Министерство образования и науки Российской Федерации
Федеральное государственное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт лингвистики и международных коммуникаций
Кафедра международных отношений и зарубежного регионоведения

РАБОТА ПРОВЕРЕНА
Рецензент, (должность)
_____(И.О. Ф.)
_____2017 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой, к.т.н., доцент
_____ Л.И. Шестакова
_____ 2017 г.

Противодействие международному кибертерроризму в Российской Федерации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–410305.2017.1895.ПЗ ВКР

Руководитель ВКР, к.и.н., доцент
_____ А.А. Попов
_____ 2017 г.

Автор проекта
студент группы ЛМ-425
_____ К.Р. Муслимова
_____ 2017 г.

Нормоконтролер, к.и.н., доцент
_____ А.А. Попов
_____ 2017г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Кибертерроризм — это многогранный феномен, обусловленный во многом бесконтрольным использованием глобальных сетей, недостаточным вниманием со стороны государства, гражданского общества и спецслужб к данному сегменту политики, проявляющийся в атаках на компьютеры, компьютерные программы и сети или находящуюся в них информацию, с целью создания атмосферы страха и безысходности в обществе во имя достижения целей и интересов субъектов террористической деятельности, требующий объединения усилий мирового сообщества для эффективного противодействия ему.

Современная ситуация требует скорейшей разработки механизмов предотвращения и пресечения террористического поведения в киберпространстве. В настоящее время проблематика международной информационной безопасности и глобального управления Интернетом выдвинулась на центральное место в перечне вызовов международной безопасности.

Актуальность данной работы обусловлена серьезной угрозой человечеству со стороны кибертерроризма. Имеющийся на данный момент у мирового сообщества опыт недостаточен для полноценного противодействия данной угрозе и говорит о наличии гарантированной уязвимости любого государства. Это напрямую связано с тем, что кибертерроризм является транснациональным явлением, а его участники имеют возможность угрожать информационным системам из любой точки мира. Ведь используя глобальную сеть Интернета террористам можно собрать подробную информацию об объектах атак, их местонахождении. Так же осуществление сбора денег для поддержки террористических движений.

Успешность решения задачи пресечения деятельности экстремистских и террористических организаций в информационном пространстве во многом зависит от глубокой теоретической проработки данной проблемы. Но до сих пор отсутствуют даже общепринятые определения кибертерроризма и

киберэкстремизма как порожденных глобализацией явлений, представляющих особую опасность для личности, общества и государства.

Объектом исследования является кибертерроризм как социально-политический феномен и политика противодействия ему.

Предметом исследования является направления государственной политики противодействия кибертерроризму, а также противоречия, влияющие на процесс разработки и реализации политики противодействия кибертерроризму в современной России.

Цель исследования заключается в изучении приоритетных направлений государственной политики противодействия этому виду терроризма, выработке рекомендаций по предупреждению актов кибертерроризма, совершенствованию стратегии борьбы, с этим негативным явлением с учетом российского и зарубежного опыта.

Цель исследования определила необходимость решения следующих **задач:**

1. Систематизировать основные научные подходы к изучению феномена кибертерроризма;
2. Выявить причины возникновения и активизации кибертерроризма на современном этапе, его особенности и тенденции функционирования;
3. Выявить противоречия, влияющие на процесс разработки и реализации политики противодействия кибертерроризму;
4. Выявить значение международного опыта противодействия кибертерроризму для разработки и эффективной реализации данного вида политики в современной России.

В исследовании использовались **методы** политологического, исторического, сравнительного, статистического анализа, классификации, систематизации, обобщения, описания. Совокупность данных методов позволила автору всесторонне подойти к изучению такого сложного феномена, как кибертерроризм, выявить его специфику среди других явлений и определить приоритетные направления противодействия ему.

Источниковую базу исследования составили нормативно-правовые документы стран и международных организаций. В данной работе были использованы такие нормативно-правовые акты как ФЗ РФ, указы президента, а также международные конвенции, которые регулируют главные направления развития политики, направленной на противодействие кибертерроризму, программные политические документы, политическая публицистика, информационные материалы конференций и новостные статьи.

Теоретическая значимость дипломной работы. Проведенное исследование, дополняя, уже имеющиеся работы по данной проблематике, расширяет возможности дальнейшего изучения особенностей и тенденций функционирования феномена кибертерроризма в политическом процессе РФ, углубляет представления о факторах, детерминирующих это явление, помогает в поисках эффективных путей минимизации последствий воздействия кибертерроризма.

Практическая значимость дипломной работы заключается в том, что полученные выводы и рекомендации могут помочь повысить эффективность практической деятельности органов государственной власти и силовых структур.

Результаты данной работы могут быть учтены при разработке современной стратегии кибербезопасности Российской Федерации, дальнейшей корректировке государственной политики противодействия кибертерроризму, выявлении наиболее эффективных направлений предупреждения и нейтрализации кибератак. Материалы дипломной работы могут использоваться для подготовки учебных пособий и программ, преподавания спецкурсов в высшей школе, а также системе специальных учебных заведений.

1 ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ФЕНОМЕНА КИБЕРТЕРРОРИЗМА

1.1 Анализ понятия «кибертерроризм»

Одна из возможных сфер современного терроризма — кибертерроризм, в том числе информационный, связанный с дестабилизацией работы компьютерных систем и сетей. Учитывая роль этих систем в современном мире, легко представить себе последствия вызванных этим крупных сбоев в работе транспорта, связи, энергоснабжения, правительственных и полицейских структур — так называемых «критических инфраструктур» современного общества. Как отмечает А.В. Федоров, особенность кибертерроризма в том, что он может быть составной частью или средством обеспечения другого теракта, который имеет больший масштаб и другую направленность. Более того, можно ожидать, что именно он может стать сутью и обязательным элементом всех будущих уже супертеррористических актов[1].

