УДК 341.4

Кибертерроризм

Елеубай Абылайхан
abylaikhaan123@gmail.com
Студент 3 курса, группа МП-32, Юридического факультета
кафедры Международного права
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель: Мурзагалиев Е.Ч.

Аннотация

В настоящей статье рассмотрены основные особенности такого явления современного мира как кибертерроризм. Кибертерроризм можно считать преднамеренным использованием подрывной деятельности или угрозы таковой в отношении компьютеров и сетей с намерением причинить вред или достигнуть иных социальных, идеологических, религиозных, политических или аналогичных целей с запугиванием определенных граждан или иных лиц в интересах достижения подобных целей.

Ключевые слова: кибертерроризм, международное уголовное право, киберпространство, информационные технологии, противодействие киберпреступности.

Аннотация

Осы мақалада кибертерроризм сияқты қазіргі әлемнің құбылыстарының негізгі ерекшеліктері қарастырылған. Кибертерроризмді зақым келтіру немесе басқа да әлеуметтік, идеологиялық, діни, саяси немесе осыған ұқсас мақсаттарға қол жеткізу мақсатында белгілі бір Азаматтарды немесе өзге де тұлғаларды осындай мақсаттарға қол жеткізу мүддесінде қорқыту ниетімен компьютерлер мен желілерге қатысты бүлдіру қызметін қасақана пайдалану немесе мұндай қауіп-қатерлер деп есептеуге болады.

Ғылыми мақаланың кілт сөздері: кибертерроризм, халықаралық қылмыстық құқық, киберкеңістік, ақпараттық технологиялар, киберқылмысқа қарсы іс-қимыл.

Annotation

This article discusses the main features of such a phenomenon of the modern world as cyber terrorism. Cyber terrorism can be considered a deliberate use of subversive activities or threats thereof with respect to computers and networks with the intent to harm or achieve other social, ideological, religious, political or similar goals with the intimidation of certain citizens or other persons in the interest of achieving such goals.

Keywords of the scientific article: cyber terrorism, information technology, cyberspace, countering cybercrime.

С появлением глобальной сети возникла одна из наиболее опасных разновидностей киберпреступности - кибертерроризм, который, по сравнению с традиционным терроризмом, при совершении террористических акций прибегает к новейшим достижениям науки и техники.

Компьютерный терроризм (кибертерроризм) — использование компьютерных и телекоммуникационных технологий (прежде всего, Интернета) в террористических целях.

Термин был предложен в 1980-х годах старшим научным сотрудником Института безопасности и разведки (англ. Institute for Security and Intelligence) Барри Коллином, который использовал его в контексте тенденции к переходу терроризма из физического в виртуальный мир, возрастающего пересечения и срастания этих миров.

Общепринятого определения данного понятия не существует: зачастую, «кибертерроризмом» называют проявления киберпреступности, кибервойны или «обычного» терроризма. Отмечается, что термин используется чрезмерно часто, а опасность явления преувеличивается СМИ и производителями средств информационной безопасности, желающими увеличить продажи своих продуктов [1].

Общепринятого определения данного понятия не существует: зачастую, «кибертерроризмом» называют проявления киберпреступности, кибервойны или «обычного» терроризма. Отмечается, что термин используется чрезмерно часто, а опасность явления преувеличивается СМИ и производителями средств информационной безопасности, желающими увеличить продажи своих продуктов.

Кибертерроризм является одной из наиболее опасных форм проявления современного терроризма. Это связано, прежде всего, с особенностями, присущими глобальной сети Интернет: трансграничность (транснациональность), высокая анонимность, общедоступность и др. Тем не менее в юридической литературе отсутствует единое понятие «кибертерроризма».

Кибертерроризм является одной из наиболее опасных форм проявления современного терроризма. Это связано, прежде всего, с особенностями, присущими глобальной сети Интернет: трансграничность (транснациональность), высокая анонимность, общедоступность и др. Тем не менее в юридической литературе отсутствует единое понятие «кибертерроризма» [2].

В настоящее время проблема кибертерроризма затрагивает все мировое сообщество. Поэтому исследование данной категории преступлений является актуальной задачей на международном уровне.

Для полного понимания картины и масштабности угроз, которые стоят не только перед отдельно взятой страной, но и перед мировым сообществом в целом необходимо перейти к рассмотрению некоторых способов осуществления кибертеррористической преступности.

