УДК 343
DOI 10.24412/3005-8023-2025-3-33-38

КИБЕРПРЕСТУПЛЕНИЯ КАК НОВЫЙ МЕТОД ТЕРРОРИЗМА: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА

Акилова Мукаддас Мирмухамадовна, *канд. юрид. наук, доцент кафедры теории государства и права ТГУПБП (Худжанд, Таджикистан)*

КИБЕРҶИНОЯТ ЧУН РАВИШИ НАВИ ТЕРРОРИЗМ: ТАВСИФИ ҶИНОЯТӢ - ҲУҚУҚӢ

Акилова Муқаддас Мирмуҳамадовна, *н.и.ҳ., дотсенти кафедраи назарияи давлат ва ҳуқуқи ДДҲБСТ (Хуҷанд, Тоҷикистон)*

CYBERCRIMES AS A NEW METHODS OF TERRORISM: CRIMINAL-LEGAL CHARACTERISTICS

Akilova Mukaddas Mirmuhamadovna, *PhD in Law, associate professor of the department of theory of state and law, TSULBP (Khujand, Tajikistan)* ***e-mail:*** *firdavs.akilov@mail.ru*

Рассматриваются киберпреступления как новая форма террористических актов в условиях цифровизации общества. Отмечается, что использование информационно-коммуникационных технологий, наряду с положительными возможностями, порождает новые угрозы безопасности, наиболее опасной из которых является кибертерроризм. Он выражается в атаках на критическую инфраструктуру, в блокировании деятельности государственных и финансовых систем, распространении вредоносных программ и дезинформации, что отличает его от традиционных форм терроризма анонимностью, трансграничностью и высокой латентностью. Проведён уголовно-правовой анализ норм Уголовного кодекса Республики Таджикистан, который выявил отсутствие самостоятельной статьи, регулирующей ответственность за кибертерроризм. Действующие положения о терроризме и преступлениях в сфере компьютерной информации лишь частично охватывают данную категорию деяний, что создаёт правовые пробелы и снижает эффективность противодействия. В качестве рекомендации предлагается включить в уголовное законодательство отдельную норму, устанавливающую ответственность за кибертерроризм с учётом его объективных и субъективных признаков. Одновременно подчеркивается необходимость гармонизации национального права с международными стандартами и развития сотрудничества между государствами для создания эффективных механизмов предупреждения и пресечения кибертеррористических угроз.

Ключевые слова*: кибертерроризм, киберпреступность, терроризм, уголовное право, информационная безопасность, Республика Таджикистан, цифровая угроза*

Ҷиноятҳои кибернӣ ҳамчун шакли нави амалҳои террористӣ дар шароити рақамикунонии ҷомеа баррасӣ шудааст. Қайд мегардад, ки истифодаи технологияҳои иттилоотӣ-коммуникатсионӣ дар радифи имкониятҳои мусбат, хавфҳои дигарро ба бехатарӣ ба миён меорад, ки кибертерроризм хавфи аз ҳама хатарнок ба ҳисоб меравад. Он дар ҳамлаҳо ба инфрасохтори муҳим, маҳдуд сохтани фаъолияти низоми давлатӣ ва молиявӣ, паҳн кардани барномаҳои зараровар ва маълумоти бардурӯғ зоҳир мегардад, ки аз шаклҳои анъанавии терроризм бо маҳфулият, фаромарзӣ ва сахт ниҳонӣ будан фарқ мекунад. Дар натиҷаи таҳлили ҷиноятӣ-ҳуқуқии меъёрҳои Кодекси ҷиноятии Ҷумҳурии Тоҷикистон набудани моддаи алоҳида, ки ҷавобгариро барои кибертерроризм танзим мекунад, ошкор карда шудааст. Муқаррароти амалкунанда оид ба кибертерроризм ва ҷиноятҳои соҳаи иттилооти компютерӣ ин категорияи кирдорҳоро қисман дарбар мегирад, ки дар натиҷа норасоиҳои ҳуқуқиро ба миён оварда, самарабахшии муқобилатро

