**УДК 343.9**

**Абдирова Г.А.**

кандидат юридических наук

Костанайская академия МВД Республики Казахстан им. Ш. Кабылбаева

**Abdirova G.A.**

Candidate of Juridical Sciences

Kostanay Academy of the MIA of the Republic of Kazakhstan named after Sh. Kabylbayev

 **Особенности совершения преступления в сфере кибертерроризма**

**\***

**The specifics of committing a crime in the field of cyberterrorism**

**Аннотация**

В статье рассматривается актуальная проблема кибертерроризма, как одной из новых форм угроз в современном цифровом мире. Автор анализирует концептуальные основы кибертерроризма, выявляя его ключевые признаки и отличия от традиционного терроризма. Внимание уделяется основным методам и инструментам, используемым в кибертеррористических атаках, а также последствиям таких действий для государственной безопасности и общества в целом.

Статья подчеркивает трудности, с которыми сталкиваются правоохранительные органы и государственные структуры при разработке и реализации мер противодействия кибертерроризму, включая недостаток международного сотрудничества и отсутствие четких правовых рамок.

**Ключевые слова:** кибертерроризм, информационные преступления, правоохранительные органы.

**Annotation**

*The article examines the current problem of cyberterrorism as one of the new forms of threats in the modern digital world. The author analyzes the conceptual foundations of cyberterrorism, identifying its key features and differences from traditional terrorism. Attention is paid to the main methods and tools used in cyberterrorist attacks, as well as the consequences of such actions for state security and society as a whole.*

*The article highlights the difficulties faced by law enforcement agencies and government agencies in developing and implementing measures to counter cyberterrorism, including a lack of international cooperation and a lack of clear legal frameworks.*

**Key words:** *cyberterrorism, information crimes, law enforcement agencies.*

**Введение**

Особенности совершения преступления в сфере кибертерроризма заключаются в целенаправленном использовании информационных технологий для деструктивных целей, включая причинение масштабного ущерба как организациям, так и государствам. Кибертеррористы применяют сложные методы взлома, манипуляции данными и вирусные атаки, чтобы создать панику и подорвать доверие к системам управления. Одним из ключевых аспектов их деятельности является анонимность, обеспечиваемая использованием темных сетей и различных средств шифрования, что затрудняет расследование и раскрытие преступлений.

Важной особенностью кибертерроризма является его глобальный характер. Преступления могут быть совершены из любой точки мира, что делает их непредсказуемыми и трудно поддающимися контролю. Кроме того, кибертеррористы часто используют социальные сети для распространения своей идеологии, привлечения последователей и координации действий, что ставит перед правоохранительными органами новые вызовы в борьбе с данными угрозами.

**Основная часть**

Современный этап развития Европейского сообщества характеризуется быстрым прогрессом в научно-технической области, включая сферу высоких технологий.

В Окинавской хартии глобального информационного общества *(принята главами государств и правительств «Группы восьми» 22 июля 2000 г. Документ посвящен общим представлениям лидеров стран G8 о возможностях информационных технологий)* глобального информационного общества отмечалось, что «...информационные телекоммуникационные технологии выступают одним из ключевых факторов, формирующих структуры общества XXI века. Их революционное воздействие затрагивает образ жизни людей, образование и трудовую деятельность, а также взаимодействие между правительством и гражданским обществом. Быстро развивающиеся информационно-коммуникационные технологии становятся важным средством для стимулирования прогресса Европейского сообщества» [1]. Вместе с тем, развитие научно-технического прогресса всегда сопровождается всплеском негативных культур, в частности таких, как преступность.

Одновременно с применением технических средств возникла преступность, связанная с электронной обработкой информации, в том числе и преступность террористической направленности - «Акт терроризма» (ст. 255 УК РК), «Пропаганда терроризма или публичные призывы к совершению акта терроризма» (ст. 256 УК РК), «Создание, руководство террористической группой и участие в ее деятельности» (ст. 257 УК РК), «Заведомо ложное сообщение об акте терроризма» (ст. 273 УК РК) [2].

Согласно мнению экспертов, использование современных достижений в области высоких технологий может представлять собой не меньшую угрозу, чем ядерный или бактериологический терроризм. Арсеналы террористов сегодня могут включать в себя различные вирусы, а также компьютерные логические бомбы — специальные команды, заранее встроенные в программное обеспечение и активируемые в нужный момент.