1. Использование компьютерных технологий с целью размещения в сети информации, способной оказать на людей устрашающее воздействие и обладающей признаками совершенного террористического акта. Например, размещение видеороликов террористического характера в Интернет-ресурсах. Содержание подобных видеоматериалов преследуют такие цели, как пропаганда терроризма, разжигание вражды и ненависти по принципу национальности, вероисповеданию и другим, предупреждения о готовящихся либо совершенных терактах и т.п. Подобные видеоролики служат рычагом давления на общество и государство, вводят в панику население, подрывают авторитет государственной власти.

2. Посредством сети Интернет происходит вербовка и вовлечение граждан в террористические сообщества. Поскольку сеть Интернет обладает повышенной анонимностью найти потенциального участника и завербовать его в террористическое сообщество не представляет особой сложности. С использованием сети Интернет организуется подготовка террористических операций, с непосредственными исполнителями проводится инструктаж, решаются тактические задачи во время проведения терактов. Аналогичным путем происходит финансирование террористической деятельности, планирование действий и общение между участниками такого преступного формирования, приобретение оружия и иных боеприпасов.

3. Преступные посягательства на объекты компьютерной инфраструктуры и информационные сети. Специалисты относят к таковым, например, выведение из строя информационных систем, которое приведет к бесконтрольному функционированию поражаемого объекта (что особенно опасно на предприятиях атомного и химического производства, а также в военной сфере для систем защиты и нападения) либо организацию разрушительных атак (уничтожение информационных ресурсов и линий коммуникаций либо физическое уничтожение структур, в которые включаются информационные системы) [3].

Арсенал компьютерных террористов – различные вирусы, логические бомбы – команды, встроенные заранее в программу и срабатывающие в нужный момент. Современные террористы используют Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие. Однако можно предполагать, что компьютерный терроризм сегодня уже представляет реальную угрозу обществу. В настоящее время существует весьма мало систем, которые можно назвать надежно защищенными. В связи с тем, что компьютерный терроризм уже представляет собой реальность, необходимо закрепить на государственном уровне обязанность государственных структур по разработке и внедрению технических, правовых и организационных мер, обеспечивающих защиту компьютерных сетей как одного из уязвимых элементов современного российского общества [4].

Рассмотрев основные способы совершения кибертерроризма, а также его значение и цели, на наш взгляд, направлением по решению имеющихся проблем будут являться следующие действия:

1. Необходимо ввести специальную ответственность за указанные преступные деяния, регламентируя их путем внесения в качестве квалифицирующего признака в ст. 256 УК РК. (Те же деяния, совершенные лицом с использованием своего служебного положения либо лидером общественного объединения, либо с использованием средств массовой информации или сетей телекоммуникаций, либо группой лиц или группой лиц по предварительному сговору, в том числе с использованием средств, полученных из иностранных источников, наказываются лишением свободы на срок от семи до двенадцати лет с конфискацией имущества) [5].

2. Организация и проведение курсов повышения квалификации сотрудников правоохранительных структур. Целесообразным представляется создание внутренних подразделений в структуре правоохранительных органов специализирующихся по борьбе с кибертерроризмом.Важной особенностью данного преступления является то, что жертва в последующем может включиться в преступную деятельность, связанную с торговлей людьми, например, в вербовку или эксплуатацию.

3. Мониторинг Интернет ресурсов с выявлением уже имеющихся факторов риска. Блокировка подобного характера сайтов и ресурсов.

4. Разработка научно-методического обеспечения по предотвращению трансграничных террористических кибератак, тем самым вырабатывая единый понятийный аппарат для всех стран.

5. Внедрение программ на уровне мирового сообщества по оперативному реагированию и по нейтрализации определенных зон террористической деятельности.

Подводя итог, отметим, что кибертерроризм приобретает повсеместный характер. Отмеченные проблемы касаются всех стран, именно поэтому предложенные пути решения данной проблемы в основном направлены на международное сотрудничество.

Актуальность данной проблемы стоит очень остро, так как новейшие технологии позволяют террористам расширять собственные границы деятельности. Данные вопросы требуют безотлагательного решения как внутри страны, так и во всем мире. Эффективное международное сотрудничество в области предупреждения и ликвидации последствий кибертерроризма имеет огромное значение.

Список использованных источников

1. Васенин В.А. Информационная безопасность и компьютерный терроризм // https://istina.msu.ru/publications/article/212734/
2. Гаврилов Ю.В. Современный терроризм: сущность, типология, проблемы противодействия - с. 66 // http://lawlibrary.ru/izdanie45445.html
3. Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия
4. Усилинский Ф.А. Кибертерроризм в России: его свойства и особенности. Право и кибербезопасность, 2014. № 1 – С. 6-11
5. Уголовное право Республики Казахстан, Акт терроризма ст.256, www.zakon.kz%2F4981877-k-kakim-pravovym-posledstviyam-mogut.html