паст мекунад. Тавсия шудааст, ки ба Кодекси ҷиноятии Ҷумҳурии Тоҷикистон моддаи мустақил оид ба танзими ҷавобгарӣ барои кибертерроризм бо назардошти аломатҳои объективӣ ва субъективии он ворид карда шавад. Ҳамзамон зарурати ҳамоҳанг сохтани ҳуқуқи миллӣ бо стандартҳои байналхалқӣ ва инкишофи ҳамкории байналмилалӣ байни давлатҳо баҳри эҷоди механизмҳои муассири пешгирӣ ва рафъи таҳдидҳои кибертеррористӣ таъкид шудааст.

Калидвожаҳо: *кибертерроризм, киберҷиноят, терроризм, қонуни ҷиноятӣ, амнияти иттилоотӣ, Ҷумҳурии Тоҷикистон, таҳдиди рақамӣ*

The article examines cybercrime as a new form of terrorist attack in the context of digitalization of society. It notes that the use of information and communications technologies, along with positive opportunities, creates new security threats, the most dangerous of which is cyberterrorism. It manifests itself in attacks on critical infrastructure, blocking the activities of government and financial systems, and spreading malware and disinformation, which distinguishes it from traditional forms of terrorism by its anonymity, cross-border nature, and high latency. A criminal-legal analysis of the provisions of the Criminal Code of the Republic of Tajikistan was conducted, which revealed the absence of a separate article regulating liability for cyberterrorism. Current provisions on terrorism and cybercrime only partially cover this category of crimes, which creates legal gaps and reduces the effectiveness of counteraction. As a recommendation, it is proposed to include in criminal legislation a separate provision establishing liability for cyberterrorism, taking into account its objective and subjective characteristics. At the same time, the need to harmonize national law with international standards and develop cooperation between states to create effective mechanisms for preventing and combating cyber-terrorist threats is emphasized.

Key-words: *cyberterrorism, cybercrime, terrorism, criminal law, information security, Republic of Tajikistan, digital threat*

В условиях стремительной цифровизации все более актуальной становится проблема кибертерроризма – феномена, совмещающего киберпреступность и террористическую деятельность. Развитие информационных технологий предоставило террористическим структурам новые средства воздействия на государственные институты и население. Современные киберугрозы уже не ограничиваются экономическим ущербом или кражей информации – они становятся частью системных атак на критическую инфраструктуру, дестабилизируя общественную безопасность и нарушая основы правопорядка.

Особое значение данная тема приобретает для Республики Таджикистан – государства, находящегося на пересечении цифровых и геополитических вызовов Центральной Азии. Актуальность темы также обусловливается необходимостью усовершенствования уголовного законодательства в условиях глобальных киберугроз и активизации радикальных течений в цифровом пространстве. Говоря об этих угрозах 28 декабря 2022 года на торжественном собрании, посвященном профессиональному празднику сотрудников органов национальной безопасности Республики Таджикистан, Президент Республики Таджикистан Эмомали Рахмон справедливо отметил: «…вдобавок к этому, серьёзное негативное влияние на международную безопасность оказывают экологические и биологические проблемы, киберпреступления и кибертерроризм как новые угрозы…» [5].

Целью настоящего исследования является комплексный уголовно-правовой анализ киберпреступлений как нового метода осуществления террористической деятельности, с акцентом на выявление пробелов и противоречий в уголовном законодательстве Республики Таджикистан, а также выработка предложений по его совершенствованию с учётом

международных стандартов и современных вызовов информационной безопасности.

В соответствии с этой целью исследование направлено на:

- раскрытие сущности и признаков кибертерроризма как особого вида преступной деятельности;
- анализ действующих уголовно-правовых норм Республики Таджикистан, применимых к кибертеррористическим проявлениям;
- выявление основных проблем квалификации кибертерроризма в правоприменительной практике;
- формулирование рекомендаций по законодательному закреплению отдельного состава преступления «кибертерроризм» в Уголовном кодексе Республики Таджикистан.

