ИСТОРИЯ И ПОЛИТОЛОГИЯ

Каскарбаева Зауре Айтошевна
старший преподаватель
Казахский агротехнический университет им. С. Сейфуллина
г. Астана, Республика Казахстан

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОМУ ТЕРРОРИЗМУ КАК ОДНО ИЗ ПРИОРИТЕТНЫХ НАПРАВЛЕНИЙ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

Аннотация: *статья посвящена проблеме противодействия кибертерроризму. Как отмечает автор, в современном мировом сообществе данный проблемный вопрос стал одним из важнейших вопросов, требующих объединения усилий всех государств мира.*

Ключевые слова*: информационное общество, компьютерный терроризм, кибертерроризм.*

Современное общество вступило в эпоху, которую американский философ Олвин Тоффлер охарактеризовал как информационное или постиндустриальное общество, где главным фактором развития человеческой цивилизации является производство и использование информации. В связи с этим вся история современного мирового сообщества может быть осмыслена через методы сбора, производства, анализа и использования информации и управления информационным ресурсами в обществе.

Сегодня информация передаётся, обрабатывается и воспроизводится с помощью компьютеров, создаются всемирные компьютерные, телекоммуникационные и космические сети связи и передачи информации. Информатизация ведёт к созданию единого мирового информационного пространства, в рамках которого производится накопление, обработка, хранение и обмен информацией между субъектами этого пространства – людьми, организациями, государствами. Но подобно тому, как быстрый промышленный рост создал угрозу экологии

земли, а успехи ядерной физики породили в своё время опасность ядерной войны, так и информатизация может стать источником целого ряда проблем, в том числе и компьютерного терроризма.

Этот новый вид терроризма будет осуществляться в информационной сфере, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

По оценке американских экспертов, эффект компьютерного терроризма может быть сравним с применением оружия массового уничтожения. По их мнению, угроза осуществления компьютерного терроризма прямо пропорциональна уровню технологического развития и масштабам использования компьютерной техники в системах управления государством.

Способы использования террористами сети Интернет разнообразны: 1. Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристике. 2. Сбор денег для поддержки террористических движений. Так, например, сайт о Чеченской республике (amino.com) представляет номер счета банка в Калифорнии, на который можно перечислить средства для поддержки чеченских террористов. 3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов. 4. Вымогательство денег у финансовых институтов с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию. 5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте, а также предание террористами с помощью Интернета широкой гласности своей ответственности за совершение террористических актов. 6. Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма». С помощью Интернета можно посеять панику, ввести в заблуждение,

привести к разрушению чего-либо. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями. 19 декабря 1997 года по национальному телевидению Японии демонстрировался анимационный фильм, содержащий контаминацию цветовой гаммы, мигания визуальной информации, от просмотра которого десятки людей получили психофизические расстройства различной тяжести 7. Вовлечение в террористические сети ничего не подозревающих соучастников – например, хакеров, которым неизвестно, к какой конечной цели приведут их действия. Кроме того, если раньше сеть террористов обычно представляла разветвленную структуру с сильным центром, то теперь это сети, где не просматривается четких командных пунктов – такую возможность предоставляет Интернет [1].

Под компьютерным терроризмом (кибертерроризмом), следует понимать преднамеренную, политически мотивированную атаку на информацию обрабатываемою компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей или наступления других тяжких последствий, если такие действия были содеянные с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. Под компьютерным терроризмом (кибертерроризмом), следует понимать запугивание населения и органов власти, с целью достижения преступных намерений. Это проявляется в угрозе насилия, поддержания состояния постоянного страха с целью достижения определенных политических или иных целей, принуждения к определенным действиям, привлечения внимания к личности кибертеррориста или террористической организации, которую он представляет. Причинение или угроза причинения вреда есть своеобразным предупреждением о возможности причинения более тяжких последствий, если условия кибертеррориста не будут выполнены.

Характерной особенностью кибертерроризма и его отличием от киберпреступности есть его открытость, когда условия террориста широко оповещаются.

Кибертерроризм – это серьезная угроза человечеству, сравнимая с ядерным, бактериологическим и химическим оружием, причем степень этой угрозы в силу своей новизны, не до конца еще осознана и изучена. Опыт, который уже имеется у мирового сообщества в этой области со всей очевидностью свидетельствует о несомненной уязвимости любого государства, тем более, что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. Обнаружить и нейтрализовать виртуального террориста весьма сложно из-за слишком малого количества оставляемых им следов, в отличие от реального мира, где следов содеянного остается все же больше. Особую озабоченность у правоохранительных органов вызывают террористические акты, связанные с использованием глобальной сети Интернет, из открытых источников которой, как утверждает ФБР, можно получить технологию изготовления биологического, химического и даже ядерного оружия террористов [2].

Борьба с компьютерным терроризмом, как, впрочем, и с терроризмом в целом, не может быть уделом отдельно взятых государств, поэтому необходимо обеспечить взаимодействие спецслужб, включая национальные службы безопасности и специальные подразделения по борьбе с терроризмом на национальном, региональном и международном уровнях.

Столь масштабная задача требует много времени и существенных финансовых затрат. Однако современная реальность такова, что существование той или иной страны во многом определяется ее способностью своевременно формировать эффективный ответ на вызовы внешнего мира. Поэтому вопрос о функционировании национальной системы противодействия компьютерному терроризму -это вопрос о выживании развитых государств в современных условиях [3].

Список литературы

1. Серебряник И.А. Компьютерный терроризм: современные особенности / И.А. Серебряник, Д.М. Золотухина [Электронный ресурс]. – Режим доступа: http://grani3.kznscience.ru/data/documents/9_Serebryanik2.pdf

2. Голубев В. Кибертерроризм как новая форма терроризма [Электронный ресурс]. – Режим доступа: Crime-reserarch.org

3. Региональный научно-практический центр исследования межэтнических и межконфессиональных процессов ПГУ им. С. Торайгырова [Электронный ресурс]. – Режим доступа:rukhanialem.psu.kz