Государственные субъекты всё чаще используют кибератаки как инструмент давления с целью уничтожения инфраструктуры и дезорганизации работы противника. В условиях новой геополитической реальности кибертерроризм¹ стал мощным дестабилизирующим фактором и серьёзной угрозой для национальной безопасности. Также кибертерроризм может использоваться и для распространения пропаганды, и для манипулирования общественным мнением, что чревато социальными и политическими потрясениями.

В настоящее время универсального определения международного терроризма нет, что создаёт серьёзные препятствия для эффективного международного сотрудничества². Отсутствие единой дефиниции терроризма в международном праве образует опасную правовую серую зону, в которой

СВИРИДОВ Игорь Владимирович – заместитель директора ФГБУ НИИ «Интеграл» (Минцифры).
E-mail: igoindigo@yandex.ru

Ключевые слова: киберпреступность, кибертерроризм, гибридная война, цифровой суверенитет, национальная безопасность.

¹ *Побегайло А.Э.* Киберэкстремизм – угроза национальной безопасности // Обозреватель–Observer. 2025. № 5. С. 105–119.

² *Холов С.Х.* Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений // Вестник МГЛУ. 2025. № 1. С. 41–52.

кибертерроризм не может быть последовательно преследуем в судебном порядке³.

Следует отметить, что в отличие от международного уровня во многих государствах сформированы собственные правовые подходы к определению террористических действий, что создаёт дополнительные сложности для международного сотрудничества из-за различий в квалификации одних и тех же действий.

Так, в российском законодательстве закреплено легальное определение терроризма: ст. 361 Уголовного кодекса Российской Федерации определяет акт международного терроризма как совершение вне пределов территории Российской Федерации взрыва, поджога или иных действий, подвергающих опасности жизнь, здоровье, свободу или неприкосновенность граждан Российской Федерации, совершённых в целях нарушения мирного сосуществования государств и народов либо направленных против интересов Российской Федерации, а также угрозу совершения указанных действий^{4, 5}.

Конституционный Суд России в отношении терроризма опирается на нормы действующего уголовного законодательства РФ (УК РФ) и нормы международного права⁶. При этом им выработана важная концептуальная позиция, которая имеет принципиальное значение для понимания этой угрозы: терроризм должен рассматриваться не только как преступление против общественного порядка, но и как преступление против безопасности человечества.

Законодательство США также содержит развёрнутое определение международного терроризма в разделе 2331 Кодекса США (18 U.S.C. § 2331)^{7, 8, 9}.

В Китайской Народной Республике определение терроризма закреплено в Законе о борьбе с терроризмом от 27 декабря 2015 г.^{10, 11}

³ Diwaker S. Cyber-Terrorism and the Changing Definition of Terrorism: Prospects for India in International Law // International Journal of Law Management & Humanities. 2026.

⁴ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.04.2023). Статья 361 «Акт международного терроризма» // URL: https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3ezdca/

⁵ Котова М. Пароль к периметру. Почему защита высокотехнологичной экономики больше не делится на «цифру» и «физику» // Коммерсантъ. 2026. 22 апреля.

⁶ Постановления Конституционного Суда РФ от 25 сентября 2014 г. № 2055-О // URL: <https://normativ.kontur.ru/document?moduleId=7&documentId=242563#10>; 31 марта 2022 г. № 804-О // <https://normativ.kontur.ru/document/7/422237-opredelenie-konstitutsionnogo-suda-rf-ot-31-03-2022-n-804-o>

⁷ 18 U.S.C. § 2331 – Definitions (United States Code). – Title 18, Part I, Chapter 113B // URL: <https://www.law.cornell.edu/uscode/text/18/2331>

⁸ Котова М. Пароль к периметру.

⁹ Montasari R. Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. Cham: Springer NATURE Switzerland AG, 2024. – 270 p.

¹⁰ Закон Китайской Народной Республики о борьбе с терроризмом от 27 декабря 2015 г. (Counter-Terrorism Law of the People's Republic of China) (принят на 18-й сессии ПК ВСНП 12-го созыва) // URL: https://www.spp.gov.cn/tt/201512/t20151228_109920.shtml

¹¹ Маслов К.Н. OSINT в условиях цифрового суверенитета: методы, ограничения, перспективы // Журнал международного права и информационной безопасности. 2024. Т. 12. № 3. С. 45–62.

В Европейском союзе правовой основой для гармонизации национальных подходов является Рамочное решение Совета ЕС 2002/475/JHA о борьбе с терроризмом (с изменениями 2008/919/JHA)^{12, 13}.

Разнообразие национальных подходов к определению международного терроризма, различающихся по признакам субъекта, целей, способов совершения и порогов наказуемости, создаёт дополнительные сложности для экстрадиции и международного правового сотрудничества, что подтверждает необходимость выработки универсальной дефиниции на уровне ООН.

В современных условиях террористические организации активно используют искусственный интеллект (ИИ) для вербовки, коммуникации и планирования атак¹⁴. Как показывает анализ данной проблематики, развитие искусственного интеллекта снижает порог входа для злоумышленников, что облегчает использование ИИ без необходимости обладания обширными навыками или технической экспертизой¹⁵.

Понятие кибертерроризма и история возникновения

Кибертерроризм – это преднамеренные, политически, идеологически или религиозно мотивированные действия в киберпространстве. Его цель – не просто нанести технический ущерб, а дестабилизировать работу государственных институтов, вызвать панику в обществе, оказать давление на власть, распространить страх или дискредитировать государственные структуры.

Одновременно с этим существует узкая трактовка кибертерроризма: совершение террористических актов в киберпространстве, комплекс противозаконных действий в информационном пространстве, представляющих собой атаки на ком-

пьютерные и телекоммуникационные технологии, направленные на создание угрозы международной и государственной безопасности с целью влияния на решение политических, экономических и иных задач. При таком подходе сущность кибертерроризма составляет деятельность по подготовке и реализации кибератак.