В настоящем исследовании используется комплекс общенаучных и специальных юридических методов, направленных на всесторонний анализ киберпреступлений как формы террористической деятельности. Базовым является формально-юридический метод, применённый для анализа норм уголовного законодательства Республики Таджикистан, регулирующих ответственность за террористические преступления и киберпреступления. Для выявления правовых пробелов и разработки предложений по совершенствованию законодательства применяется сравнительно-правовой метод, позволяющий сопоставить нормы законодательства и нормативно-правовых актов. Системный и логический анализ используется для структурирования теоретических и нормативных подходов, а также для выявления взаимосвязей между правовыми категориями в области кибертерроризма. Кроме того, применяется метод обобщения правоприменительной практики, что дало возможность исследовать реальные проблемы квалификации, а также доказывания и предотвращения кибертеррористических преступлений в Таджикистане. Применённый методологический подход обеспечил объективность, научную обоснованность и прикладной характер полученных выводов.

Исследование киберпреступлений и их трансформации в инструмент террористической деятельности пока остаётся сравнительно новой темой в правовой науке Таджикистана. Тем не менее, в научной среде страны в последние годы можно наблюдать рост интереса к проблематике, касающейся информационной безопасности, цифрового права и противодействия терроризму.

Так, в трудах М. М. Саидзода подчёркивается, что современная киберсфера становится ареной не только экономических, но и идеологических и террористических столкновений. Автор утверждает, что «именно через виртуальное пространство экстремистские группировки могут более эффективно пропагандировать свою идеологию и скрытно осуществлять террористическую деятельность» [6, с. 35]. Таким образом, М. Саидзода делает акцент на идеологическом и информационном аспекте угроз, исходящих из цифровой среды.

Исследователь Ю. А. Абдуназаров в своих публикациях обращает внимание на необходимость пересмотра уголовного законодательства с учётом технологических реалий. В частности он подчёркивает, что действующий Уголовный кодекс Республики Таджикистан «не содержит специальной нормы, охватывающей все ключевые признаки кибертерроризма, что снижает эффективность уголовно-правовой защиты» [1, с. 19]. Он предлагает инкорпорировать в УК РТ отдельную статью, прямо посвящённую кибертеррористической деятельности, с определением её состава и отграничением от смежных преступлений.

Х. Р. Ниёзов, анализируя проблемы квалификации преступлений в цифровой среде, указывает на трудности правоприменения, когда киберпространство является транснациональной средой. Он пишет: «В наше время виртуальный мир бросает вызов государственным правовым границам, и без международного сотрудничества национальное законодательство само по себе не может устранить угрозу

кибертерроризма» [3, с. 47]. Это подчеркивает важность интеграции международных норм в национальное право. Особый вклад в развитие понимания киберпреступлений внес К.Д. Давлатзода, который подчеркивает необходимость принятия государственной стратегии по обеспечению кибербезопасности и предлагает разработанный проект Закона РТ «О кибернетической безопасности» [2, с. 15].

Таким образом, таджикские учёные выделяют следующие ключевые аспекты:

- необходимость отдельного уголовно-правового регулирования кибертерроризма;
- недостаточность традиционных механизмов квалификации;
- угрозу распространения экстремизма через интернет;
- важность межгосударственного сотрудничества и имплементации международных норм.

Но, несмотря на актуальность темы, системные комплексные исследования кибертерроризма как совокупного феномена пока находятся в стадии формирования, что подчёркивает научную новизну и значимость настоящей статьи.

Кибертерроризм представляет собой использование информационных технологий в террористических целях – с целью устрашения населения, дестабилизации государственных структур или оказания давления на политические процессы. Как отмечает таджикский исследователь М. М. Саидзода, «терроризм в киберсреде — это качественно новый этап эволюции экстремистских практик, не требующий физического присутствия, но обладающий разрушительным потенциалом» [6, с. 35].