Возникновение данной формы терроризма связано с интенсивным развитием сети Интернет и расширением количества ее пользователей. Сеть Интернет на сегодняшний день охватывает около 150 стран мира. Особую озабоченность у правоохранительных органов вызывают террористические акты, которые связанны с использованием этой глобальной сети. Кибертеррористы распространяют вирусы, получая, таким образом, контроль над компьютерами полиции, больниц, аэропортов. Используя информацию в этих системах, возможно сбивать с курса самолеты и изменять истории болезни пациентов, что может привести к смерти людей.

[1]Лебедева, М.М. Мировая политика: учебник / М.М. Лебедева. – 4-е изд., стер. – М.: КНОРУС, 2016. – С.131-138.

Федеральный закон «О противодействии терроризму»[2] определяет «терроризм» как идеологию насилия и практику воздействия на принятие решения органами государственной власти, местного самоуправления или международными организациями, связанные с устрашением населения или иными формами противоправных насильственных действий.

Таким образом, кибертерроризм это не что иное, как особая разновидность терроризма, которая направлена на устрашение и иное воздействие на принятие решений различных структур с использованием современных информационно-телекоммуникационных технологий.

Но приравняв кибертерроризм к терроризму, не был сделан следующий шаг в борьбе с ним на международном уровне.[3]

Специалисты по информационной безопасности и борьбе с киберпреступностью делят кибертерроризм на следующие 3 уровня:

1. Неструктурированный: «хаки» используются против информационных систем, как правило используются программы, созданные кем-то другим (не самими кибертеррористами). Самый простой вид атак, потери от которого либо минимальны, либо незначительны.

2. Расширенный – структурированный: ведутся более сложные атаки против нескольких систем или сетей. Также возможно изменение или создание инструментов взлома. Организация с определённой структурой, управлением и прочими функциями полноценных организаций. Также участники таких группировок проводят обучение новоприбывших хакеров.

---

[2] Федеральный закон от 6 марта 2006 г. N 35-ФЗ О противодействии терроризму [Электронный ресурс] // Российская газета. – 10.03.2006. – №4014(0). – Режим доступа: https://rg.ru/2006/03/10/borba-terrorizm.html. – Загл. с экрана.

[3] Бочаров, Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю [Электронный ресурс] / Ю. Бочаров // International expert Centre for Electoral Systems. – 2011. – Режим доступа: http://www.elections-ices.org/russian/publications/region:world/textid:12835/%3E, свободный. – Загл. с экрана.

3. Комплексные – координированные: Способы к скоординированной атаке, которая может вызвать массовое нарушение систем безопасности страны. Возможность создания сложных инструментов взлома. Отличаются строгой структурой, зачастую представляют собой организации, способные здраво анализировать свои действия, вырабатывать какие-то планы атак и прочее[4].

На ряду с этими уровнями и угрозами существует одно очень важное и стремительно развивающееся благодаря современным IT технологиям направление, которое просто не может оставаться незамеченным с точки зрения проблематики развития кибертерроризма в современном мире. Речь идет о промышленном шпионаже. Его развитие имеет длинную историю в развитых индустриальных государствах, и с развитием новых технологий лица, занимающиеся этим видом шпионажа, получили новые возможности по добычи необходимой информации.

Шпионаж может осуществляться в пользу государства, организации или индивидуального «заказчика». Хотя промышленный шпионаж обычно ассоциируется с частными корпорациями, он может также быть осуществлен против военных сил государства.

В правовой науке существует 2 основных подхода к понятию кибертерроризма.

Согласно первому понятие кибертерроризма включает в себя группу признаков, связанных с деяниями (атакой или угрозой атаки) против компьютеров, сети или информации.

Д. Деннинг, авторитетный американский специалист по IT безопасности, говорит о кибертерроризме как о противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью

[4] Определение кибертерроризма [Электронный ресурс] / Elcomrevue. – 21 мая 2014. – Режим доступа: http://elcomrevue.ru/opredelenie-kiberterrorizma/, свободный. – Загл. с экрана.

принудить органы власти к содействию в достижении политических или социальных целей[5].

А.В. Рубанов считает, что «кибертерроризм преднамеренная, политически мотивированная атака на охраняемую законом информацию в критических сегментах государства, а также частном секторе, представленную в электронном виде на машинных носителях, с помощью преступного использования информационной системы, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий или угрозу совершения указанных действий в целях, свойственных терроризму»[6].

Аналогичной позиции придерживаются А. Уразбаев, Ю.В. Гаврилин, Р. Горбенкош и Л.В. Смирнов[7].

Второй подход к определению понятия «кибертерроризм» акцентирует внимание на целевом характере данных деяний. Р. Гереев и В.А. Мазуров основным признаком кибертерроризма предлагают считать «запугивание населения и органов власти с целью достижения преступных намерении, проявляющихся в угрозе насилия, поддержании состояния постоянного страха с мотивацией политических или иных целей, принуждения к определенным действиям, привлечения внимания к личности кибертеррориста или террористической организации, которую он представляет».

---

[5] Denning, D.E. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy / D.E. Denning // Networks and netwars: The future of terror, crime, and militancy. – 2001. – P.239-288.

[6] Рубанов, В.А. О согласовании процессов международного сотрудничества и национальных интересов в сфере информационной безопасности [Электронный ресурс] / В.А. Рубанов. – Agentura.ru, 2011. – Режим доступа: http://archive.is/d2tiJ, свободный. – Загл. с экрана.