Управление ООН по наркотикам и преступности (UNODC) определяет кибертерроризм как «использование интернета для осуществления террористической деятельности, включая атаки на информационные системы, которые приводят или могут привести к гибели или ранению людей, повреждению иму-

¹² Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (as amended by Council Framework Decision 2008/919/JHA) // Official Journal of the European Union, L 164, 22.6.2002. P. 3–7 // URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002F0475>

¹³ Холов С.Х. Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений.

¹⁴ Krisnayanto Suryadi. Exploring the Dark Horizon: Artificial Intelligence (AI) as Cyberterrorism Tools // Journal of Terrorism Studies. 2025. Vol. 7. № 1.

¹⁵ Ibid.

щества или нарушению работы основных служб»¹⁶.

Европейское агентство по сотрудничеству в сфере правоохранительной деятельности (Европол – *Europol*) трактует кибертерроризм как «использование интернета для совершения насильственных действий, которые приводят или угрожают привести к гибели людей или причинению значительного вреда здоровью, с целью достижения политических или идеологических выгод путём запугивания»¹⁷.

В то же время в расширенной трактовке речь идёт не только о совершении террористических актов с помощью компьютерных сетей, но и о гибридном формате, когда цифровые средства применяются для пропаганды идеологии терроризма, вербовки и обучения новых членов террористических организаций, поддержания коммуникации между ячейками, координации их деятельности, поиска и осуществления финансирования террористической деятельности, проведения реальных террористических атак.

Однако с точки зрения государственной политики противодействия кибертерроризму представляется не совсем верным сводить сущность и содержание кибертерроризма только к террористическим актам в киберсреде, связанным главным образом с нанесением ущерба критически важным и потенциально опасным объектам,

объектам обеспечения жизнедеятельности населения или созданием опасности причинения значительного вреда жизни, здоровью или имуществу неопределённого круга лиц, национальной безопасности государства. Целесообразно рассматривать кибертерроризм как противозаконную деятельность, направленную на распространение идеологии экстремизма и терроризма посредством интернета, вербовку лиц для совершения преступлений террористического характера в киберпространстве, финансирование терроризма, а также атаки на критически важные объекты информационной инфраструктуры.

Сам термин «кибертерроризм» был предложен в 1982 г. старшим научным сотрудником Института безопасности и разведки (*Institute for Security and Intelligence*) США Б. Коллином¹⁸. Концепция кибертерроризма начала формироваться в 90-х годах, когда мир стал активно переходить в цифровую эпоху, а интернет становился всё более доступным. С развитием технологий возможности для кибертеррористов также расширялись, делая угрозу более серьёзной и многообразной. Исторически первые проявления кибертерроризма были связаны с простыми вирусами и хакерскими атаками, но со временем они стали более сложными и тонко настроенными, способными поражать целые

¹⁶ The Use of the Internet for Terrorist Purposes. Vienna: United Nations, 2012. – 96 p. // URL: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

¹⁷ Internet Organised Crime Threat Assessment (IOCTA) 2025. The Hague: European Union Agency for Law Enforcement Cooperation, 2025. – 112 p. // URL: <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2025>

¹⁸ Diwaker S. Cyber-Terrorism and the Changing Definition of Terrorism: Prospects for India in International Law.

секторы инфраструктуры и национальной безопасности.

Сегодня это явление эволюционировало от разрозненных действий до полноценного инструмента гибридной войны и стратегического фактора дестабилизации. В современных условиях кибертерроризм интегрируется с ментальным терроризмом – методом ведения гибридной войны в цифровом обществе¹⁹.

Новая промышленная революция, происходящая в мире, в своей основе имеет революционные пре-

образования в сфере информационных технологий. В XXI в. в геометрической прогрессии растёт ущерб от киберпреступлений, и фактически ни один из крупных террористических актов не обходится без использования современных информационных технологий. В условиях четвёртой промышленной революции кибертерроризм приобретает двойственную природу – выступая одновременно как угроза и как объект для международного реагирования²⁰.

Объекты и цели кибертерроризма

Суть кибертерроризма заключается в том, что для достижения идеологических, политических, религиозных или социальных целей злоумышленники используют цифровые инструменты. Они воздействуют либо на то, что формирует мнения и настроения людей (массовое сознание, доверие к институтам), либо на саму цифровую среду и управляемые ею реальные процессы.

Воздействие на сознание – это, например, распространение дезинформации, пропаганды или пугающих сообщений через соцсети и мессенджеры, чтобы вызвать панику, раскол в обществе, сформировать определённые установки.

Воздействие на инфраструктуру – это кибератаки на объекты, которые в современном мире полностью зависят от цифровых технологий (системы управления энергосетями, во-

доснабжением, транспортом, финансовыми системами, базами данных медицинских учреждений). Цель таких атак – вывести объекты из строя, создать угрозу техногенных аварий, нанести экономический ущерб или дестабилизировать работу целых отраслей.

Под удар попадают самые разные объекты:

- государственная и военная сферы (правительственные сети, учреждения, оборонные предприятия, системы военного управления);
- критическая инфраструктура (энергетические объекты, системы водоснабжения и очистки воды, транспортные системы, телекоммуникационные сети);
- финансовый сектор (банки, платёжные системы, биржи);
- бизнес (крупные корпорации и компании);

¹⁹ Савушкина М.А. Ментальный терроризм как метод ведения гибридной войны в цифровом обществе // Вестник Челябинского государственного университета. 2024. № 7. С. 48–54.

²⁰ Montasari R. Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses.

- отдельные личности (политики, общественные деятели, эксперты);
- программное обеспечение и сети.