Современные террористы активно используют Интернет не только для распространения своей идеологии, но и для передачи информации, хотя, по сути, они не рассматривают его как новое оружие. Однако становится очевидным, что кибертерроризм уже стал неотъемлемой частью реальной жизни общества. С каждым годом возрастает опасность кибератак, причем защитимые системы можно считать редкостью в этом быстро меняющемся цифровом мире. В связи с тем, что компьютерные технологии и интернет стали основными аспектами современного общества, крайне важно установить на государственном уровне требования к разработке и внедрению технических, правовых и организационных мер, направленных на защиту компьютерных сетей. Компьютерные сети, в данной ситуации, являются одним из самых уязвимых элементов, и их защита должна стать приоритетом для государственных структур.

В условиях нестабильной глобальной ситуации, обеспечение кибербезопасности требует не только создания надежных программных и аппаратных решений, но и формирования комплексного подхода, включающего законодательные инициативы, образовательные программы для специалистов, а также сотрудничество между различными странами в борьбе с киберугрозами. Без этого общества рискуют столкнуться с серьезными последствиями, угрожающими как безопасности граждан, так и функционированию критически важных инфраструктур.

Согласно закону Республики Казахстан «О противодействии терроризму» от 13 июля 1999 года № 416 в Статьи 1 указано, что под терроризмом понимается идеология насилия и практика воздействия на принятие решения государственными органами, органами местного самоуправления или международными организациями путем совершения либо угрозы совершения насильственных и (или) иных преступных действий, связанных с устрашением населения и направленных на причинение ущерба личности, обществу и государству) [3]. Следовательно, под кибертерроризмом понимается сложное и многогранное явление, которое включает в себя широкий спектр противоправных действий, направленных на подрыв безопасности, стабильности и благополучия общества. Под руководством кибертерроризма подразумевается не только использование высоких технологий и информационных систем для реализации своих намерений, но и применение психологических угроз и манипуляций.

Во-первых, кибертерроризм может проявляться в действиях, непосредственно угрожающих жизни и здоровью людей. Это могут быть кибератаки на критическую инфраструктуру, такие как системы здравоохранения или транспортные сети, которые могут привести к массовым жертвам. Нападения на такие объекты подчеркивают важность защиты информационных технологий, которые управляют жизненно важными функциями общества.

Во-вторых, такие действия могут включать в себя деструктивные атаки на материальные объекты, например, через разрушение систем управления промышленными предприятиями, что в свою очередь может привести к серьезным экономическим потерям и экологическим катастрофам. Это создает не только физические, но и психологические последствия для населения, вызванные страхом и неопределенностью.

Кроме того, кибертерроризм может использовать обширные объемы информации и данных с целью дезинформации, пропаганды и манипуляции общественным мнением. Группы, осуществляющие такие действия, могут создавать ложные повествования, сеять ненависть и недовольство, что приводит к социальной нестабильности и конфликтам внутри общества.

Кибертеррористы могут использовать свои действия как средство политического давления, пытаясь добиться определенных целей через запугивание государственных структур и населения. При этом они могут действовать как индивидуально, так и в организованных группах, используя сетевые технологии для координации своих действий.

Он может включить в себя кибершпионаж, кибератаки на критическую инфраструктуру, распространение наследственных программ, вымогательство взамен на продолжение кибертеррора, шантаж высокопоставленных лиц и т.д. Данные методы чаще всего использовались для финансового обогащения, реже в местах 2, 3, как это было указано выше. Не исключено, что средства, полученные за счет кибератак, затем пойдут на распространение терактов в стране или на развитие террористической организации за счет вербовки новых участников или объединений с другими организациями [4, с. 4].

По мнению ученого В.А. Голубева кибертерроризм - это атака на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжелых последствий, если такие действия были совершены с целью нарушения принципа безопасности, запугивания населения или провокации военного конфликта [5].

По мнению Ю.В. Гаврилова и Л.В. Смирнова, сущность кибертерроризма заключается в оказании противоправного воздействия на системы, совершенного в целях создания опасности, причиняющей вред жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для возникновения чрезвычайной ситуации и катастроф техногенного характера либо с точки зрения угрозы такой опасности [6].

Террористический акт, совершённый с использованием высоких технологий, или кибертеракт, становится всё более актуальной угрозой в условиях глобализации и расширения экономических связей. Современные телекоммуникационные технологии, проникающие во все сферы общества - от связи, энергетики и транспорта до финансовой системы и обороны - создают уникальные уязвимости. Зарубежные эксперты указывают, что новые методы управления процессами производства становятся катализатором для увеличения таких террористических актов. На конференции по защите от кибертеррора в Вашингтоне в 2000 году было подчеркнуто, что «…электронный терроризм - это не теория. Это реальность» [7]. Особенно остро кибертерроризм угрожает всемирным экономическим системам, зависящим от информационных сетей и стремительной интеграции технологий. С каждым годом растёт и число пользователей Интернета: в США - около 158 миллионов, в Европе - 95 миллионов, в Азии - 90 миллионов, что подчеркивает глобальное покрытие и доступ к сетевым ресурсам в любую точку планеты.