[7] Чернядьева, Н.А. Международный терроризм: происхождение, эволюция, актуальные вопросы правового противодействия. Монография / Н.А. Чернядьева. – «Издательство «Проспект»», 2016.

В. А. Мазуров считает, что необходимо дифференцировать причинение вреда компьютерным системам и кибертерроризм. Ученый называет виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированную модификацию компьютерных данных, а также иные противоправные общественно опасные действия с помощью или посредством компьютера, компьютерных сечей и программ преступлением, совершенным в киберпространстве[8].

В. Васенин под кибертерроризмом понимает «совокупность противоправных действий в киберпространстве, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимущества при решении политических, экономических или социальных задач»[9].

Кибертерроризм - политически или идеологически мотивированная атака на информацию, данные пользователей или компьютерные системы с намерением причинить разрушительные последствия. Кибертеррористы и обычные хакеры используют общие тактические средства, но обычно имеют различные мотивы[10].

С правовой точки зрения Кибертерроризм объединяет группу родственных террористических преступлений, в которых объект преступления и (или)

---

[8] Мазуров, В.А. Кибертерроризм: понятие, проблемы противодействия [Электронный ресурс] / В.А. Мазуров // Доклады ТУСУРа. – 2010. – июнь. – № 1 (21), часть 1. – Режим доступа: http://old.tusur.ru/filearchive/reports-magazine/2010-1/41-45.pdf, свободный. – Загл. с экрана.

[9] Чернядьева, Н. А. Международный терроризм: происхождение, эволюция, актуальные вопросы правового противодействия. Монография / Н. А. Чернядьева. – «Издательство «Проспект»», 2016. – С.220.

[10] Шмидт, Э., Коэн, Д. Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – С.175.

объективная сторона тесно связаны с Интернетом, телекоммуникационными сетями, в том числе компьютерной техникой, программами и информацией.

Не каждый человек или группа, которая использует информационные технологии для продвижения своей повестки дня или нападения на своих противников, обязательно являются кибертеррористами. Тем не менее, часто бывает трудно определить, произошла ли атака от террористов или от учеников старших классов с техническим опытом доступа к вашей системе. Это часто заставляет задуматься о том, что действительно является кибертерроризмом и что такое просто хакерство. Существуют различные категории злоумышленников, с которыми можно столкнуться на кибер-арене.

❖ Хакеры

Это продвинутые пользователи компьютеров, которые проводят много времени на компьютерах или с ними, и упорно трудятся, чтобы найти уязвимости в ИТ-системах. Некоторые хакеры, известные как хакеры Whitehat, ищут уязвимости, а затем работают с поставщиком уязвимой системы, чтобы исправить эту проблему. Типичные хакеры, однако, их часто называют Blackhat Hackers, это люди, которые незаконно врезаются в другие компьютерные системы, чтобы нанести ущерб системе или данным, украсть информацию или вызвать сбой в сетях для личных мотивов, таких как денежная выгода или статус. Однако у них, как правило, отсутствует мотивация к насилию или серьезному экономическому, или социальному ущербу. Опасения вызывает то, что хакеры могут делать с информацией, которую они крадут у военных.

❖ Хактивисты

Это комбинация хакеров и активистов. У них обычно есть политический мотив для их деятельности, и они идентифицируют эту мотивацию своими действиями, например, срывают сайты противников, применяя контринформацию или дезинформацию. В одиночку эти действия имеют такое же отношение к кибертерроризму, как и кража, вандализм или граффити относятся к

традиционному физическому терроризму. Они могут быть вспомогательной частью террористической кампании.

А. Самуэль определила Хактивизм как применение ненасильственных, но незаконных или не вполне законных цифровых методов в политических целях. Это определение позволяет отделить хактивизм от онлайн-активизма, использующего конвенциональные формы интернет-участия и от кибертерроризма, применяющего вредоносные или насильственные методы[11].

Появление хактивистов политически или социально мотивированных и хакерских групп вроде Anonymous говорит о зрелости как идей, так и методов и позволяет представить, что нас ждет ближайшие годы.

Anonymous – современная международная сеть активистов и хактивистов, которая провела ряд протестов и других акций в ответ на цифровые антипиратские кампании, различных торгово-промышленных, кинозаписывающих и иных организаций. Некоторые аналитики восхваляют «Анонимус» как борцов за свободу интернета, или как «цифрового Робина Гуда». Однако, критики осуждают их как «анархических кибер-партизан», «толпу киберлинчевателей» или «кибертеррористов». В 2012 году американский журнал Time включил «Анонимус» в список 100 наиболее влиятельных людей года[12].

Наиболее распространенные формы хактивизма включают, но не ограничиваются ими, виртуальные забастовки и блокады, электронные бомбы, веб-сайты и вирусы и черви. Виртуальные забастовки являются эквивалентом традиционного метода протеста, при котором определенный сайт, связанный с

[11]Новикова, С.А. Процесс артикуляции политической идентичности в контексте политизации интернета : дис….канд. полит. наук : 23.00.02 / С.А. Новикова ; Пермск. Гос. Нац. Исследов. ун-т. – П., 2015. – 150 с.

[12] Fantz, A. Who is Anonymous? Everyone and no one [Электронный ресурс] / A. Fantz // CNN. – 2012. – 9 February. – Cable News Network, 2017. – Режим доступа: http://edition.cnn.com/2012/02/09/world/anonymous-explainer/index.html, свободный. – Загл. с экрана.