На первый взгляд кибертерроризм и иные киберпреступления могут казаться схожими: и там и там атакуют компьютеры, сети, данные. Но ключевое отличие кибертерроризма от других видов киберпреступлений лежит в мотивации, где на первый план выходят политические, идеологические или социальные задачи, а не личная или корпоративная выгода. В корыстных мошеннических киберпреступлениях мотив чаще сугубо личный или корпоративный: кража денег (например, через взлом банковского счёта), хищение коммерческой тайны для перепродажи, шантаж с целью получения выкупа, распространение запрещённого контента. Если киберпреступление обычно направлено на конкретный объект (человека, компанию, систему), то кибертерроризм нацелен на достижение широких системных последствий. Преступники атакуют критически важную инфраструктуру (энергетические системы, банки, транспортные сети, государственные порталы), чтобы вызвать масштабный сбой, парализовать работу целых секторов, посеять панику.

Основные задачи:

- запугивание и дестабилизация (посеять страх среди населения, подорвать доверие к государственным институтам);
- распространение дезинформации, влияние на общественное мнение или создание искажённой картины событий, оказание давления на власть и изменение политики (принудить государство к определённым решениям);

– нарушение общественной безопасности (вывод из строя объектов инфраструктуры);

– распространение идей и требований (использование цифровых каналов для пропаганды);

– сбор разведданных (кибершпионаж);

– финансовый ущерб как средство давления.

По своему характеру воздействия кибертерроризм часто подразумевает открытость: злоумышленники могут публично заявлять о своих требованиях, демонстрировать угрозу для усиления психологического эффекта. Это создаёт атмосферу постоянного страха и неопределённости.

В «обычных» киберпреступлениях фокус направлен на конкретного пользователя или организацию: взлом личного аккаунта, кража данных клиента магазина, компрометация корпоративной тайны. В кибертерроризме мишенью становятся не столько коммерческие структуры, сколько государственные институты, международные организации, символы власти, публичные фигуры. Основная цель – нанесение удара по доверию к институтам в целом.

Если хакер взломал базу данных больницы, чтобы продать данные конкурентам, – это киберпреступление (финансовая выгода).

Если тот же взлом использовали, чтобы спровоцировать панику, нарушить работу системы экстренного реагирования и выдвинуть политические требования властям – это уже кибертерроризм.

Иногда действия, изначально нацеленные на личную выгоду, со временем приобретают политический подтекст (например, крупная утечка данных большой компании, которую затем используют для политического

давления). Но базовое отличие сохраняется – в первичном стимуле и масштабе последствий для общества. Для любого террористического акта должны быть выполнены два ключевых элемента: оперативная способность провести атаку и мотив или мотивация для её осуществления²¹.

Понимание этих форм помогает выстраивать защиту, укреплять кибербезопасность критически важных объектов, развивать системы обнаружения атак и совершенствовать международное сотрудничество в сфере противодействия таким угрозам.

Основные формы кибертерроризма

Косновным формам кибертерроризма относятся: атаки на информационные системы и критически важную инфраструктуру, взлом государственных и корпоративных систем с целью кражи информации, подмены данных или саботажа, распространение вредоносного программного обеспечения (вирусов, троянов, программ-вымогателей), деструктивная пропаганда и вербовка через интернет, нарушение работы и захват каналов связи, СМИ и распространение дезинформации.

Атаки на информационные системы и критически важную инфраструктуру – это наиболее опасная форма кибертерроризма, нацеленная на вывод из строя энергосетей, транспортных узлов, банковских учреждений, систем водоснабжения и здравоохранения и других жизненно важных объектов. Злоумышленники проникают в компьютерные системы, чтобы нарушить их работу, вывести из строя оборудование или ПО, иска-

зить данные, вызывая физические разрушения и техногенные катастрофы (*DDoS-атаки*, внедрение вирусов и программных закладок, захват управления технологическими процессами).

В 2025 г. основными целями атак стали правительственные учреждения (22%), промышленные организации (16%) и оборонные подрядчики (10%). В 2025–2026 гг. фокус сместился на физическую деструкцию и диверсии, а атаки окончательно перешли из плоскости ИТ в область операционных технологий²².

Например, в 2025 г. в Европе были зафиксированы кибератаки на энергетические объекты Швеции и Польши, а также на системы водоснабжения в некоторых польских городах. В частности, в январе 2025 г. шведская теплоэлектростанция в г. Кристинехамн подверглась кибератаке, в результате которой злоумышленники получили доступ к системам управления и на несколько часов отключили отопление в городе, оставив без тепла около 10 тыс. жителей²³.

В декабре 2025 г. зафиксирована масштабная скоординированная кибератака на польскую энер-

²¹ Trifunović D. Intelligence and Counterterrorism // National Security and The Future. 2025. Vol. 26. № 1. P. 179–192.

²² Котова М. Пароль к периметру.

²³ Fjärrvärmen i Kristinehamn slogs ut av cyberattack. 15 januari 2025 // URL: <https://www.svt.se/nyheter/lokalt/varmland/fjarrvarmen-i-kristinehamn-slogs-ut-av-cyberattack>

госеть: были выведены из строя ветряные и солнечные электростанции, а также промышленные системы управления, что привело к неремонтопригодному повреждению оборудования²⁴.

Кроме того, в 2025 г. было взломано не менее пяти водоочистных станций в небольших польских городах, где злоумышленники получили доступ к системам, отвечающим за работу насосов, фильтров и дозирования химикатов²⁵.

В России за первый квартал 2026 г. на критическую информационную инфраструктуру (КИИ) пришлось рекордные 77% всех кибератак на организации, а общее количество атак на отрасли КИИ превысило 9 тыс. за три месяца. Доля высококритичных атак в секторе КИИ достигла 27%, тогда как в остальных отраслях этот показатель не превышает 20%²⁶.

Одной из крупнейших кибератак на инфраструктуру в России в 2025 г. была атака на авиакомпанию «Аэрофлот», уничтожено около 7 тыс. физических и виртуальных серверов, похищено 12 Тбайт баз данных, 8 Тбайт конфиденциальной информации.

