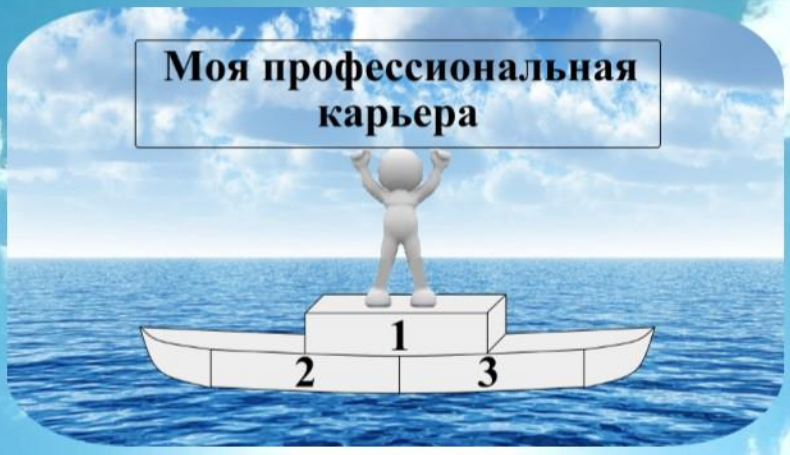
mpcareer@mail.ru

http://mpcareer.ru

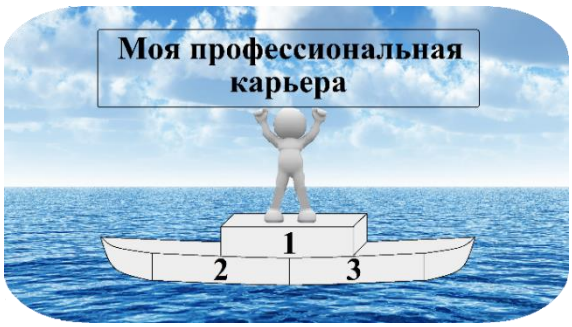


Научно-практический электронный журнал

МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА

ISSN 2658-7998

Выпуск №6 (том 1)
(ноябрь, 2019)



Международный научно-практический электронный журнал «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»
Сайт: http://mpcareer.ru

ISSN 2658-7998
УДК 001
ББК 94
И72

Международный научно-практический электронный журнал «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА». Выпуск №6 (том 1) (ноябрь, 2019)

Сборник содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Информация об опубликованных статьях предоставляется в систему Российского индекса научного цитирования (РИНЦ) и размещена на платформе научной электронной библиотеки (eLIBRARY.RU). **Лицензионный договор № 284-07/2019 от 30 июля 2019 г.**

Миссия научно-практического электронного журнала «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает представителей экспертного сообщества, докторов, преподавателей, научных сотрудников, бакалавров, магистрантов, аспирантов и иных лиц, интересующихся вопросами, освещаемыми в журнале.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

© ООО «МОЯ ПРОФЕССИОНАЛЬНАЯ КАРЬЕРА»
© Коллектив авторов

УДК 343

Никитина У.О.
Студентка 3 курса
Казанский государственный энергетический университет
г. Казань
Научный руководитель: **Шевко Н.Р.**
кандидат экономических наук, доцент
Казанский государственный энергетический университет
г. Казань

КИБЕРТЕРРОРИЗМ КАК НАИБОЛЕЕ ОПАСНАЯ ФОРМА ТЕРРОРИЗМА

Аннотация: В настоящей статье рассматриваются два подхода к определению компьютерного терроризма, как уголовно-правовой категории, представлены три категории данного вида преступления с конкретными примерами проявления. Автором предложены меры по предотвращению и профилактике проявлений кибертерроризма с привлечением соответствующих административных и технологических ресурсов.

Ключевые слова: Кибертерроризм, кибервойна, опасность для человечества, хакерские программы, интернет, террористические группы.

Annotation: This article discusses two approaches to the definition of computer terrorism as a criminal law category, presents three categories of this type of crime with specific examples of manifestation. The author proposed measures to prevent and prevent manifestations of cyber terrorism with the involvement of relevant administrative and technological resources.

