Дата поступления рукописи в редакцию: 27.05.2026 г.
Дата принятия рукописи в печать: 19.06.2026 г.
DOI: 10.24412/2224-9133-2026-5-53-58

ГАДЖИЭМЕНОВ Багавдиншайих Абдулкадирович,
кандидат юридических наук, доцент,
руководитель НИЦ по изучению правовых проблем
противодействия экстремизму, терроризму и коррупции
Юридического института Дагестанского государственного университета,
доцент кафедры уголовного права и криминологии, старший советник юстиции,
Заслуженный юрист Республики Дагестан,
член правления ДРОО «Поддержка курса Главы Республики Дагестан»,
e-mail: mail@law-books.ru

КИБЕРТЕРРОРИЗМ КАК НОВАЯ УГРОЗА: ОСОБЕННОСТИ, КАНАЛЫ РАСПРОСТРАНЕНИЯ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация. *Статья посвящена комплексному анализу кибертерроризма как качественно новой и стремительно эволюционирующей угрозы национальной и международной безопасности. Автором выявлены и проанализированы ключевые особенности кибертерроризма, среди которых: анонимность, дистанционность, низкая себестоимость атаки при потенциально высоком деструктивном эффекте, сложность атрибуции, а также мультипликативный пропагандистский эффект. Детально рассмотрены основные каналы распространения данной угрозы в современном киберпространстве – от открытых социальных сетей до закрытых сегментов даркнета и мессенджеров. На основе критического анализа доктринальных позиций ведущих российских и зарубежных исследователей, а также актуального состояния отечественного законодательства, обоснован комплексный подход к противодействию кибертерроризму. Предлагаются конкретные меры правового, организационно-технического и международно-правового характера, формулируются предложения по совершенствованию уголовного законодательства.*

Ключевые слова: *кибертерроризм, информационная безопасность, киберпространство, каналы распространения, даркнет, социальные сети, противодействие терроризму, уголовное законодательство, критическая информационная инфраструктура.*

GADZHIEMENOV Bagavdinshaiykh Abdulkadirovich,
Candidate of Legal Sciences, Associate Professor, Head of the Research
Center for the Study of Legal Problems of Countering Extremism,
Terrorism and Corruption, Law Institute, Dagestan State University,
Associate Professor of the Department of Criminal Law and Criminology,
Senior Counselor of Justice, Honored Lawyer of the Republic of Dagestan,
Board Member of the Dagestan Regional Public Organization
“Support for the Course of the Head of the Republic of Dagestan”

CYBERTERRORISM AS A NEW THREAT: FEATURES, DISTRIBUTION CHANNELS AND COUNTERMEASURES

Annotation. *The article is devoted to a comprehensive analysis of cyberterrorism as a qualitatively new and rapidly evolving threat to national and international security. The author identifies and analyzes the key features of cyberterrorism, including anonymity, remoteness, low cost of an attack with a potentially high destructive effect, the difficulty of attribution, and a multiplier propaganda effect. The main channels for the spread of this threat in modern cyberspace are examined in detail – from open social networks to closed segments of the darknet and messengers. Based on a critical analysis of the doctrinal positions of leading Russian and foreign researchers, as well as the current state of domestic legislation, a comprehensive approach to countering cyberterrorism is substantiated. Specific measures of a legal, organizational-technical and international legal nature are proposed, and proposals for improving criminal legislation are formulated.*

Key words: *cyberterrorism, information security, cyberspace, distribution channels, darknet, social networks, countering terrorism, criminal law, critical information infrastructure.*

Стремительное развитие информационно-коммуникационных технологий, выступая фундаментом современного «цифрового общества», сформировало принципиально новую среду для реализации как законных, так и противоправных интересов. Киберпространство, лишенное государственных границ и во многом свободное от традиционных форм социального контроля, стало ареной острого противостояния, в котором все более заметное место занимает кибертерроризм – гибридное явление, соединившее разрушительную идеологию терроризма с колоссальным потенциалом информационных технологий. Актуальность глубокого научного осмысления данного феномена обусловлена целым рядом тревожных тенденций. Во-первых, налицо экспоненциальный рост числа и изощренности атак на объекты критической информационной инфраструктуры (КИИ): по данным экспертов, только за 2025 год количество инцидентов с использованием программ-вымогателей увеличилось на 15%, причем значительная их часть уже не укладывается в рамки обычной киберпреступности, обнаруживая явные признаки диверсионной и политической мотивации [8]. Во-вторых, транснациональные террористические организации превратили цифровую среду в основной инструмент пропаганды, вербовки, финансирования и координации, что качественно повысило их живучесть и оперативные возможности. В-третьих, мировая практика демонстрирует все более активное вовлечение прогосударственных хакерских группировок в гибридные конфликты, размывающих грань между кибершпионажем, диверсией и собственно актами кибертерроризма. Несмотря на очевидную остроту проблемы, в юридической науке и правоприменительной практике до сих пор не выработано единого подхода к дефиниции «кибертерроризм», что существенно затрудняет как законотворческую деятельность, так и практическое противодействие этой угрозе.