В результате атаки было отменено более 100 рейсов, а недополученная выручка авиакомпании могла составить порядка 275 млн руб.²⁷

Число кибератак с использованием ИИ на российскую критическую

инфраструктуру в 2025 г. почти удвоилось по сравнению с 2024 г.

Общее количество атак с использованием ИИ по всему миру выросло за прошлый год на 93%. По прогнозам, в 2026 г. глобальное осуществление 85% кибератак будет проводиться с использованием ИИ²⁸.

Как было отмечено в Конвенции ООН против киберпреступности, принятой Генеральной Ассамблеей ООН 24 декабря 2024 г., кибератаки с использованием искусственного интеллекта могут уничтожить критически важную инфраструктуру или нарушить её работу в считанные минуты, что превращает ИИ в мощнейший мультипликатор угроз для национальной безопасности в новой геополитической реальности²⁹. Злоумышленники всё чаще используют легальные коммерческие ИИ-модели в качестве инструментов вторжения.

Например, атака на водоканал в Мексике (декабрь 2025 – февраль 2026): хакеры использовали модели *Claude (Anthropic)* и *GPT (OpenAI)*. *Claude* применялся для планирования проникновения и разработки инструментов, а *GPT* – для аналитических задач и работы с испаноязычными документами³⁰.

При этом, согласно отчёту Европейского агентства по кибербезопас-

²⁴ Poland says Russian hackers targeted its energy grid in December. 10 January 2026 // URL: <https://www.reuters.com/world/europe/poland-says-russian-hackers-targeted-its-energy-grid-december-2026-01-10/>

²⁵ Polish water utilities hit by cyberattacks in 2025. 15 December 2025 // URL: <https://therecord.media/polish-water-utilities-cyberattacks-2025>

²⁶ Котова М. Пароль к периметру.

²⁷ Там же.

²⁸ Актуальные киберугрозы: итоги 2025 года. М.: Positive Technologies, 2026 // URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2025/>

²⁹ Convention against Cybercrime: strengthening international cooperation in combating certain crimes committed through information and communications technology and sharing electronic evidence in real time. N.Y.: United Nations, 2024. – 45 p.

³⁰ AI-Assisted Cyberattacks: Case Study of Mexico Water Utility. (December 2025 – February 2026). 2026 // URL: <https://www.recordedfuture.com/research/mexico-water-utility-ai-attack>

ности (ENISA), более 65% конфиденциальных цифровых коммуникаций остаются вне зоны досягаемости стандартных поисковых алгоритмов³¹. В то же время злоумышленники постоянно адаптируют свои стратегии, используя ИИ для повышения эффективности атак и манипулирования системами безопасности на основе ИИ³².

Взлом государственных и корпоративных систем с целью кражи информации, подмены данных или саботажа. Цель – получить доступ к конфиденциальной информации (личным данным граждан, государственным и военным секретам, коммерческим тайнам). Это может быть взлом баз данных, использование методов социальной инженерии (фишинг, спуфинг), эксплуатация уязвимостей (в том числе «нулевого дня»). В 2025–2026 гг. эта форма кибертерроризма превратилась в одну из главных угроз национальной безопасности. Основным трендом является переход от точечной кражи данных к полному уничтожению инфраструктуры и саботажу, при этом всё чаще используются технологии искусственного интеллекта.

В июне 2026 г. произошла атака на системы федеральных ведомств США (*SolarWinds*): хакеры, проникшие в системы через уязвимости в программном обеспечении *SolarWinds* и *Microsoft*, по-

хищили секретные данные о расследованиях американской контрразведки и санкционной политике.

Произошла утечка данных 70 тыс. французских госслужащих (*Tchap*), в результате кибератаки на приложение для обмена сообщениями *Tchap* могли быть похищены данные государственных служащих и до 643 тыс. сообщений³³.

В 2026 г. группировка *ShinyHunters* использовала критическую уязвимость «нулевого дня» в *Oracle PeopleSoft* (CVE-2026-35273) для взлома более 100 организаций по всему миру, включая Совет Европы и Университет Ноттингема, похитив более 297 Гб данных.

«Лаборатория Касперского» выявила продолжающуюся с начала 2025 г. кампанию кибершпионажа, организованную АPT-группой *Tomiris*. Основными целями атак были государственные учреждения и дипломатические службы в России и странах СНГ.

Государственные организации России стали главной мишенью для хакеров в 2025 г., на них пришлось 73% всех утечек данных в стране. Всего за отчётный период в сеть утекло более 145 млн строк данных. Атаки на структуры госсектора в первую очередь связаны с политической мотивацией хакеров³⁴.

Атаки на государственный сектор чаще всего вызывают сбои в основной деятельности организаций (48%), утечки данных (41%) и угрожают интересам государства (27%). Хакеры активно применяют фишинговые, ИИ- и OSINT-инструменты, изучая по открытым источникам сотрудников и инфраструктуру для подбора индивидуальных сценариев атак³⁵.

³¹ Cybersecurity and Data Protection in the Era of Encrypted Communications. Athens: ENISA, 2025. – 112 p.

³² Syllaidopoulos I., Ntalianis K.S., Salmon I.A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions // IEEE Access. 2025. Vol. 13. P. 1–32.

³³ Котова М. Пароль к периметру.

³⁴ Котова М. Кибератаки июня 2026: SolarWinds, Tchap, ShinyHunters, Tomiris и утечки в госсекторе России // Коммерсантъ. 2026. 25 июня.

³⁵ Маслов К.Н. OSINT в условиях цифрового суверенитета: методы, ограничения, перспективы.

Распространение вредоносного ПО (вирусов, троянов, программ-вымогателей). Эта форма кибер-терроризма предполагает создание и распространение ПО, специально разработанного для вывода из строя промышленного оборудования и технологических процессов. Одно и то же вредоносное ПО всё чаще используется как для кибершпионажа, так и для деструктивных атак, что стирает грань между этими видами деятельности.