противостоящими или репрессивными политическими интересами, физически занят активистами. Электронные бомбы - это инструменты, используемые для перегрузки почтовых систем, почтовые отправления. Это приводит к переполнению системы, тем самым блокируя законный трафик. Вирусы, черви и другие виды вредоносного ПО малопригодны для хактивистов. Тем не менее, они были использованы организациями по всему миру. Один из таких примеров разрушительного последствия атаки вредоносного программного обеспечения произошел в 1989 году против НАСА, когда его компьютеры стали мишенью для злоумышленника, известного как червь WANK. Целью хакера была остановка запуска шаттла, который переносил зонд Galileo на его начальном участке к Юпитеру. Джон МакМахон, менеджер протокола в офисе SPAN NASA, оценил стоимость червя в 500 000$ в потраченное впустую время и ресурсы[13].

❖ Компьютерные преступники

Преступники обнаружили, что они могут использовать компьютерные системы, главным образом, для получения финансовой выгоды. Компьютерное вымогательство является одной из форм этого преступления. В качестве примера можно привести корпорацию Майкла Блумберга, которая была взломана двумя подозреваемыми, которые потребовали от «Блумберга» 200 000$ на «консалтинговые сборы», чтобы они молчали, как они скомпрометировали компьютерную систему Bloomberg. Другой пример касается получения несанкционированного доступа к государственным компьютерам и кражи информации для получения финансовой выгоды.

❖ Промышленный шпионаж

Промышленные шпионы могут быть спонсируемыми правительством или зависимыми от коммерческих организаций или частных лиц. Их цель может быть открытием служебной информации о финансовых или договорных вопросах, либо

[13] De Arimatéia da Cruz, J. Terrorism, War, and Cyber (In)Security [Электронный ресурс] / J. de Arimatéia da Cruz // Small Wars Journal. – 2013. – October 27. – Режим доступа: http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity, свободный. – Загл. с экрана.

приобретением секретной информации о уязвимых научно-исследовательских работах и разработках.

❖ Инсайдеры

Хотя ИТ-специалисты делают все возможное для защиты своих систем от посторонних, всегда существует угроза инсайдера с полномочным доступом к системе, проводящей атаку. Этими инсайдерами могут быть недовольные сотрудники, работающие в одиночку, или они могут работать совместно с другими террористами, чтобы использовать их доступ, чтобы помочь скомпрометировать систему.

❖ Консультанты / подрядчики

Еще одна проблема заключается в практике многих организаций использовать внешних подрядчиков для разработки программных систем. Это часто предоставляет этим подрядчикам доступ к кибертерроризму.

❖ Террористы

Несмотря на то, что террористические группы еще не совершали крупных кибератак, которые унесли жизни или вызвали серьезные физические разрушения, некоторые правительственные эксперты полагают, что террористы приближаются к той ступени развития, где они могут использовать Интернет в качестве прямого средства для причинения жертв[14].

26 апреля 2016 года команда хакеров, поддерживающих террористическую группировку «Исламское государство» объявила о том, что овладела персональными данными сотрудников Госдепартамента США. В доказательство было опубликовано несколько скриншотов с этой информацией и обещание «раздавить» США. «Ваша система не смогла отбить наши атаки. Мы сокрушим вас снова,» — гласит заявление группировки, известной как «Объединенный киберхалифат» (United Cyber Caliphate). Хакеры заявили, что они заполучили

[14] Cyber Operations and Cyber Terrorism [Электронный ресурс] // Handbook. – 2005. – 15 Aug. – No. 1.02. – Threats For Leavenworth, 2005. – Режим доступа: http://handle.dtic.mil/100.2/ADA439217, свободный. – Загл. с экрана.

личные данные 18 000 работников органов безопасности Саудовской Аравии. Ранееза нелелю до этого, аналитики сообщили, что связанная с ИГ группа разместила в Сети имена более чем 3500 жителей Нью-Йорка с заявлением «Мы хотим, чтобы они были мертвы»[15].

Но в чем же кибертерроризм проявляется или какова его тактика воздействия в глобальной сети Интернет? Если говорить о видах воздействия или о различных приемах кибертерроризма, то к ним можно отнести:

1) Нанесение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания, наведение помех и др.);
2) Кража или уничтожение информационного, программного и технического ресурсов, которые имеют общественную значимость, путем преодоления систем защиты, внедрения вирусов и т.п.;
3) Воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;
4) Раскрытие и угроза опубликования или само опубликование закрытой информации о функционировании информационной инфраструктуры страны, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.;
5) Захват каналов СМИ для распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
6) Уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутации;

[15] Хакеры-исламисты заявили о краже данных сотрудников Госдепа США [Электронный ресурс] // Интерфакс. – 2016. – 26 апреля. – Режим доступа: http://www.interfax.ru/world/505598, свободный. – Загл. с экрана.

7) Проведение информационно-психологических операций;
8) Ложная угроза акта кибертерроризма, влекущая за собой серьезные экономические последствия;
9) Воздействие на операторов, разработчиков информационных и телекоммуникационных сетей и систем с помощью насилия или угрозы насилия, шантажа, подкупа, использования НЛП, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и др.[16].

Вышеперечисленные приемы постоянно совершенствуются в зависимости от средств защиты, применяемых разработчиками компьютерных сетей.

1.2 Причины возникновения и условия функционирования кибертерроризма в XXI веке

В результате глобализации, компьютеризации и появления сетевого общества многие авторы утверждают, что кибертерроризм становится все более привлекательным для террористов по нескольким причинам.

Во-первых, кибертерроризм обычно считается более рентабельным, чем традиционные террористические методы.

Типичные компьютеры и телефоны или широкополосные Интернет-соединения, как правило, намного дешевле и их легче приобрести, чем традиционные виды вооружения, как например взрывчатые вещества и военные автомобили. Кибертеррористические атаки также не приводят к гибели нападавшего, как это имеет место с террористами-смертниками, и, как это, возможно, имеет место в случае традиционных террористических актов.

