УДК 00.004

Шарыпова Т.Н.,
кандидат экономических наук, доцент кафедры информационных технологий и защиты информации Ростовский Государственный Экономический университет
Россия, г. Ростов-на-Дону
Винкерт В.В.,
студент
1 курс, факультет «Юридический»
Ростовский Государственный Экономический университет
Россия, г. Ростов-на-Дону

КИБЕРТЕРРОРИЗМ: СУЩНОСТЬ, ОПАСНОСТЬ, МЕТОДЫ БОРЬБЫ

Аннотация: *в статье рассмотрены основные черты кибертерроризма, опасность данного явления и методы борьбы с ним.*

Ключевые слова: *информационные технологии, компьютерная сеть, киберпространство, кибератака, кибертерроризм.*

Annotation: *the article discusses the main features of cyberterrorism, the danger of this phenomenon and methods of combating it.*

Keywords: *information technology, computer network, cyberspace, cyber attack, cyber-terrorism.*

С развитием информационно – коммуникационных технологий увеличивается число новых угроз для безопасности общества. Одной из таких является кибертерроризм. Широкое распространение интернета и повсеместная компьютеризация в последние годы сделали общество особенно уязвимым перед этим новым видом преступности.

Существует различные определения понятию кибертерроризм. Общепринято понимать под данным термином проявление киберпреступности, использующей информационные технологии и, в частности, интернет, для совершения террористических актов [3]. Впервые понятие «киберторроризм» было использовано в 1980 году старшим научным сотрудником Калифорнийского института безопасности и разведки Барри Коллином. Оно связано с предшественником современного интернета – сетью ARPANET, объеденявшей лишь несколько компьютеров на территории США. Ученый был уверен, что вскоре возможности данной технологии будут взяты на вооружение террористов [1].

Кибертеррористы используют для совершения террористических актов не взрывчатку или стрелковое оружие, а современные информационные технологии с целью проникновения в компьютерные сети и уничтожения информационного ресурса [3]. Для совершения терактов в киберпространстве используются различные приёмы:

-разрушение инфраструктуры и нанесения экономического ущерба с помощью внедрения вредоносных вирусов в программное обеспечение, повергаемых атаке объектов;

-наведение помех на информационную инфраструктуру;

-хищение и уничтожение программного, или технического ресурса, имеющего стратегическую значимость;

-воздействие на программное обеспечение и информацию, с целью их искажение;

-хищение и раскрытие секретной информации;

-захват каналов вещание с целью дезинформации, пропаганды, дестабилизации обстановке, либо демонстрации силы;

-уничтожение и подавление линий связи [3].

Кибертерроризм является серьёзной угрозой для современного общества и способен нанести огромный ущерб современной экономике. Например, ущерб от атаки на всемирно известные Web-сайты Yahoo.com, Amazon.com, CNN.com,

eBay.com и другие, совершённой в феврале 2000 г. оценивается в 1,2 млрд. долларов [2]. По словам спецпредставителя президента РФ по вопросам международного сотрудничества в области информационной безопасности А. Крутских, ущерб от киберпреступности в 2016 году составил примерно 500 млрд. долларов [2].

Кибертерроризм, как и обычный терроризм имеет, в первую очередь, политические цели, что отличает его от остальных видов киберпреступности [1]. Но в сравнение с обычным терроризмом кибернетический характеризуется высокой степенью анонимности и низкой раскрываемостью: вычислить виртуального террориста очень сложно, поскольку компьютер с которого произведена кибератака может находится в любой точки планеты. Ещё одна проблема состоит в том, что киберторрористы практически не оставляют следов, способных помочь в обнаружении преступников [4]. Таким образом кибертерроризм является более опасным, нежели классический.

Для борьбы с кибертрроризмом имеется развёрнутая международная правовая система, основанная на соответствующих актах ООН и ОБСЕ, договорённостях в рамках ШОС и ЕС. Международное сотрудничество в этой области продолжает усиливаться. Параллельно отдельные страны также прилагают все больше усилий для защиты от кибертеррора. Так, например, Пентагон разрабатывают концепцию превентивных кибератаках для защиты своих интересов. В России создаётся единая система обнаружения, предупреждения и отражения компьютерных атак на информационные ресурсы, активно блокируются пропагандистке интернет ресурсы террористов, идёт подготовка специалистов для противостояния киберугрозам. Мероприятия для защиты от действий кибертеррористов проходят в других развитых странах. Однако требуется серьёзная работа над законодательством о кибертерроризме. Как пример несовершенства законодательства в области кибертерроризма, можно привести тот факт, что само это понятие законодательно закреплено лишь в двух странах: США и Украине. Данная проблема характерна для большинства стран [5].

Итак, кибертрерроризм является серьёзной угрозой для современного общества. Он наносит огромный экономический ущерб, нарушая работу, как информационных систем, так и объектов инфраструктуры, или промышленности. Кибертерроризм преследует, как и обычный терроризм, политические цели, что отличает его от других видов киберпреступности. Вместе с тем, в сравнении с обычным терроризмом, выйти на след кибертеррористов гораздо сложнее. Для борьбы с кибертерроризмом существует международная система сотрудничества, основанная на нормативно-правовых актов, заключенных в рамках международных организаций. Кооперация между государствами в данной области продолжает усиливаться. В развитых странах, на национальном уровне, разрабатываются различные механизмы для противодействия кибертерроризму. Вместе с тем, существуют и серьёзные проблемы в этой области. Главная из них – несовершенство законодательства в большинстве стран мира. Так, само понятие «кибертерроризм» юридически закреплено лишь в двух странах мира.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Васильев, М.В. Кибертерроризм как элемент гибридной войны. [Электронный ресурс]. – Режим доступа: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny .

2. Кошечкина, Е.А. К вопросу о мерах противодействия кибертерроризму // Омский научный вестник. – 2017. – №4 - С. 97-101.

3 Мазуров, В.А Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. – 2010. – №1 (21). - С. 41-45.

4. Шарыпова Т.Н., Свириденко А.А. Кибертерроризм – глобальная проблема современности. Научно-практический электронный журнал Аллея Науки. №1(28) 2019.

5. Шарыпова Т.Н., Сиваков В.Н. Киберпреступления. цели, последствия и методы защиты. Научно-практический электронный журнал Аллея Науки. №1(28) 2019.