В 2025 г. в России зафиксировано рекордное количество украденных учётных данных (около 2,86 млрд), включая данные из вредоносного ПО типа инфостилер, баз данных утечек и подпольных рынков³⁶.

В том же году – 7549 жертв программ-вымогателей по всему миру (на 45% выше, чем в 2024 г.), причём более 53% из них находились в США.

В июне 2026 г. червь *Miasma* скомпрометировал более 70 репозиторий компании *Microsoft* на платформе *GitHub*. Под удар попали проекты в организациях *Azure*, *Azure-Samples*, *Microsoft* и *MicrosoftDocs*. Атака началась с того, что злоумышленники получили доступ к учётной записи одного из контрибьюторов и добавили вредоносный коммит в репозиторий *Azure/durabletask*.

Одним из заметных примеров атак стала кампания кибершпионажа *DreamJob* 2025 г., которую проводила связанная с Северной Кореей группировка *Lazarus Group* против европейских компаний, производящих беспилотники и оборонные

комплектующие. В результате были похищены технические данные, что нанесло удар по военной безопасности нескольких стран³⁷.

Искусственный интеллект позволяет злоумышленникам автоматизировать генерацию и модификацию вредоносного кода, делая его менее заметным для традиционных антивирусных систем.

Дополнительно количество заражений операционной системы *macOS* увеличилось с менее чем 1000 случаев (2024 г.) до более чем 70 тыс. (2025 г.)³⁸. Кроме того, было зафиксировано вредоносное ПО *HONESTCUE*, использующее *API Google Gemini* для динамической генерации и выполнения вредоносного кода в памяти системы³⁹.

В конце декабря 2025 – начале января 2026 г. специалисты *BI.ZONE* обнаружили деятельность группировки *Forbidden Hyena*, которая применяла ИИ для атаки на российские госорганы, системы ЖКХ и здравоохранения⁴⁰.

Деструктивная пропаганда и вербовка через интернет. Интернет-пространство используется террористическими организациями для радикализации населения, вербовки новых членов и распространения пропаганды. Мессенджеры *Telegram* и *WhatsApp** являются основными инструментами для этого.

³⁶ HONESTCUE: AI-Assisted Malware Using Gemini API. 2026 // URL: <https://cloud.google.com/blog/products/security/honestcue-malware-gemini-api>

³⁷ Cyber Threat Report 2025: Ransomware, Data Breaches, and Cyber Espionage Trends. Singapore: Group-IB, 2026 // URL: <https://www.group-ib.com/resources/threat-research/2025-cyber-threat-report/>

³⁸ Malwarebytes. macOS Threat Report 2025. Santa Clara: Malwarebytes, 2026 // URL: <https://www.malwarebytes.com/resources/macOS-threat-report-2025>

³⁹ HONESTCUE: AI-Assisted Malware Using Gemini API. 2026.

⁴⁰ Котова М. Пароль к периметру.

* Мессенджеры Telegram и WhatsApp принадлежит Meta, которая признана экстремистской и запрещена на территории Российской Федерации на законодательном уровне.

В марте 2025 г. было зафиксировано 294 аккаунта вербовщиков в *Telegram*, а к маю их число превысило тысячу.

Злоумышленники вступают в игровые чаты, заводят контакт, создают иллюзию дружбы. Они используют игровые механики (прокачка, награды, достижения), чтобы сформировать чувство принадлежности к группе. Игровые платформы *Discord*, игровые чаты в *Counter-Strike*, *PUBG*, *Fortnite*, а также «песочницы» вроде *Roblox* и *Minecraft* стали новой серой зоной для радикализации⁴¹.

В 2025 г. 78% попыток вовлечения молодёжи в деструктивные группы стартовали именно через эти каналы. В 2026 г. антитеррористический центр Казахстана предупредил о новой волне вербовки подростков через видеоигры. Террористическая организация «Исламское государство»* активизировала вербовку в интернете, делая ставку на молодёжь. После потери территорий в Сирии и Ираке группировка перешла к модели скрытой электронной вербовки, используя современные технологии.

Так, франкоязычный международный телеканал *TV5 Monde* подвергся масштабной кибератаке: хакеры, заявившие о связи с террористической группировкой ИГ, заблокировали трансляцию 11 каналов, взломали сайт и аккаунты в социальных сетях, включая *Facebook*, в которых появились

фотографии людей в чёрной одежде с подписью «Киберхалифат» и «Я – ИГ».

Этот инцидент продемонстрировал, что кибертерроризм может быть использован не только для дестабилизации инфраструктуры, но и для прямого захвата медийного пространства с целью распространения идеологии и запугивания широкой аудитории.

Деструктивная пропаганда и вербовка в интернете превратились в высокоорганизованную индустрию, угрожающую национальной безопасности. Используя уязвимости людей и несовершенство модерации на многих платформах, вербовщики эффективно вовлекают граждан в экстремистскую деятельность, что напрямую ведёт к росту числа как киберпреступлений, так и реальных террористических атак.

Одновременно были представлены данные об активном использовании нейросетей и чат-ботов для вербовки, агитации, совершения кибертерроризма⁴².

Нарушение работы и захват каналов связи, СМИ и распространение дезинформации. В последние годы кибератаки на СМИ и телекоммуникационную инфраструктуру стали важным инструментом гибридной войны. Злоумышленники используют взлом каналов вещания для распространения дезинформа-

⁴¹ Голубова В.И., Жук М.Г. Уголовно-правовые и процессуальные механизмы борьбы с кибертерроризмом, осуществляемым с применением искусственного интеллекта // Nextgen-наука глазами молодёжи: искусственный интеллект и междисциплинарные решения. Материалы XVII Междунар. науч.-практ. конф. обучающ., посвящ. Году цифровизации и искусственного интеллекта, Семей, 19 марта 2026 г. Семей: Alikhan Bokeikhan University, 2026. С. 114–117.

⁴² Холов С.Х. Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений.