[16] Григорьев, Н., Террористические действия в виртуальном пространстве опасны [Электронный ресурс] / Н. Григорьев, Э. Родюков // Независимое военное обозрение. – 2016, – Режим доступа: http://nvo.ng.ru/armament/2016-07-22/12_cyber.html, свободный. – Загл. с экрана.

Во-вторых, кибертерроризм обладает определенной степенью анонимности, которая не встречается в более традиционных формах терроризма. Глобальное расширение компьютерных технологий в постиндустриальных обществах способствовало мобильности и развертыванию террористов. Таким образом, органам безопасности становится все труднее определять настоящую самобытность террористов. Это сложное препятствие еще больше усиливается из-за отсутствия таможни, границ или контрольно-пропускных пунктов в киберпространстве. Хотя остается фактом, что весь интернет-трафик проходит по меньшей мере через один из тринадцати центральных серверов, которые выступают в качестве основы Всемирной паутины, огромное количество передаваемой информации создает значительные проблемы для анализа данных и эффективного сбора разведывательных данных.

В-третьих, количество и качество целей возрастает по мере того, как общество переходит к дальнейшей зависимости от информационных технологий. Количество потенциальных целей уже огромно, от правительственных военных систем до гражданских экономических и научных сетей.

В-четвертых, кибертерроризм устраняет или уменьшает потребность в географической близости к цели. Это фактически устраняет традиционные требования к физической и психологической подготовке, чтобы избежать захвата и риска смерти. Удаленная способность вести кибертерроризм является ключевым фактором транснационального характера совершения террористических актов и привлечения новых членов.

В-пятых, кибертерроризм потенциально может оказывать прямое воздействие на большее число людей, чем традиционные террористические методы, что приводит к широкому распространению и повышению осведомленности о конкретных причинах (например, благодаря более широкому освещению в СМИ). В то время как террорист-смертник может разрушить здание, убив десятки или сотни человек внутри, нападение кибертеррориста на управление отходами или

энергетическую систему потенциально может убить или повредить тысячи, если не миллионы людей[17].

На сегодняшний день понятие кибертерроризма пересекло границы фантастических романов и широко обсуждается в СМИ, на правительственном и корпоративном уровне. Однако необходимо признать тот факт, что кибератаки на самом деле могут иметь значительные последствия. Многие энергетические компании и водное оборудование управляют своими ресурсами при помощи систем контроля и сбора данных (Supervisory Control and Data Acquisition (SCADA), которые могут быть уязвимы к кибератакам. Более 80% критичной сетевой инфраструктуры США являются собственностью частных компаний, которые зачастую не являются достаточно осведомленными в вопросах информационной безопасности и на которые сложно повлиять при помощи целевых государственных программ.

Подключение к Интернету даёт дополнительную возможность проникновения злоумышленников в компьютерные системы. По мнению экспертов, наиболее уязвимой в отношении кибератак является инфраструктура самой сети Интернет. Достаточно привести пример сетевого червя Nimda, который нанёс организациям, подключенным к Интернету, совокупный ущерб, который оценивается в 3 млрд долларов.

Наибольшая угроза со стороны Интернета, с точки зрения правоохранительных органов, заключается в возможностях глобальных коммуникаций, которые она предоставляет, отследить которые чрезвычайно сложно. Для того чтобы осуществить перехват переговоров террористов, осуществляемых с использованием сети Интернет, ФБР продолжает расширение штата своих высококвалифицированных ИТ специалистов. Так, по словам Дона Кавендера, специального агента и инструктора Центра компьютерного обучения

[17] Che, E. Securing a network society cyber-terrorism, international cooperation and transnational surveillance / E. Che // Research paper. – 2007. – September. – No. 113. - Research institute for European and American Studies (RIEAS), 2007. – P.15.

ФБР, их беспокоит не столько угроза кибертерроризма, сколько использование террористами Интернета для планирования и подготовки физических террористических актов[18].

По заявлениям западных спецслужб и правоохранительных органов активно используют возможности Интернета такие террористические организации, как «Аль-Каида», «Хезболла», «Абу Нидаль» и др. С учетом данных, полученных в ходе проведенных в Казахстане оперативно-розыскных мероприятий, к ним можно также отнести «Жамаат моджахедов Центральной Азии» и «Исламское движение Узбекистана». С использованием Интернета ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение новых членов, финансирование, эффективная и законспирированная связь.

Террористы и джихадистские организации признали важность Интернета как части своего арсенала оружия в «театре страха», поскольку они пытаются завоевать сердца и умы перспективных сочувствующих и новобранцев. Интернет стал одним из самых важных инструментов в войне Аль-Каиды против неверных и их сторонников. Так называемые джихадистские сайты распространились после 11 сентября 2001 года террористических нападений на США. Не только распространение веб-сайтов джихадистов, но и качество, содержание и сообщения также стали более изощренными и профессиональными[19].

Серьезная угроза кибератак со стороны международных террористов стоит в настоящее время перед США, Великобританией, Германией и рядом других стран Запада. По данным экспертов, в настоящее время в них резко возросло количество атак на государственные информационные системы, последствия, которых не

[18] Астахов, А. Искусство управления информационными рисками / А. Астахов. – М.: ДМК Пресс, 2010. – 312 с. – С.41

[19] De Arimatéia da Cruz, J. Terrorism, War, and Cyber (In)Security [Электронный ресурс] / J. de Arimatéia da Cruz // Small Wars Journal. – 2013. – October 27. – Режим доступа: http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity, свободный. – Загл. с экрана.

менее опасны, чем традиционные террористические акты с использованием смертников, взрывчатки и т. д. Такие атаки могут выводить из строя системы управления и функционирования атомных и других важных объектов, нефте- и газопроводов, электростанций, железных дорог, аэропортов, объектов водоснабжения.