Не имея государственных границ, кибертеррористы способны угрожать информационным системам с любой точки мира, а их виртуальные следы зачастую настолько неуловимы, что выявить и нейтрализовать их представляет собой огромную проблему.

Террористический акт с использованием современных технологий — это сложная операция, в которой проявляется преднамеренная, политически мотивированная атака на системы, создающая реальную угрозу для жизни людей. Кибертеррористы способны не только осуществлять атаки, но и получать доступ к конфиденциальной информации, размещенной на сайтах государственных органов, включая схемы подземных коммуникаций и личные данные пользователей.

Директор Центра защиты национальной занятости ФБР США Рональд Дик в докладе, опубликованном на сайте Федерального бюро расследований, отмечает, что «в мире сформировалась новая форма терроризма - «кибертерроризм», который использует компьютеры и сетевые связи для разрушения национальных меньшинств и достижения своих целей». Мы каждый день сталкиваемся с компьютерными атаками на правительственные организации. Ахиллесова пятеро современного мира - растущая зависимость от компьютерных систем и информационных технологий» [8].

Кибертерроризм представляет собой новую форму терроризма, отличную от традиционных методов терроризма, использующих взрывчатые вещества или стрелковое оружие. В отличие от обычного террориста, который применяет официальные основания, кибертеррорист использует передовые технологии, компьютерные системы и сети для достижения своих разрушительных целей. Его основной результат становится так называемым «компьютерным оружием» — специальными программами и вирусами, разработанными для несанкционированного доступа к компьютерным системам, их взлома и манипуляций с их применением [10].

Кибертеррористы определяют различные виды программных средств, таких как вирусы, «троянские» программы, логические бомбы и другие формы приоритетного прогрманого обеспечения, которые могут проникнуть в системы данных и причинить серьезный ущерб. Эти программы способны не только изменять или уничтожать важные данные, но и вести скрытую разведку, получать конфиденциальную информацию, которая может быть использована для других злонамеренных целей. Вредоносные закладки и вирусы могут быть внедрены в компьютерные системы таким образом, чтобы незаметно действовать в течение длительного времени, оставаясь необнаруженными техническими средствами, пока этого не произойдет.

Таким образом, кибертерроризм может включать в себя широкий спектр атак, начиная с уничтожения важной информации, паралича важнейших инфраструктурных объектов и заканчивая манипуляциями с данными, которые могут привести к политическим или политическим последствиям.

В киберпространстве могут быть использованы различные приемы для совершения террористических актов, включая:

* Нанесение ущерба элементам киберпространства, разрушение сетей электропитания, создание помех, использование специализированных программ и стимуляция уничтожения аппаратных средств.
* Хищение или уничтожение информационного и программного обеспечения, а также ресурсов киберпространства.

Террористы могут применять стратегические инновации, используя достижения системной защиты, международные вирусы и программные закладки для воздействия на программное обеспечение и информацию с целью их изменения. Это может включать:

* Влияние на информационное обеспечение и компьютерное управление.
* Раскрытие и угроза публикации закрытой информации о функционировании систем кодирования, используемых в государственных, общественно значимых и военных информационных системах.
* Захват каналов телекоммуникационного вещания с помощью дезинформации, слухов и электронных средств террористических организаций, а также объявление их требований.
* Уничтожение и активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов связи, а также воздействие на операторов и разработчиков информационных и телекоммуникационных систем с целью принуждения к определенным действиям.

Информационный подход высокого уровня делится на две основные категории, каждая из которых отражает уникальные аспекты воздействия на информационные системы

Первая категория - это вывод из строя информационных систем. Хакерские действия, относящиеся к этому типу, являются наиболее распространенными. Они направлены на временное отключение или парализацию нижних систем управления и контроля, а также ограничение доступа к программной информации. Результатом таких действий становится неконтролируемое функционирование поражаемого объекта, что создаёт значительные угрозы, особенно в сферах атомной и химической промышленности, а также в военной области.

В этих секторах электронные системы защиты и нападения играют ключевую роль, и их ненадлежащая работа может привести к катастрофическим последствиям.