Keywords: Cyber terrorism, cyber war, danger to humanity, hacker programs, the Internet, terrorist groups.

В середине 1980-х годов появился термин «кибертерроризм», его автором стал Бэрри Коллин, старший научный сотрудник в американском Институте безопасности и Разведки. Автор вкладывал в этот термин следующий смысл: террористические действия в виртуальном пространстве. Применялся только для прогнозирования [2]. На тот момент Бэрри Коллин не мог и представить, что кибертерроризм будет реальным уже через десятилетие. Хотя уже в 1983 году в США была арестована первая группа хакеров «414S»: юноши в возрасте от 16 до 22 лет взломали десятки крупнейших компьютерных сетей. Их выходка привела к правительственным слушаниям о киберпреступности, а также к введению шести законопроектов в Нижней палате конгресса США.

Рассмотрим два определения компьютерного терроризма:

Узкое определение. Заключается в том, что атаки направлены на компьютерные системы, в основном через Интернет, и несут угрозу для имущества, жизни и здоровья человека, и, конечно, влекут за собой серьезные нарушения в функционировании объектов [2].

Широкое определение. Рассматривается как сознательное совершение действий, которые нарушают функционирование компьютеров и/или телекоммуникационных сетей, и так же причиняют вред по определенным мотивам: социальные, идеологические, политические, религиозные, экономические, так же личного характера [2].

Юристы и многие должностные лица считают, что компьютерный терроризм представляет собой значительную угрозу человеческому обществу, сравнимую едва ли не с оружием массового поражения. К примеру, МЧС России отмечает, что особенно уязвимыми для кибератак являются энергетические системы [3]. В последние годы Россия активно внедряет в различные отрасли хозяйства автоматизированные и информационные технологии, что выводит вопрос борьбы с кибертерроризмом в разряд одной из важнейших государственных задач.

Кибертерроризм не утихает с каждым годом, новые технологии дают больше возможностей для атак:

НАТО в 2017 году отметило, что число хакерских атак на системы Североатлантического союза увеличились на 60 %, причем каждый месяц в НАТО отражали до 500 атак [4]. В этом же году НКЦКИ зафиксировало 2,4 млрд кибератак, 12 из которых были особо опасные [5]. Но резкое увеличение произошло в 2018 году, когда проходил Мировой Чемпионат по футболу, тогда зафиксировали 25 млн вредоносных манипуляций [6].

Разновидность киберпреступлений увеличивается из года в год, но среди них выделяют 3 основных вида компьютерного терроризма [7].

Первый – комплексный или координированный, так называемый кибертерроризм в буквальном смысле, когда террористические действия совершаются с помощью информационных технологий таких как компьютер и компьютерные сети, чтобы вызвать нарушение систем безопасности страны. Подобные атаки способны анализировать и вырабатывать свои действия. Второй вид: расширенный или структурированный, – использование глобальной сети Интернет для организации террористических групп, как правило, организация имеет определенную структуру, управление и занимается обучением новоприбывших участников. И третий, простой или неструктурированный, заключается в использовании программ, созданные не самими кибертеррористами. Затраты в данном случае минимальные.

Первый вид компьютерного терроризма характерен такими инструментами совершения как: атаки, которые несанкционированно проникают в сеть или перехватывают ее управление; распространение компьютерных вирусов, модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем; внедрение в программу логических бомб, которые срабатывают при определенных условиях; использование вредоносной программы, такие как «троянский конь», вредоносная программа, вложенная внутрь обычной программы, которая на первый взгляд кажется безопасной.

Следует отметить, что все эти средства нарушения и подавления информационного обмена в сетях. Особо следует выделить, что по сведениям аналитиков наибольший интерес для террористов представляют следующие

сферы: военная и ядерная, энергетическая, финансовая, сфера транспортных перевозок, так же и воздушный транспорт.