Формирование эффективной государственной политики противодействия любой угрозе неразрывно связано с ее точной терминологической фиксацией. Однако именно в отношении кибертерроризма как в отечественной, так и в зарубежной науке сложился широкий плюрализм мнений, обусловленный многогранностью самого феномена. Анализ доктрины позволяет выделить два магистральных подхода: узкий (строгий) и широкий. Сторонники узкого подхода, у истоков которого стояли такие исследователи, как Д. Деннинг и М. Поллит, а в российской науке его отчасти разделяет В. А. Мазуров, стремятся отграничить кибертерроризм от смежных явлений. С их точки зрения, кибертерроризм – это непременно атака именно на компьютерные системы, сети и обрабатываемую в них информацию, которая создает реальную опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных тяжких общественно опасных последствий, осуществляемая для устрашения населения или воздействия на органы власти [3, с. 149]. Достоинством данного подхода является высокая степень формальной определенности, позволяющая минимизировать риски расширительного толкования. Вместе с тем, он оставляет за рамками целый пласт террористической активности, которая хотя и не сопряжена с непосредственным разрушительным воздействием на киберфизические системы, но является неотъемлемой частью террористической деятельности – пропаганду, радикализацию, рекрутинг, сбор финансовых средств.

Данный пробел восполняется представителями широкого подхода, который в российской науке активно разрабатывается Л. А. Бураевой, Б. А. Тарчоковым, А. А. Шпаком. Эти ученые исходят из того, что кибертерроризм охватывает любое использование киберпространства в целях, свойственных терроризму, будь то непосредственные атаки на инфраструктуру или же обеспечивающая деятельность. Как справедливо подчеркивает Л. А. Бураева, возможности глобальной сети «все чаще используются террористическими группировками не только для совершения хакерских кибератак, но и для устрашения общества, проведения антиобщественной пропаганды, вербовки, распространения планов возможных террористических атак, в разведывательных целях» [1, с. 147]. Действительно, современные реалии таковы, что виртуальная ячейка, члены которой никогда не встречались в физическом мире, может спланировать и осуществить реальный теракт, а пропагандистский ролик, распространенный через соцсети, способен радикализировать сознание человека и подтолкнуть его к преступным действиям. Следовательно, ценность широкого подхода заключается в его прагматизме и нацеленности на охват всего спектра угроз, хотя его критики и высказывают обоснованные опасения относительно размывания границ состава преступления.

Наиболее взвешенной и пригодной для целей законотворчества представляется попытка синтеза, предложенная Д. В. Пучковым, который определяет «кибертерроризм как «противоправное использование информационно-коммуникативных технологий в отношении компьютерной информации, компьютерных систем и сетей в критических сегментах государства и в частном секторе, которые создают опасность гибели людей, причинения значительного имущественного ущерба или наступления иных общественно опасных последствий, с целью нагнетания страха

и напряженности, а равно воздействия на органы власти по политическим или иным, свойственным идеологии терроризма, мотивам» [4, с. 385]. Именно такой подход, акцентирующий внимание на объекте, целях и мотивах деяния, позволяет непротиворечиво вписать кибертерроризм в систему уголовно-правовых запретов и отграничить его от киберпреступности, хактивизма и кибершпионажа. С учетом этого, мы полностью разделяем позицию А. И. Диденко, что «в авангарде борьбы с кибертерроризмом должно быть уголовное право» [2, с. 92], однако отправной точкой здесь должно стать не доктринальное толкование, а четкая легальная дефиниция, закрепленная в федеральном законе. Лишь на этом фундаменте можно выстроить логичную и непротиворечивую систему мер противодействия.