* Террористическая организация, деятельность которой на территории Российской Федерации запрещена на законодательном уровне.

ции и пропаганды, а также применяют методы *swatting* – ложные вызовы экстренных служб для нарушения работы СМИ⁴³. Эта форма направлена на дестабилизацию общества через распространение дезинформации, фейковых новостей и манипуляцию поведением людей для того, чтобы транслировать ложные сведения, слухи, пропаганду, предъявлять свои требования. Цель – посеять панику в обществе, повлиять на общественное мнение. Сюда же можно отнести создание и распространение дипфейков.

Одним из самых масштабных захватов эфира произошёл 24 августа 2025 г., когда был взломан российский провайдер украинскими киберподразделениями, которые вывели на 116 телеканалах видеоролик о потерях Российской армии. Трансляция продолжалась более трёх часов в вечерний прайм-тайм, видео увидели не менее 50 тыс. абонентов Москвы и других регионов. Кибертеррористы заблокировали доступ администраторов провайдера к серверу, чтобы затруднить прерывание трансляции.

В мае 2026 г. польская полиция расследовала крупномасштабную кибератаку на сотрудников правого телеканала *TV Republika*. Злоумышленники отправили в полицию ложные сообщения о

том, что по адресам сотрудников канала находятся дети в опасности и есть взрывчатка. Личные данные и *email*-аккаунты были взломаны и использованы для сокрытия следов преступников.

Кибератаки на СМИ всё чаще сочетают технический взлом (отключение эфира, удаление баз данных) с психологическим воздействием (дезинформация, угрозы, паника), что делает их особенно опасными для национальной безопасности. Дипфейки стали мощным инструментом пропаганды и психологического воздействия. Возможность фальсифицировать и манипулировать аудио- и видеоматериалами с использованием ИИ угрожает целостности информации, усиливает поляризацию и может спровоцировать дипломатические кризисы⁴⁴.

В настоящее время кибертерроризм – это не одна изолированная атака, а комбинация.

Например, сначала идёт фишинговая рассылка с вредоносным вложением, затем вредоносное ПО проникает в систему, после чего злоумышленники используют захваченный канал для распространения дезинформации и одновременно угрожают дальнейшей атакой, если не будет выплачен выкуп.

Угроза кибертерроризма в новой геополитической реальности

Кибертерроризм стал повсеместной глобальной угрозой, выходящей за пределы национальных границ и угрожающей критической инфраструктуре, национальной безопасно-

сти и международному миру. Развитие интернета вещей, искусственного интеллекта и цифровой взаимосвязанности предоставляет террористическим организациям новые возмож-

⁴³ Cybersecurity and Data Protection in the Era of Encrypted Communications.

⁴⁴ Савушкина М.А. Ментальный терроризм как метод ведения гибридной войны в цифровом обществе.

ности для анонимных и эффективных действий⁴⁵.

Согласно данным *ENISA*, в 2025 г. доля атак на субъекты КИИ выросла с 47% в 2023 г. до 64% в 2024 г.⁴⁶

В настоящее время можно выделить четыре ключевых фактора, усиливающих угрозу кибертерроризма в современных условиях.

Во-первых, геополитическая напряжённость: обострение отношений между государствами переводит киберугрозы в новую фазу, когда кибератаки становятся инструментом политического давления и элементом гибридных конфликтов. Стороны могут использовать киберпространство для нанесения ущерба оппоненту, не прибегая к прямому военному столкновению.

Во-вторых, анонимность и трансграничность: киберпространство не знает границ, что позволяет злоумышленникам действовать из любой точки мира, усложняя идентификацию и привлечение к ответственности. В условиях политизации международных отношений это ещё больше затрудняет сотрудничество в расследовании.

В-третьих, технологическое развитие: злоумышленники активно внедряют новые инструменты, включая искусственный интеллект для автоматизации поиска уязвимостей, генерации фишинговых сообщений или создания дипфейков.

В-четвёртых, рост зависимости от цифровых технологий: чем больше сфер жизни опирается на цифровые системы, тем выше потенциальный ущерб от успешной атаки.

Противодействие кибертерроризму

Борьба с кибертерроризмом с учётом трудностей, возникающих при противодействии ему, включает несколько проблем:

- отсутствие единого международного определения. На глобальном уровне нет консенсуса, что именно считать кибертерроризмом, а что – киберпреступностью или кибервойной;

- отсутствие консенсуса в определении кибертерроризма затрудняет

выработку общих правовых норм и механизмов взаимодействия⁴⁷. Международное право в области кибертерроризма сталкивается с серьёзными вызовами из-за отсутствия единой дефиниции, и существующие региональные инициативы, такие как Будапештская конвенция о киберпреступности (2001 г.), имеют ограничения по географии и не охватывают специфику кибертерроризма⁴⁸;

⁴⁵ Ransomware Report 2025: Trends and Statistics. N.Y.: Chainalysis, 2026 // URL: <https://www.chainalysis.com/ransomware-2025/>

⁴⁶ Cybersecurity and Data Protection in the Era of Encrypted Communications.

⁴⁷ Холов С.Х. Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений.

⁴⁸ Diwaker S. Cyber-Terrorism and the Changing Definition of Terrorism: Prospects for India in International Law.

– сложность расследований. Удалённость преступника, использование сложных технических приёмов и необходимость взаимодействия разных юрисдикций осложняют поиск и доказательство вины;

– необходимость комплексного подхода. Эффективное противодей-

ствие требует не только технических мер (например, защита инфраструктуры, внедрение безопасных решений и т. д.), но и работы в правовой, информационной и психологической сферах, включая многоуровневое международное сотрудничество.

Борьба с кибертерроризмом

Для результативной борьбы с кибертерроризмом необходимо применять комплексные меры на государственном, корпоративном и индивидуальном уровнях.