Мы считаем, что ключевые признаки киберпреступлений как нового вида терроризма включают:

- преднамеренное нарушение функционирования систем связи, энергоснабжения, транспорта и здравоохранения;
- внедрение вредоносного программного обеспечения для различных террористических целей (вирусы, шифровальщики);
- распространение идеологии терроризма через цифровые платформы;
- угрозу жизни и здоровью граждан через манипуляцию инфраструктурой.

В законодательстве Республики Таджикистан прямое определение кибертерроризма отсутствует, однако его элементы можно усмотреть в ряде норм Уголовного кодекса. Так, статья 179 УК РТ предусматривает ответственность за терроризм, а также глава 28 УК РТ устанавливает уголовную ответственность за преступления в сфере информационной безопасности [6, с. 35-42; 7]. Особую значимость имеют следующие положения.

Статья 179 УК РТ. Террористический акт, включающий действия, направленные на подрыв деятельности органов государственной власти и силовых структур, устрашение населения либо оказание воздействия на принятие решений органами власти. Потенциально может включать кибератаки при соответствующей цели и последствиях.

Статья 298 УК РТ. Неправомерный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, который в совокупности с террористическим умыслом может образовать состав кибертерроризма.

Статья 300 УКР РТ. Компьютерный саботаж, т.е. уничтожение, блокирование либо приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя.

Статья 304 УК РТ. Нарушение правил эксплуатации ЭВМ, сетей и программ, применяемое при атаках на инфраструктуру.

Как подчеркивает Ю. А. Абдуназаров, «необходимость обновления уголовного законодательства обусловлена расширением арсенала террористических средств за счет

информационных и компьютерных технологий» [1, с. 18-25]. Однако текущая редакция уголовного закона РТ еще не содержит дифференцированной нормы о кибертерроризме, что порождает правовую неопределенность.

Главной проблемой уголовно-правовой характеристики кибертерроризма является сложность в квалификации: отсутствие прямой нормы о кибертерроризме вынуждает правоприменителя прибегать к совокупности статей, что снижает правовую определенность и затрудняет борьбу с подобными преступлениями. Также, обращая внимание на эту проблему, Х. Р. Ниёзов указывает: «Квалификация кибертеррористических действий на основе общего состава терроризма (ст. 179 УК) не учитывает специфику киберпространства как среды преступления» [3, с. 45-50].

Изучая данный вопрос, мы пришли к выводу, что:

- отсутствуют специализированные следственные методики расследования кибертеррористических преступлений;
- должным образом не разработаны нормы, регулирующие международное сотрудничество в борьбе с кибертерроризмом;
- отсутствуют санкции, адекватные (соразмерные) цифровым методам причинения ущерба.

Опасность кибертерроризма заключается в том, что его непосредственным объектом является не только общественная безопасность, как в классических террористических преступлениях, но и информационная инфраструктура, которая функционирует как критически важная структура в жизни общества. При кибертерроризме объектом посягательства становятся:

- системы энергоснабжения;
- государственные информационные ресурсы;
- транспортная и банковская инфраструктура;
- электронные базы данных правоохранительных органов и спецслужб.

Таким образом, кибертерроризм посягает одновременно на безопасность личности и общества, функционирование жизненно важных государственных систем, цифровой суверенитет и стабильность государства.

Также главным отличием кибертерроризма является форма реализации преступного умысла: он выражается в использовании информационно-коммуникационных технологий как основного орудия совершения преступления.

Субъективная сторона данного преступления характеризуется прямым умыслом, террористической целью является устрашение населения, дестабилизация власти, давление на решения государственных органов и создание последствий, связанных с массовыми сбоями, паникой, экономическими потерями или человеческими жертвами.

При этом кибертеррорист не нуждается в физическом контакте с жертвой, не присутствует на месте совершения преступления и может действовать анонимно, используя сложные схемы маскировки IP-адресов и цифровых маршрутов. Эти обстоятельства требуют специального подхода в доказывании субъективной стороны и в установлении вины.