Закономерным следствием неоднородности подходов к определению является и отсутствие в науке и практике единой системы свойств, которые бы всесторонне характеризовали кибертерроризм как угрозу нового типа. Проведенный в рамках настоящей работы анализ позволяет выделить и детально обосновать несколько ключевых особенностей, совокупность которых придает данному явлению качественную новизну. Первой и, пожалуй, системообразующей особенностью выступает абсолютная анонимность и дистанционность. В отличие от традиционного терроризма, где исполнитель физически присутствует на месте преступления, кибертеррорист может находиться в тысячах километров от объекта атаки, в юрисдикции другого государства, используя цепочки прокси-серверов, VPN-сервисы и зашифрованные каналы связи. Это не просто затрудняет идентификацию злоумышленника, а в корне подрывает один из базовых принципов уголовного права – принцип неотвратимости наказания. Как точно замечено в литературе, «киберпространство не имеет границ, что позволяет террористам действовать вне национальной юрисдикции» [1, с. 151], а следовательно, и вне досягаемости для национальных правоохранительных систем без сложных и долгосрочных международных процедур. Вторая особенность – беспрецедентная асимметрия между затратами на атаку и ее потенциальным ущербом. Если подготовка и проведение классического теракта, как правило, требует значительного финансирования, логистики и человеческого ресурса, то разрушительная кибератака может быть осуществлена одним человеком или небольшой группой при минимальных затратах на оборудование и программное обеспечение. При этом ущерб для экономики и общества может достигать астрономических сумм. Согласно прогнозам экспертов, глобальный ущерб от киберпреступности, в которую органично встроена и кибертеррористическая деятельность, в 2026 году может достичь 11,9 трлн долларов [9]. Эта пугающая экономика делает кибертерроризм крайне привлекательным инструментом для асимметричного давления на государства. Третья особенность, тесно связанная с первой, – это колоссальная сложность атрибуции, то есть установления не только конкретного исполнителя, но и источника атаки, заказчика, его политической или государственной принадлежности. Современные технологии позволяют фальсифицировать цифровые следы, имитировать деятельность одной группировки от имени другой, оставляя реальных организаторов в тени. Данное обстоятельство превращает кибертерроризм в идеальное орудие ведения гибридных войн, когда агрессор, оставаясь формально непричастным, может наносить критический урон противнику, дестабилизируя его финансовую систему, энергетику и транспорт. Четвертая особенность, кардинально меняющая природу устрашения, – мультипликативный пропагандистский эффект. Кибертеррорист, в отличие от террориста традиционного, не зависит от СМИ как посредника для распространения информации о своих действиях. Он самостоятельно, напрямую, в режиме реального времени может донести информацию об успешной атаке до многомиллионной аудитории, сопроводив ее собственными комментариями и угрозами, что многократно усиливает психологический эффект и создает в обществе атмосферу паники и недоверия к государственным институтам. Пятой особенностью является перманентная технологическая эволюция инструментария атак, напоминающая гонку вооружений. Киберпреступные и террористические группы активно заимствуют новейшие достижения в области искусственного интеллекта, квантовых вычислений и, что особенно опасно, используют бизнес-модель «вредоносное ПО как услуга» (Malware-as-a-Service), делая сложнейший инструментарий доступным даже для непрофессионалов. Это ведет к постоянному сокращению времени между появлением уязвимости и ее использованием в атаках, требуя от государства и бизнеса столь же быстрой реакции. Наконец, шестой, часто недооцениваемой особенностью, является изощренная эксплуатация «человеческого фактора». Как показывают исследования, подавляющее большинство успешных атак на защищенные системы начинается не со взлома сложных алгоритмов шифрования, а с использования методов социальной инженерии, фишинга и психологических манипуляций в отношении конкретных сотрудников [5, с. 44]. Таким образом, самым уязвимым звеном любой, даже самой технологически совершенной системы защиты, остается человек, что выводит проблему кибертерроризма далеко за пределы

сугубо технических вопросов и делает ее комплексной социальной и правовой проблемой.