Таким образом, в пятерку стран по наибольшему количеству киберугроз на 27 января 2017 года по данным интерактивной карты киберугроз Лаборатории Касперского[20] вошли: Россия, Германия, Вьетнам, США, Индия. Данные отображены в приложениях А2 и А3.

С 12 мая 2017 года по всему миру начал распространяться вирус-вымогатель WannaCry, шифрующий данные на заражённом компьютере и требующий оплаты в биткоинах для их расшифровки. Как выяснили специалисты, данный вирус заражает только компьютеры с ОС Windows. Распространяется WannaCry по электронной почте. Жертвам приходит зашифрованный сжатый файл, поражающий компьютер при загрузке. Все заражённые файлы меняют расширение на WNCRY, а объявление на экране монитора требует отправить от 300 до 600 долларов для расшифровки. В противном случае вирус грозит удалить данные с компьютера.

Впервые об атаке вируса сообщили в Испании. Там он поразил сети больниц, консалтинговой компании и банков. После вирус начал стремительно распространяться по всему миру. Особо пострадали медучреждения Великобритании и компания Deutsche Bahn в ФРГ. В России вирус атаковал сети российских телекоммуникационных компаний «МегаФон» и «ВымпелКом». Атакам также подверглись МВД и Следственный комитет. 13 мая 2017 года появилось сообщение о заражении сетей «Российских железных дорог». Хакеры также атаковали сети Минздрава РФ и Сбербанка, но там сообщили об успешном

[20] Интерактивная Карта Киберугроз [Электронный ресурс]. – ЗАО «Лаборатория Касперского», 2017. – Режим доступа: https://cybermap.kaspersky.com/ru/subsystems/, свободный. – Загл. с экрана.

отражении атак. В общей сложности десятки тысяч компьютеров в 74 странах подверглись кибератаке[21].

Кибертерроризм порой сравнивают по эффекту применения с воздействием ядерного, бактериологического и химического оружия.

Во время первой войны в Персидском заливе (1990-1991 гг.) израильские хакеры начали вирусные атаки против правительственных систем Ирака, с целью нарушить их коммуникационную способность во время вторжения в США.

Сейчас кибертерроризм вышел на новый уровень, связанный с использованием быстроразвивающегося интернета вещей. Создание угроз и опасности для информации, против безопасности данных и нормального функционирования сети. В октябре 2016 года на DNS-сервисы компании DYN прошла DDoS-атака, которая оказалась одной из крупнейших хакерских атак этого года. На сервера компании обрушилось более терабита информации в секунду, обрушив их за считанные секунды. Она задела не только саму компанию-провайдера, но и всех её клиентов. Среди них самые популярные во всей сети платформы и сервисы: Amazon, Twitter, GitHub, Heroku, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, The New York Times, Starbucks, HBO, CNN, Basecamp, PayPal, Etsy. Этот список далеко не полный. В него попало более чем 75 участников: интернет-платформы новостных ресурсов, финансовых организаций, продавцов услуг, социальных сетей, сайты компаний-разработчиков. Примерные потери приравниваются к 110 000 000$ – за одни сутки. Событие вышло за рамки администрирования, на «федеральный» уровень. Все, кто

[21] Сошников, А. WannaCry: как работает крупнейшее компьютерное вымогательство / А. Сошников // Русская служба Би-би-си. – 2017. – 13 мая. – Би-би-си, 2017. – Режим доступа: http://www.bbc.com/russian/features-39905001, свободный. – Загл. с экрана.

пострадал, будут восстанавливать репутацию. Стало понятно, что никто не надежен настолько, насколько это казалось ещё недавно[22].

По данным Verisign, ведущей компании по кибербезопасности, DDoS-атаки атакуют большие объемы вредоносного трафика в онлайн-ресурсах с целью вызвать истощение или полное потребление ресурсов системы или процесса, что делает их недоступными или непригодными для пользователей. Существует множество методов DDoS, которые злоумышленник может и будет использовать. Но независимо от формы атаки DDoS, ее намерения, как правило, нарушают работу системы таким образом, чтобы не позволить законному пользователю получить доступ к операциям системы. Одна из форм DDoS, например, - это исчерпание ресурсов. В этой методике бот-мастер, контроллер зараженной компьютерной системы, перегружает систему до такой степени, что она больше не отвечает на законные запросы[23].

Согласно отчету «Лаборатории Касперского», первый квартал 2017 ознаменовался традиционным для начала года спадом числа DDoS-атак. При этом общий вектор развития угрозы подтверждает прогнозы экспертов компании. По сравнению с аналогичным периодом предыдущего года количество и сложность атак продолжает расти[24].

Системой Kaspersky DDoS Intelligence в первые три месяца 2017 года были зафиксированы атаки по целям, расположенным в 72 странах мира.

---

[22] Уварова, А. Опасность и безопасность – гонка виртуальных вооружений [Электронный ресурс] / А. Уварова // Хабрахабр. – 2016. – 26 октября. – «ТМ», 2017. – Режим доступа: https://habrahabr.ru/post/313460/, свободный. – Загл. с экрана.

[23] José de Arimatéia da Cruz Terrorism, War, and Cyber (In)Security [Электронный ресурс] / José de Arimatéia da Cruz // Small Wars Journal. – 2013. – October 27. – Режим доступа: http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity, свободный. – Загл. с экрана.

[24] Khalimonenko, A. DDOS attacks in Q1 2017 [Электронный ресурс] / A. Khalimonenko, O. Kupreev // SecureList. - AO Kaspersky Lab., 2017. - Режим доступа: https://securelist.com/ddos-attacks-in-q1-2017/78285/, свободный. – Загл. с экрана.