Таким образом, для организации эффективной борьбы с этими угрозами кибертерроризм требует его признания в качестве отдельной формы терроризма, обладающей специфическими уголовно-правовыми признаками, и для повышения эффективности противодействия ему следует включить в УК РТ новую статью, специально посвящённую кибертерроризму, с чётким описанием его элементов. Также необходимо разработать подзаконные акты и инструкции для оперативных и следственных органов по выявлению, квалификации и доказыванию кибертеррористических преступлений. Об этой необходимости также указывается в Будапештской конвенции Совета Европы о киберпреступности [4].

Киберпреступность как метод современного терроризма представляет собой растущую угрозу национальной и международной безопасности. Отсутствие специализированных норм в уголовном законодательстве Республики Таджикистан затрудняет правоприменение и борьбу с данным видом преступлений. Учитывая глобальный характер киберугроз, необходимы системные меры законодательного и институционального характера. Интеграция международных подходов, развитие национальной правовой базы и подготовка кадров – ключевые шаги к формированию эффективной модели противодействия кибертерроризму.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. *Абдуназаров Ю. А. Кибертерроризм ва ҳуқуқи ҷиноятии Ҷумҳурии Тоҷикистон: ниёз ба ислоҳот / Абдуназаров Ю. А. // Маҷаллаи ҳуқуқшиносӣ. – 2023. – № 2(18).*
2. *Давлатзода К.Д. Масъалаҳои ҳуқуқӣ-ҷиноятӣ ва криминологии муқовимат бо киберҷиноятҳо: проблемаҳои назариявӣ ва амалӣ: дисс… д-ра юрид.наук / К.Д. Давлатзода. – Душанбе, 2024. -*
3. *Ниёзов Х. Р. Масъалаҳои мураккаби таҳсиси ҷиноятҳои киберӣ дар Тоҷикистон / Х. Р. Ниёзов // Паёми ДМТ. Силсилаи ҳуқуқ. – 2021. – № 1(99).*
4. *Конвенция Совета Европы о киберпреступности (Будапешт, 2001). Статья 12. https://www.wipo.int/wipolex/ru/text/502391.(Дата обращения: 10.05.2025)*
5. *Речь Президента Республики Таджикистан на торжественном собрании, посвященном профессиональному празднику работников органов национальной безопасности Республики Таджикистан. https://president.tj/event/domestic_trips/27266 (Дата обращения: 10.05.2025).*
6. *Саидзода М. М. Таҳдидҳои амниятӣ дар фазои иттилоотӣ ва чолишҳои замони муосир / Саидзода М. М. // Ҳуқуқ ва ҷомеа. – 2022. – № 4.*
7. *Уголовный кодекс Республики Таджикистан. Глава 28. base.mmk.tj/view_sanadhoview.php?showdetail=&sanadID=23&language=ru. (Дата обращения: 10.05.2025).*

REFERENCES:

1. *Abdunazarov Yu. A. Cyberterrorism in the future of Tojikiston: need to amendment //Abdunazarov U.A.// Legal journal. – 2023. – No. 2(18).*
2. *Davlatzoda K.D. Legal-Criminal and Criminological Issues of Combating Cybercrimes: theoretical and practical problems: dissertation… doctor of legal sciences Dushanbe. 2024*
3. *Niyozov H. R. The Problems of Cybercrime in Tajikistan // Message of NTU. The problems of cybercrime in Tajikistan. - 2021. - No. 1 (99).*
4. *The Council of Europe Convention on Cybercrime (Budapest, 2001). Article 12. https://www.wipo.int/wipolex/ru/text/502391. (Date of appeal: 05/10/2025)*
5. *Speech of the President of the Republic of Tajikistan at the Ceremonial Meeting dedicated to the professional holiday of employees of the national security agencies of the Republic of Tajikistan. https://president.tj/event/domestic_trips/27266 (Date of appeal: 05/10/2025).*
6. *Saidzoda M. M. Security Threats in the Information Space and Challenges of Modern Times // Law and Society. – 2022. – No. 4. – PP. 35–42.*
7. *Criminal Code of the Republic of Tajikistan. Chapter 28. base.mmk.tj/view_sanadhoview.php?showdetail=&sanadID=23&language=ru. (Date of appeal: 05/10/2025).*