Совершенствование и внедрение технических мер. Представляется целесообразным использование и внедрение следующих технических мер по противодействию кибертерроризму:

– инструменты для своевременного выявления и оперативной блокировки террористических ресурсов путём внедрения аналитических систем и автоматизированных аппаратно-программных комплексов мониторинга национального сегмента интернета;

– решения по противодействию использованию пользователями интернета средств обеспечения анонимности в преступных целях (прокси-серверы различных видов, SSH-туннели, TOR, VPN-сервисы и др.). Борьба с ними возможна как глобальным запретом и блокировкой систем анонимизации пользовате-

лей («Великий китайский файервол»), так и привлечением к ответственности виновных в создании и распространении таких средств;

– информационные системы на основе технологий ИИ, позволяющие анализировать большие объёмы информации (IP-адреса, история активности, различная вторичная информация и сведения) и с высокой степенью вероятности устанавливать личность пользователя;

– инструменты для отслеживания денежных потоков, в том числе криптовалютных операций, используемых для финансирования деятельности кибертеррористов⁴⁹;

– технологические решения, эксплуатирующие уязвимости сайтов и сетей с целью определения IP-адресов пользователей и иных данных, обеспечивающих идентификацию преступников.

Технологии прогнозной аналитики, обработки естественного языка и машинного обучения значительно повышают возможности обнаружения угроз, но при этом вызывают серьёзные проблемы, связанные с

⁴⁹ Меркурьев В.В., Боброва О.В. Финансирование террористической и иной противоправной деятельности. Правовая характеристика. Часть 2. Новое в российском законодательстве по противодействию террористической и диверсионной деятельности // Обозреватель–Observer. 2026. № 4. С. 139–161.

алгоритмической предвзятостью, качеством данных и управленческими вызовами⁵⁰.

Расширение международного сотрудничества и разработка эффективной правовой базы. В условиях новой геополитической реальности, когда кибертерроризм превратился в системный фактор дестабилизации, международное сотрудничество выходит на принципиально новый уровень.

Так, принятая Генеральной Ассамблеей ООН (24 декабря 2024 г.) и подписанная представителями 71 страны (25 октября 2025 г., Ханой, Вьетнам) Конвенция ООН против киберпреступности стала первым глобальным многосторонним договором, посвящённым борьбе с киберпреступностью⁵¹. Она устанавливает единые правовые стандарты для государств в сфере предотвращения, выявления, расследования и преследования преступлений, совершённых с использованием информационно-коммуникационных технологий.

Документ закладывает правовую основу для обмена электронными доказательствами в режиме реального времени, экстрадиции преступников и совместных мер по противодействию легализации криминальных доходов. Он направлен на установление общих составов преступлений и процессуальных полномочий, а также на лишение безопасного убежища тех, кто вовлечён в киберпреступность. Конвенция закладывает правовую основу для обмена электронными доказательствами

ми в режиме реального времени и экстрадиции преступников.

Одновременно с этим в рамках глобальной контртеррористической деятельности по кибербезопасности и новым технологиям принята программа *CT TECH+*, инициированная Управлением ООН по противодействию терроризму (*UNOCT*) и Интерполом. Финансирование обеспечивается Европейским союзом со сроком реализации: январь 2025 г. – декабрь 2026 г. Цель программы – укрепление потенциала правоохранительных органов государств-партнёров в противодействии использованию новых технологий в террористических целях.

Параллельно развивается региональное сотрудничество.

Так, 20 ноября 2025 г. прошёл второй структурированный диалог ЕС и НАТО по кибербезопасности, на котором стороны обсудили инициативы по усилению способности обнаруживать, сдерживать и защищаться от вредоносной кибердеятельности, а также вопросы повышения киберустойчивости и готовности.

Ключевым достижением стало оформление (май 2026 г.) соглашения киберпартнёрства НАТО с тремя ведущими ИТ-компаниями (*Microsoft*, *Palo Alto Networks* и *ESET*). Эти некоммерческие стратегические партнёрства направлены на обмен разведывательной информацией и укрепление коллективной киберобороны.

В октябре 2025 г. в Таджикистане прошла Третья конференция СНГ по борьбе с терроризмом и экстремизмом с участием более 150 представителей. Участники договорились о запуске Сети раннего

⁵⁰ Syllaidopoulos I., Ntalianis K.S., Salmon I.A Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions.

⁵¹ Convention against Cybercrime: strengthening international cooperation in combating certain crimes committed through information and communications technology and sharing electronic evidence in real time.

предупреждения в Центральной Азии, чтобы оперативнее обмениваться сигналами о киберугрозах.

Весной 2025 г. в Санкт-Петербурге прошла международная конференция по противодействию использованию искусственного интеллекта и новых технологий в террористических целях с участием более 100 представителей из 22 международных организаций. В её итоговом документе зафиксировано, что неправомерное использование ИИ создаёт «беспрецедентные правовые, этические и оперативные проблемы».

В России внесены изменения в Федеральный закон «О противодействии экстремистской деятельности»⁵², которые запрещают использование интернета для осуществления экстремистской деятельности. Также рассматриваются законопроекты, обязывающие операторов связи отключать любую связь по запросу ФСБ при угрозах безопасности.

Организация должного межведомственного взаимодействия органов исполнительной власти с общественными организациями и объединениями, т. е. создание площадок для выработки стратегических решений.

Примером служит Межведомственная комиссия Совета Безопасности РФ по общественной безопасности, которая определяет дополнительные меры по противодействию

преступлениям с использованием *IT-технологий*.

На региональном уровне проводятся координационные совещания с участием территориальных органов федеральной власти и межведомственные рабочие группы для выработки конкретных мер.

Одновременно с этим организуется сотрудничество с *IT-компаниями* и некоммерческими организациями, например, МВД России и АНО «Диалог Регионы» совместно проводят мониторинг публичного поля для выявления деструктивного контента и мошеннических схем.

С начала 2026 г. аналитики зафиксировали уже порядка 500 опасных информационных поводов.