Согласно приложению А1, первое место по числу серверов управления ботнетами (сеть связанных между собою вирусом компьютеров, которые управляются злоумышленниками из командного центра) остается за Южной Кореей, а на второе вышли США. Нидерланды впервые с апреля 2015 года вытеснили из тройки лидеров Китай, который опустился на седьмую позицию. Россия осталась на четвертом месте. Кроме того, из десятки стран с наибольшим числом командных серверов вышли Япония, Украина и Болгария. Вместо них появились Гонконг, Румыния и Германия.

Так, события 11 сентября 2001 года сопровождались кибератаками на навигационные системы Нью-Йоркского аэропорта. В 2000 года в России неизвестные злоумышленники взломали компьютерную сеть РАО «Газпром» и на некоторое время получили полный контроль над центральным пунктом распределения газовых потоков. В мае и июне 2002 года действовавшие индивидуально британский и австрийский хакеры взломали коды системы управления стратегическими ядерными силами и Центра космической разведки вооруженных сил США. Трудно представить последствия этих акций, если бы они были осуществлены в террористических целях.[25]

Для террористов электронные средства представляют некоторое преимущество по сравнению с физическими. С их помощью можно действовать отдаленно и анонимно, они дешевы, не требуют взрывчатых веществ и миссий самоубийц. Такие теракты вероятно получили бы широкую огласку в СМИ, поскольку и журналисты, и публика заинтересуются виртуальным нападением. Одно известное исследование рисков компьютерных систем начиналось с

[25] Пиджаков, А. Ю. Избранные труды / А. Ю. Пиджаков. – Изд-во «Юридический центр Пресс», 2010. – 574 с.

параграфа, резюмировавшего: «Завтрашний террорист способен с клавиатурой сделать гораздо больше, чем с бомбой»[26].

Выводы по главе один.

В данном разделе были раскрыты основные научные подходы к изучению феномена кибертерроризма, что являлось одной из поставленных задач для достижения основной цели работы.

Было отмечено, что Кибертерроризм является особой формой терроризма, которая направлена на устрашение и иное воздействие на принятие решений различных структур, с помощью использования специального программного обеспечения в киберпространстве.

Были выявлены 2 подхода к понятию кибертерроризма.

Согласно первому понятие кибертерроризма включает в себя группу признаков, связанных с деяниями против компьютеров, сети или информации. Данной позиции придерживаются Д. Деннинг, А.В. Рубанов, а также А. Уразбаев, Ю. В. Гаврилин, Р. Горбенкош и Л. В. Смирнов.

Второй подход к определению понятия «кибертерроризм» делает акцент на целевом характере данных деяний. С данным подходом согласны Р. Гереев, В.А. Мазуров и В. Васенин.

Кибертеррористы и обычные хакеры используют общие тактические средства, но обычно имеют различные мотивы. Исходя из этого, стоит различать категории злоумышленников, с которыми можно столкнуться на кибер-арене. Те же самые хакеры делятся на Whitehat и Blackhat Hackers.

Также хакеры могут обладать политическим мотивом в своих действиях и являться при этом так называемыми хактивистами. Хактивизм - применение ненасильственных, но незаконных или не вполне законных цифровых методов в политических целях. Кроме того, стоит выделить компьютерных преступников,

[26] Denning, D. E. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy / D. E. Denning // Networks and netwars: The future of terror, crime, and militancy. – 2001. – P. 239-288.

занимающихся компьютерным вымогательством, промышленных шпионов, инсайдеров, и, наконец, террористов.

Примером подобного рода террористов является «Объединенный киберхалифат» (United Cyber Caliphate), команда хакеров, которая поддерживает террористическую группировку «Исламское государство». Были рассмотрены приемы, с помощью которых кибертеррористы осуществляют свою деятельность. Исходя из этого было выявлено, что данные приемы постоянно совершенствуются в зависимости от средств защиты, которые применяют разработчики компьютерных сетей.

Помимо всего вышеперечисленного, были исследованы причины возникновения кибертерроризма и условия его функционирования в XXI веке.

Таким образом, причины возникновения кибертерроризма следующие:

- Рентабельность, в сравнении с традиционным терроризмом;
- Кибератаки также не приводят к гибели нападавшего;
- Анонимность (органам безопасности все труднее определять настоящую самобытность террористов);
- Возросшее количество и качество целей (от правительственных военных систем до гражданских экономических и научных сетей, которые все больше становятся зависимыми от информационных технологий);
- Устранение или уменьшение потребности в географической близости к цели, что является ключевым фактором транснационального характера Кибертерроризма;
- Возможность оказывать прямое воздействие на большее число людей чем традиционные террористические методы.

Наибольшее беспокойство вызывает тот факт, что Интернет предоставляет Кибертеррористам возможность глобальных коммуникаций, для планирования и подготовки физических террористических актов. Таким образом, осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой,

религиозной и других форм нетерпимости, а также вовлечение новых членов, финансирование, эффективная и законспирированная связь.

По данным интерактивной карты киберугроз Лаборатории Касперского, в пятерку стран по наибольшему количеству киберугроз на 27 января 2017 года вошли: Россия, Германия, Вьетнам, США, Индия. Данные отображены в приложениях А2 и А3.

На данный момент кибертерроризм вышел уже на новый уровень, связанный с использованием быстроразвивающегося интернета вещей.

Согласно отчету «Лаборатории Касперского», первый квартал 2017 ознаменовался традиционным для начала года спадом числа DDoS-атак. По сравнению с аналогичным периодом предыдущего года количество и сложность атак продолжает расти.