Так же 2007 году Израильская армия опробовала форму ведения кибервойны [8]. Военным хакерам из Израиля удалось тайно внедрить «троянский вирус» в код программного обеспечения сети сирийской противовоздушной обороны, благодаря чему израильтяне получили возможность управлять системой противника. Поэтому, когда израильские самолеты наносили удары по атомной энергетической установке в Сирии, на экранах сирийских радаров ничего не происходило.

Следует отметить, что летом 2017 года вирусы «Petya», вредоносная программа, сетевой червь и программа-вымогатель, которая поражает компьютеры под управлением Microsoft Windows, и «Wanna Cry» атаковали сотни компьютеров в информационных системах государственных органов, в том числе финансовых организациях в России. Данные программы предназначены для шантажа с целью получения денежных средств у владельцев зараженных компьютеров [9].

В качестве примера террористической киберугрозы ядерной структуре государства, можно привести многократные кибератаки на ядерные системы Ирана. В компьютерной системе Иранского центра по обогащению урана в 2010 году был обнаружен вирус под названием «Stuxnet», годом позже атомная структура Ирана подверглась атаке вирусом, получившим название «Stars», а еще через год, в 2012 году наиболее опасным вирусом «Flame», причинившими значительный ущерб ядерной безопасности Ирана [10].

Второй вид компьютерного терроризма – использование Интернета для организации и коммуникации террористических групп. Данные группы представляют из себя серьезную социально-опасную угрозу для всего человечества. Указанный вид кибертерроризма осуществляет: сбор информации для планирования терактов, проведение агитаций, пропаганды для привлечения в свои ряды. Террористы собирают денежных средства для поддержания своих движений, осуществляют психологическое давления на широкую аудиторию для

шантажа, наведения паники. Так же размещают в открытом доступе инструкций по самостоятельному изготовлению взрывных устройств.

Примером может служить случай в 2013 году «New York Times» и «Wall Street Journal» обвинили Китай в том, что в течение 4-х месяцев подвергаются хакерским нападениям. Китай назвал обвинения безосновательными. Дело было в группе хакеров Anonymous Mexico, которая взломала сайт обороны Мексики. Об этом сама террористическая группа сообщила в своем блоге Twitter [1].

Третий вид: простая неструктурированная атака – атака начального уровня в отношении отдельных систем с использованием программно-технических средств, разработанных чаще всего непричастными к терроризму лицами. Основной целью при этом является нарушение или замедление функционирования объекта атаки. Как правило, ее инициаторы имеют низкие возможности по анализу цели, невысокий уровень организации и инженерно-технической подготовки. Подобные атаки наиболее распространены в современном Интернете. Как правило, террорист скачивает из Всемирной сети подходящие хакерские программы и применяет их в отношении намеченной цели. Атака весьма ограничена по времени и последствиям. Если в системе установлены адекватные средства обеспечения кибербезопасности, то такая атака отражается достаточно просто, при этом восстановление системы требует минимальных усилий.

Кроме того, кибертеррористы при совершении террористических актов при помощи электронных сетей порой могут иметь возможность получения доступа к конфиденциальной информации либо государственной тайне. Сведения различной степени важности, которые содержатся в базах данных органов государственной власти с ограничением доступа к ним (схемы подземных коммуникаций, информация о строящихся стратегических объектах, личные данные граждан), потенциально могут попасть в руки к террористам. Но обезопасить себя от кибератак можно при случае, если все будут придерживаться определенным правилам. Даже сотрудник компании может нарушить договор,

заполучить данные и продать. Например, в сентябре 2019 года сотрудник Сбербанка слил в сеть персональные данные 60 млн клиентов.

Кроме того, Лаборатория Касперского проводила исследование в 2017 и выяснила, что российские компании хотят увеличить инвестиции в кибербезопасность и по прогнозам Сбербанка в 2021 году объем мировых расходов на нее возрастет в 14 раз.

Сущность вышеизложенного сводиться в следующему: компьютерный терроризм – это серьезная проблема, тем более что кибератаки осуществляются постоянно в сети Интернет. Следует отметить, что активная борьба ведется всем мировым сообществом, однако, несмотря на это, с каждым годом возрастает число призывов к насилию и совершению террористических действий в социальных сетях.