Понимание указанных особенностей невозможно без детального анализа той цифровой экосистемы, в которой зарождается, вызревает и реализуется кибертеррористическая угроза. Данная экосистема имеет ярко выраженный многоуровневый характер, и каждый из ее уровней выполняет свои специфические задачи в общей преступной стратегии. Первый, самый доступный уровень – поверхностный веб – является основным плацдармом для пропаганды и вербовки. Социальные сети, видеохостинги, новостные агрегаторы используются террористическими группами для распространения радикального контента, адресованного максимально широкой аудитории. Несмотря на все усилия администраций цифровых платформ по модерации, радикалы постоянно совершенствуют методы обхода блокировок, используя эзопов язык, «однодневные» аккаунты, закрытые сообщества и прямые трансляции. Здесь происходит первичная радикализация, выявление потенциальных сторонников и их мягкое вовлечение в орбиту террористической деятельности. Второй, более глубокий уровень – глубинный веб – служит целям защищенной коммуникации и координации. На этом уровне царит культ шифрованной связи, и ключевую роль здесь играют мессенджеры со сквозным шифрованием, в первую очередь Telegram. Как верно констатирует А. А. Шпак, с помощью данного инструмента «преступники могут общаться, вербовать соучастников, обучать их, создавать так называемые спящие ячейки террористических группировок» [6, с. 89]. Технология шифрования создает практически непреодолимые правовые и технические препятствия для правоохранительных органов, делая перехват сообщений невозможным без физического доступа к устройству одного из участников переписки, что на порядок усложняет и замедляет оперативно-розыскную деятельность. Наконец, третий, самый глубокий и скрытый уровень – теневой веб, или даркнет, – представляет собой своего рода «черный рынок» и штаб-квартиру киберпреступного мира. Доступный только через специализированное программное обеспечение, он обеспечивает практически полную анонимность. Именно даркнет, по обоснованному мнению экспертов, стал «рассадником киберпреступлений со стороны негосударственных субъектов» [7]. Здесь функционируют анонимные торговые площадки, где можно приобрести оружие, наркотики, вредоносное ПО, базы украденных данных, а также нанять хакеров для совершения целевых атак. Террористические организации используют даркнет для сбора пожертвований в криптовалюте, безопасного общения без риска деанонимизации и детального планирования будущих операций. Именно этот сегмент, в силу своей децентрализации и опоры на самые передовые технологии анонимизации, представляет наибольшую сложность для оперативного мониторинга и является основным источником наиболее опасных киберугроз.

Многоуровневый и комплексный характер описанной угрозы однозначно свидетельствует, что эффективное противодействие кибертерроризму не может быть сведено к реализации какой-то одной, пусть даже самой совершенной меры. Только системный, строго сбалансированный подход, гармонично сочетающий правовые, организационно-технические, идеологические и международные инструменты, способен дать адекватный ответ на этот вызов. В этом контексте отправной точкой должно стать кардинальное совершенствование национального законодательства. В настоящее время российское право, несмотря на наличие целого ряда норм в Уголовном кодексе РФ (ст. 205, 272, 273, 274.1 и др.), не содержит ни легальной дефиниции кибертерроризма, ни специального состава преступления. На практике это приводит к тому, что общественно опасные деяния, обладающие всеми признаками акта кибертерроризма, квалифицируются либо как совокупность общих террористических и компьютерных преступлений, либо как диверсия, что не отражает их истинной сущности и не позволяет применять адекватный комплекс профилактических мер. Хотя, как отмечается в литературе, существующая система норм и позволяет привлекать злоумышленников к ответственности [2, с. 93], подобная практика «лоскутной» квалификации противоречит принципу законности, усложняет статистический учет и не создает понятных правовых ориентиров для общества.

В этой связи представляется настоятельно необходимым реализовать ряд конкретных законодательных шагов. Во-первых, следует внести изменения в базовый Федеральный закон «О противодействии терроризму» от 6 марта 2006 г. № 35-ФЗ, дополнив его понятийный аппарат определением кибертерроризма, основанным на синтезе широкого и узкого подходов. Во-вторых, и это является логическим завершением первого шага, следует рассмотреть вопрос о введении в главу 24 УК РФ «Преступления против общественной безопасности» самостоятельной статьи «Совершение акта кибертерроризма». В диспозиции данной нормы необходимо отразить все сущностные признаки деяния, включая цель устрашения населения и воздействия на органы власти, а также особый предмет посягательства – критическую информационную инфраструктуру Российской Федерации. Подобная новелла

позволит систематизировать судебную практику, точно отграничить данное преступление от смежных составов и, что не менее важно, запустит механизм включения субъектов, привлекаемых к ответственности по данной статье, в соответствующие реестры и списки, даст правовые основания для применения в их отношении специальных мер профилактики. В-третьих, заслуживает пристального внимания и поддержки предложение Д. В. Пучкова о необходимости дополнения ст. 274.1 УК РФ особо квалифицирующим признаком и дачи соответствующих разъяснений на уровне Постановления Пленума Верховного Суда РФ [4, с. 389]. В-четвертых, в русле актуальных законодательных трендов логичной выглядит инициатива о нормативном приравнивании ряда особо опасных киберпреступлений к террористической деятельности в контексте применения профилактических мер. Это откроет дорогу для использования в отношении киберпреступников всего арсенала средств, предусмотренных антитеррористическим законодательством, от постановки на профилактический учет до контроля за их цифровыми транзакциями.