Вторая категория включает более решительные действия, которые связаны с информационными террористическими операциями против объектов информационных систем. Эти операции могут иметь разрушительные последствия, вплоть до уничтожения критически важных информационных ресурсов и линий связи, а также возможности полной манипуляции структурой управления, включая системы информирования. Если такие системы функционируют в рамках нижних уровней инфраструктуры, последствия событий, связанных с сетевыми атаками, могут быть сопоставимыми по масштабу с последствиями традиционных террористических актов, таких как взрывы. В этом контексте важно понимать, что информационный терроризм способен вызвать структурные разрушения и парализовать жизненно важные системы, что требует от государств и организаций принятия серьезных мер по защите своих информационных ресурсов.

Перемещение киберугрозы в сферу высоких технологий означает, что террористические организации могут планировать и осуществлять атаки с гораздо большей эффективностью и размахом, чем когда-либо прежде. К примеру, децентрализованные кибернетические атаки могут осуществляться из-за пределов страны, несколько облегчая задачу террористам избежать задержания и преследования.

На фоне стремительного технологического прогресса и увеличения уровня взаимосвязанности в глобальной сети, доступность сложных вычислительных систем, программного обеспечения и баз данных стала причиной того, что наоборот, положительные достижения могут обернуться угрозами. Такие технологии как облачные вычисления, большие данные и Интернет усложняют защищенность критических информационных систем, создавая новые уязвимости. Террористические организации могут использовать эти уязвимости для вторжения и манипуляции системами, участвующими в управлении энергоснабжением, транспортной инфраструктурой или даже биомедицинскими учреждениями.

Киберпространство, в свою очередь, предоставляет террористам платформы для пропаганды, вербовки сторонников и разработки стратегий. Социальные медиа и мессенджеры позволяют им эффективно взаимодействовать, обмениваться идеями и координировать свои действия, ускользая при этом от внимания правоохранительных органов. Это ставит перед миром новые вызовы в области безопасности и требует пересмотра существующих стратегий противодействия терроризму.

В то же время, борьба с таким форматом терроризма требует интеграции усилий как на уровне отдельных стран, так и на международной арене. Необходима разработка новых нормативно-правовых актов, которые обеспечили бы эффективное регулирование в сфере кибербезопасности и борьбы с террорами. Страны должны совместно работать над созданием международных стандартов и механизмов обмена информацией о киберугрозах, а также развивать программы обучения специалистов, способных реагировать на угрозы в реальном времени.

**Заключение.** Таким образом, противодействие кибертерроризму представляет собой сложную задачу, требующую неизменного внимания, инновационных подходов и сотрудничества международного сообщества. Каждый шаг, который будет предпринят для укрепления безопасности информационных систем, может стать решающим в предотвращении катастрофических последствий от высокотехнологичных атак, которые стремятся разрушить основы нашего общества и стабильности.

**Список литературы**

1 Окинавская хартия глобального информационного общества. Принята 22 июля 2000 г. // Дипломатический вестник. - 2000. - № 8 //http://www.mcrt.ru/index.php?nodeid=1218, свободный (дата обращения: 25.01.2025 время:23-45).

# 2 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 24.07.2023 г.)// //https://online.zakon.kz/Document/?doc\_id=31575252 (дата обращения: 20.01.2025 время:14-05).

# 3 Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму» (с изменениями и дополнениями по состоянию на 05.01.2024 г.)// <https://online.zakon.kz/Document/?doc_id=1013957> (дата обращения: 26.01.2025 время:09-05).

4 Васенин В.А. Информационная безопасность и компьютерный терроризм.//www.crime-research.ru, свободный (дата обращения: 19.01.2025 время:08-30).

5 Голубев В.А. Кибертерроризм - узроза национальной безопасности// www.crive-research.ru, свободный (дата обращения: 19.01.2025 время:16-08).

6 Гаврилов Ю.В. Современный мир: сущность, типология, проблемы противодействия / Ю.В. Гаврилов, Л.В. Смирнов. - М.: ЮИ МВД РФ, 2003. - 66 с.

7 Сайтарлы Т. Опыт США по расследованию компьютерных излучений//: www.crime-research.org/news/2000/09, свободный (дата обращения: 22.01.2025 время:21-17).

8 Гриняев С. США развертывают систему информационной безопасности. В дальнейшем разговоров дело пока не идет: Независимое военное обозрение № 45 (405)//http://www.cnews.ru/security/part3/rus-edu.shtml, свободный (дата обращения: 25.01.2025 время:04-17).