Рост масштабов проблемы, а также ее отрицательное влияние на развитие подрастающего поколения свидетельствует о том, что она требует выработки незамедлительных и четких решений по ее исправлению. В то же время, сиюминутное решение столь сложной задачи, как обеспечение безопасности глобального киберпространства, невозможно в принципе. Исходя из этого, наиболее оптимальным решением представляется разделение проблемы и поэтапное решение проблемы с привлечением соответствующих административных и технологических ресурсов [11]. Первоочередными шагами в этом направлении нужно предпринять следующие:

1) проведение грамотной молодежной политики: создание условий, при которых молодые люди могли бы быть уверены в завтрашнем дне, что в свою очередь будет препятствовать воздействию на них зачастую примитивной пропаганды, направленной на реализацию деструктивного протестного потенциала в политических целях;

2) активизация информационно-просветительской работы по пропаганде духовно-нравственных ценностей и традиций: патриотизма, уважения к истории своей страны, веротерпимости, законопослушности, – опять же, в среде подрастающего поколения;

3) введение как минимум возрастной цензуры компьютерных игр, многие из которых популяризуют насилие и жестокость;

4) повышение информированности населения об опасности кибертерроризма и киберэкстремизма в целях недопущения недооценки разрушительного социально-политического потенциала этих явлений;

5) проведение теоретической работы с населением в целях обучения общества умению противостоять этим угрозам;

6) отслеживание и оперативное устранение информации экстремистского характера специальными службами государства, выявление источников распространения такого рода информации, по возможности – пресечение их деятельности. При наиболее благоприятном исходе подобная работа обретет упреждающий характер, что существенно повысит безопасность в обществе в целом.

Список литературы

1. Случаи кибератак на сайты госструктур и СМИ в мире в 2012-2013 годах [Электронный ресурс] – URL: http://eurasian-defence.ru/?q=node/12608

2. Википедия Компьютерный терроризм [Электронный ресурс] – URL: https://ru.wikipedia.org/wiki/

3. Капитонова Е. А. Журнал «Известия высших учебных заведений. Поволжский регион. Общественные науки». «Особенности кибертерроризма как новой разновидности террористического акта»

4. Столтенберг сообщил об увеличении числа кибератак на системы НАТО [Электронный ресурс] – URL: https://iz.ru/news/658543

5. За год на Россию было совершено более четырех миллиардов кибератак [Электронный ресурс] – URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-soversheno-bolee-chetyreh-milliardov-kiberatak.html

6. За время ЧМ-2018 были отражены 25 млн кибератак на его [Электронный ресурс] – URL:

https://aif.ru/football2018/around/za_vremya_chm2018_byli_otrazheny_25_mln_kiberatak_na_ego_infrastrukturu

7. Цыгичко В.Н., Вотрин Д.С., Крутских А.В. и др. Информационное оружие – новый вызов информационной безопасности. − М., 2000

8. Израиль: солдаты кибервойны [Электронный ресурс] – URL: http://www.alefmagazine.com/pub2783.html

9. Petya wanna cry: какое отношение Россия имеет к вирусам 2017 года [Электронный ресурс] – URL: https://zen.yandex.ru/media/pnpru/petya-wanna-cry-kakoe-otnoshenie-rossiia-imeet-k-virusam-2017-goda--5a8ad6301410c3100b6ca60f

10. Кибератаки: вирус-диверсант Stuxnet в ядерной энергетической программе Ирана [Электронный ресурс] – URL: https://naukatehnika.com/kiberataki-virus-diversant-stuxnet-v-yadernoj-energeticheskoj-programme-irana-chast1.html

11. Шевко Н.Р./ Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения/ Ученые записки Казанского юридического института МВД России. 2016. Т. 1. № 1. С. 13-16.

© Никитина У.О., 2019

INTERNATIONAL STANDARD SERIAL NUMBER

ISSN 2658-7998

НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU

№ 284-07/2019

2019