Однако было бы глубоким заблуждением полагать, что одними лишь правовыми запретами можно решить проблему, коренящуюся в технической и социальной сферах. Не менее важен блок организационно-технических мер, который должен базироваться на принципе системности и непрерывности. Ключевым здесь является дальнейшее развитие и укрепление государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. Необходимо обеспечить не просто ее формальную работоспособность, а реальную интеграцию с информационными системами всех субъектов КИИ, внедрение автоматизированных алгоритмов обмена данными о выявленных угрозах и уязвимостях в режиме реального времени. В этом контексте огромное значение приобретает выстраивание доверительных и оперативных каналов взаимодействия между государственными регуляторами (ФСБ России, ФСТЭК России) и частными операторами, владеющими значительной частью КИИ. Без налаженного государственно-частного партнерства, основанного на взаимной заинтересованности и защищенности передаваемой информации, система раннего предупреждения будет неполной. Кроме того, в условиях беспрецедентного санкционного давления императивом выживания становится форсированное импортозамещение в области программного и аппаратного обеспечения для нужд КИИ, причем не простое копирование зарубежных решений, а создание собственных, изначально ориентированных на максимальную кибербезопасность и свободных от уязвимостей и «закладок». Наконец, констатируя эксплуатацию «человеческого фактора» как одну из главных уязвимостей, необходимо поставить на системную основу работу по повышению цифровой грамотности всех слоев населения и формированию жесткой культуры «кибергигиены» у сотрудников организаций. Регулярные тренинги, симуляции фишинговых атак и четкие регламенты поведения в цифровой среде должны стать неотъемлемой частью корпоративной культуры.

Однако все вышеперечисленные меры национального уровня будут иметь лишь ограниченный эффект без активного международного сотрудничества. Кибертерроризм – угроза заведомо трансграничная, не признающая суверенитетов, и борьба с ней невозможна в одиночку. Российская Федерация традиционно выступает за верховенство международного права и выработку универсальных механизмов под эгидой ООН. В настоящее время ключевыми площадками для такого взаимодействия являются ШОС, БРИКС и ОДКБ. В рамках ШОС ведется постоянная и последовательная работа по адаптации антитеррористических стратегий к новым цифровым реалиям, включая кибертерроризм и киберэкстремизм [10, с. 48]. На повестке дня стоят следующие первоочередные задачи: инициирование разработки под эгидой ООН всеобъемлющей конвенции по противодействию использованию ИКТ в преступных целях, которая содержала бы четкое определение кибертерроризма, обязательства государств по криминализации соответствующих деяний и процессуальные механизмы взаимной правовой помощи. Параллельно необходимо расширять практику заключения двусторонних и многосторонних соглашений о сотрудничестве в области оперативного обмена информацией, проведения совместных следственных действий и экстрадиции. При этом крайне важно в ходе международного нормотворчества не допустить крена в сторону тотальной слежки и нарушения фундаментальных прав и свобод человека, соблюдая разумный баланс между требованиями безопасности и принципами открытости и свободы интернета.

Резюмируя изложенное, можно с уверенностью констатировать, что кибертерроризм предстает перед нами как сложный, многомерный социотехнический феномен, бросающий фундаментальный вызов всей архитектуре международной и национальной безопасности. Его уникальные свойства – от абсолютной анонимности до беспрецедентной асимметрии ущерба – в корне меняют правила игры, делая малоэффективными многие традиционные подходы. Анализ экосистемы угрозы наглядно показывает, что

зона бесконтрольности сжимается: от поверхностного веба для пропаганды до глубоко эшелонированного даркнета для наиболее опасных деяний. Единственно возможным ответом на этот вызов является научно обоснованная, системная и бескомпромиссная стратегия, фундаментом которой должны стать: 1) безотлагательная имплементация в уголовное и антитеррористическое законодательство Российской Федерации легального понятия и самостоятельного состава акта кибертерроризма; 2) построение технологически суверенной и непрерывно совершенствуемой системы защиты критической информационной инфраструктуры; 3) институционализация эффективного государственно-частного партнерства и многоуровневой системы подготовки кадров и киберпросвещения населения; 4) активизация усилий по созданию глобальной международно-правовой базы, построенной на принципах уважения суверенитета и неотвратимости наказания для всех участников кибертеррористической деятельности. Только консолидированные действия государства, научного сообщества, бизнеса и институтов гражданского общества способны обуздать эту новую угрозу и поставить надежный заслон на пути превращения цифрового мира в пространство хаоса и насилия.