Также создаются профессиональные сообщества для обмена опытом.

Так, в Астраханской области в этом году запущено первое в стране профессиональное сообщество *IT-специалистов* по информационной безопасности из органов власти.

Повышение уровня осведомлённости сотрудников компаний организаций и граждан о методах кибертеррористов, обучение их действиям в случае угрозы и при реализации таких атак. Необходимо обучение их действиям в случае угрозы и при реализации таких атак.

Проведённый анализ позволяет утверждать, что современный кибертерроризм представляет собой стремительно эволюционирующую угрозу, характеризующуюся постоянным усложнением тактик (таких как цепочки поставок и атаки «нулевого дня»), появлением новых высокоэффективных векторов атак (включая эксплойты для IoT и облачных сред) и трансформацией мотивации от идеологической до геополитической и финансовой.

⁵² Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // URL: <http://www.kremlin.ru/acts/bank/18939>

Анализ текущих тенденций (рост целевых атак на критическую инфраструктуру, масштабирование программ-вымогателей, использование ИИ злоумышленниками) и возникающих угроз (потенциал квантовых вычислений для взлома шифрования, использование *deepfake-технологии*) вместе с моделированием будущих сценариев однозначно указывает на критическую необходимость формирования и имплементации стратегии по противодействию кибертерроризму, предусматривающей комплексную реализацию мер технического, юридического и социального характера как на национальном, так и международном уровне.

В новых геополитических реалиях кибертерроризм перестал быть просто технической проблемой – он стал инструментом стратегического давления. Поэтому обеспечение кибербезопасности и защита критической информационной инфраструктуры сегодня – один из ключевых элементов стратегии национальной безопасности любого государства. Именно сочетание технологических, правовых и организационных решений, дополненное повышением цифровой грамотности населения, способно сформировать устойчивую систему противодействия кибертерроризму в долгосрочной перспективе.

Ключевая проблема: требуется найти баланс между необходимостью защиты и сохранением открытости цифрового пространства с выстраиванием эффективных механизмов международного взаимодействия.

Библиография

- Актуальные киберугрозы: итоги 2025 года. М.: Positive Technologies, 2026 // URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2025/>
- Закон Китайской Народной Республики о борьбе с терроризмом от 27 декабря 2015 г. (Counter-Terrorism Law of the People's Republic of China) (принят на 18-й сессии ПК ВСНП 12-го созыва) // URL: https://www.spp.gov.cn/tt/201512/t20151228_109920.shtml
- Маслов К.Н. OSINT в условиях цифрового суверенитета: методы, ограничения, перспективы // Журнал международного права и информационной безопасности. 2024. Т. 12. № 3. С. 45–62.
- Меркурьев В.В., Боброва О.В. Финансирование террористической и иной противоправной деятельности. Правовая характеристика. Часть 2. Новое в российском законодательстве по противодействию террористической и диверсионной деятельности // Обозреватель–Observer. 2026. № 4. С. 139–161.
- Побегайло А.Э. Киберэкстремизм – угроза национальной безопасности // Обозреватель–Observer. 2025. № 5. С. 105–119.
- Постановление Конституционного Суда РФ от 25 сентября 2014 г. № 2055-О // URL: <https://normativ.kontur.ru/document?moduleId=7&documentId=242563#lo>
- Постановление Конституционного Суда РФ от 31 марта 2022 г. № 804-О // <https://normativ.kontur.ru/document/7/422237-opredelenie-konstitutsionnogo-suda-rf-ot-31-03-2022-n-804-o>
- Савушкина М.А. Ментальный терроризм как метод ведения гибридной войны в цифровом обществе // Вестник Челябинского государственного университета. 2024. № 7. С. 48–54.

- Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28.04.2023). Статья 361 «Акт международного терроризма» // URL: https://www.consultant.ru/document/cons_doc_LAW_10699/0994b72ccab34fae773ced2c837691518a3e3dca/
- Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // URL: <http://www.kremlin.ru/acts/bank/18939>
- Холов С.Х. Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений // Вестник МГУИУ. 2025. № 1. С. 41–52.
- 18 U.S.C. § 2331 // Definitions (United States Code). Title 18. Part I. Chapter 113B // URL: <https://www.law.cornell.edu/uscode/text/18/2331>
- Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (as amended by Council Framework Decision 2008/919/JHA) // Official Journal of the European Union, L 164, 22.6.2002. P. 3–7 // URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002Fo475>
- Diwaker S.* Cyber-Terrorism and the Changing Definition of Terrorism: Prospects for India in International Law // International Journal of Law Management & Humanities. 2026.
- Krisnayanto Suryadi.* Exploring the Dark Horizon: Artificial Intelligence (AI) as Cyberterrorism Tools // Journal of Terrorism Studies. 2025. Vol. 7. № 1.
- Montasari R.* Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution: Threats, Assessment and Responses. Cham: Springer NATURE Switzerland AG, 2024. – 270 p.
- Syllaidopoulos I., Ntalianis K.S., Salmon I.A* Comprehensive Survey on AI in Counter-Terrorism and Cybersecurity: Challenges and Ethical Dimensions // IEEE Access. 2025. Vol. 13. P. 1–32.
- Trifunović D.* Intelligence and Counterterrorism // National Security and The Future. 2025. Vol. 26. № 1. P. 179–192.

Статья поступила в редакцию 15 июля 2026 г.

Статья принята к публикации 23 июля 2026 г.

Уважаемые читатели!
Открыта подписка на 2027 год
на ежемесячный научно-аналитический журнал

«Обозреватель–Observer»

Подписка проводится:

- для корпоративных подписчиков «УП Урал-Пресс» по электронному каталогу на сайте **www.ural-press.ru**
- для индивидуальных подписчиков Агенством подписки «Деловая пресса» по электронному каталогу на сайте **<https://delpress.ru/catalog/>**
 тел.: +7-495-951-22-25