Список литературы:

[1] Бураева Л. А. Кибертерроризм как новая и наиболее опасная форма терроризма // Юридический вестник ДГУ. – 2020. – Т. 34, № 2. – С. 145–152.

[2] Диденко А. И. Понятие и место кибертерроризма в уголовном праве России // Пробелы в российском законодательстве. – 2022. – № 4. – С. 90–94.

[3] Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2021. – № 1. – С. 148–151.

[4] Пучков Д. В. Кибертерроризм как новая угроза // Виктимология. – 2021. – Т. 8, № 4. – С. 382–390.

[5] Тарчоков Б. А. К вопросу о понятии кибертерроризма и некоторых способах противодействия // Вестник СевКавГТИ. – 2023. – № 2. – С. 42–46.

[6] Шпак А. А. К вопросу о противодействии информационному терроризму (на примере мессенджера Telegram) // Сибирский юридический вестник. – 2024. – № 3 (106). – С. 88–92.

[7] Даркнет как фактор террористической деятельности // CRSS.uz. – 2024. – 4 июля. – URL: https://crss.uz/2024/07/04/darknet-kak-faktor-terroristicheskoj-deyatelnosti/ (дата обращения: 26.05.2026).

[8] F6 назвала главные киберугрозы в 2026 году // РБК Компании. – 2026. – 2 февр. – URL: https://companies.rbc.ru/news/rl8XAjqQ3J/f6-nazvala-glavnyie-kiberugrozyi-v-2026-godu/ (дата обращения: 26.05.2026).

[9] F6 опубликовала ежегодный аналитический отчёт о киберпреступлениях в России и Белоруссии // itsec.ru. – 2026. – 2 февр. – URL: https://www.itsec.ru/news/f6-opublikovala-ezhegodniy-analiticheskiy-otchiot-o-kiberprestupleniyah-v-rossii-i-belorusii (дата обращения: 26.05.2026).

[10] Низамов М. Кибертерроризм как современная угроза безопасности: вызовы и меры противодействия // Евразийский журнал международного права. – 2026. – Т. 17, № 1. – С. 43–51.

References:

[1] Buraeva L. A. Cyberterrorism as a new and most dangerous form of terrorism//Legal Bulletin of DSU. – 2020. - T. 34, NO. 2. - S. 145-152.

[2] Didenko A.I. The concept and place of cyber terrorism in the criminal law of Russia//Gaps in Russian legislation. – 2022. – № 4. - S. 90-94.

[3] Mazurov V. A. Cyberterrorism: concept, problems of counteraction//Actual problems of combating crimes and other offenses. – 2021. – № 1. - S. 148-151.

[4] Puchkov D.V. Cyberterrorism as a new threat//Victimology. – 2021. - T. 8, NO. 4. - S. 382-390.

[5] Tarchokov B. A. On the question of the concept of cyber terrorism and some methods of counteraction//Bulletin of SevKavGTI. – 2023. – № 2. - S. 42-46.

[6] Shpak A. A. On the issue of countering information terrorism (using the example of the Telegram messenger)//Siberian Legal Bulletin. – 2024. – № 3 (106). - S. 88-92.

[7] Darknet as a factor in terrorist activities// CRSS.uz. – 2024. - July 4. – URL: https://crss.uz/2024/07/04/darknet-kak-faktor-terroristich-eskoj-deyatelnosti/ (дата обращения: 26.05.2026).

[8] F6 named the main cyber threats in 2026// RBC Company. – 2026. - Feb. 2 – URL: https://companies.rbc.ru/news/rl8XAjqQ3J/f6-nazvala-glavnyie-kiberugrozyi-v-2026-godu/ (дата обращения: 26.05.2026).

[9] F6 has published an annual analytical report on cybercrimes in Russia and Belarus// itsec.ru. – 2026. - Feb. 2 – URL: https://www.itsec.ru/news/f6-opublikovala-ezhegodniy-analiticheskiy-otchiot-o-kiberprestupleniyah-v-rossii-i-belorusii (дата обращения: 26.05.2026).

[10] Nizamov M. Cyberterrorism as a modern security threat: challenges and countermeasures// Eurasian Journal of International Law. – 2026. - T. 17, NO. 1. - S. 43-51.