Согласно приложению А1, первое место по числу серверов управления ботнетами остается за Южной Кореей, а на второе вышли США. Нидерланды впервые с апреля 2015 года вытеснили из тройки лидеров Китай, который опустился на седьмую позицию. Россия осталась на четвертом месте. Кроме того, из десятки стран с наибольшим числом командных серверов вышли Япония, Украина и Болгария. Вместо них появились Гонконг, Румыния и Германия.

2 ПРОТИВОРЕЧИЯ, ВЛИЯЮЩИЕ НА ПРОЦЕСС РАЗРАБОТКИ И РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМА.

Современная ситуация требует скорейшей разработки правовых механизмов предотвращения и пресечения террористического поведения в киберпространстве. Среди них прежде всего необходимо обратить внимание на гармонизацию национальных законодательств в данной сфере, совершенствование универсальной системы по техническому контролю и сопровождению работы Интернета, разработку правил взаимодействия государств в части предупреждения и прекращения преступных деяний, а также привлечения к ответственности лиц, виновных в их совершении[27].

Одри Курт Кронин утверждает, что «Интернет, эффективный инструмент распространения гражданского общества и демократических идеалов, также предоставляет средства для распространения идеологий насилия, координации преступного поведения, обмена боевой тактикой, исследования мощного оружия и подрыва традиционных инструментов порядка». Как заявил председатель Объединенного комитета начальников штабов армии, генерал Мартин Э. Демпси, «распространение цифровых технологий не было безрезультатным. Это также ввело новые опасности для нашей безопасности. Игнорируйте на свой страх и риск. Кибер-атака на критическую инфраструктуру США со стороны террористической организации, транснациональной преступной организации или «одинокого волка», действуя от имени государства-изгоя из безопасной гавани и

[27] Чернядьева, Н. А. Международный терроризм: происхождение, эволюция, актуальные вопросы правового противодействия. Монография / Н. А. Чернядьева. – «Издательство «Проспект»», 2016. – С. 132.

вне пределов досягаемости властей, может привести к следующему «Цифровому Перл-Харбору»[28].

Существует мнение, что потенциальная опасность кибертерроризма сильно преувеличена. Брюс Шнайер полагает, что преувеличенное внимание к угрозе кибертерроризма отвлекает от проблем, настоящих связанных кибербезопасностью. А. Астахов провёл обзор основных мифов, которые связанны с кибертерроризмом, и пришёл к выводу о том, что крайне редко кибертерроризм может нарушить системы жизнеобеспечения и привести к гибели людей. Для этого кибертеррористам нужно не только получить доступ к определенным системам, но и обладать специальными техническими навыками и знаниями.

Иной точки зрения придерживается М.Е. Бауман, сравнивая электронный эквивалент терроризма с монгольским нашествием, произошедшим 7 столетий назад. Как и кибертеррористы, монголы прерывали коммуникации, атаковали в выбранные ими место и время, а также посылали грозные предупреждения.

Кибертерроризм необходимо рассматривать как составную часть компьютерной преступности. Луис Шелли отмечает, что «террористы и транснациональные преступники используют одни и те же стратегии для осуществления своих действий, главным образом используя компьютерные технологии для планирования и осуществления своей деятельности»[29].

Террористы будут придумывать что-то новое, подразделения по борьбе с террористами – разрабатывать контрмеры. Для ликвидации террористической сети может оказаться недостаточным заключить в тюрьму её участников. Власти, могут решить, что слишком опасно допустить, чтобы кто-то из жителей страны

[28] De Arimatéia da Cruz, J. Terrorism, War, and Cyber (In)Security [Электронный ресурс] / J. de Arimatéia da Cruz // Small Wars Journal. – 2013. – October 27. – Режим доступа: http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity, свободный. – Загл. с экрана.

[29] Талимончик, В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – ООО «Юридический центр-Пресс», 2017. – С.390.

находился «вне доступа», то есть не был подключен к технологической инфраструктуре. Понятно, что в будущем, как и сегодня, некоторые люди не пожелают пользоваться современными технологиями, онлайн-системами и смартфонами, иметь виртуальные профили. Власти могут решить, что им есть что скрывать, и в качестве контртеррористической меры создать своего рода реестр таких «людей-невидимок». И если у вас нет ни одного зарегистрированного аккаунта социальных сетей и номера сотовой связи и почти невозможно найти ссылки на вас в интернете, Вас могут посчитать кандидатом на включение в такой реестр. А попав в него, вы станете объектом отдельного регулирования, включая более тщательный досмотр в аэропортах или даже ограничения на перемещения по миру.

После терактов 9 сентября 2001 года даже страны с исторически сложившейся традицией гражданских свобод все чаще пренебрегают защитой граждан в пользу системы, повышающей безопасность и устойчивость государства. И эта тенденция будет усиливаться. После нескольких успешных атак кибертеррористов намного легче убедить людей пожертвовать чем-то, в частности согласиться, чтобы Власти имели возможность более жестко контролировать нашу активность в интернете, ради спокойствия, которое принесут эти новые меры. Побочным эффектом такого сценария помимо гонений на небольшое количество безвредных отшельников будет опасность роста числа злоупотреблений или судебных ошибок, которые допускают представители власти. Это еще одна причина продолжить борьбу за безопасность и сохранение тайны частной жизни. В ближайшие годы привычное для цифровой эпохи «перетягивание каната» между приватностью и безопасностью станет особенно заметным.

Ведомствам, которые отвечают за поиск, выслеживание и поимку опасных лиц, потребуются для этого очень сложные системы управления данными[30].

[30] Шмидт, Э. Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – С.172.

Несмотря на все меры, которые принимают для защиты тайны частной жизни пользователи, компании и неправительственные организации, эти системы неизбежно будут получать информацию о людях, не имеющих к терроризму никакого отношения. Вопрос лишь в том, как много и из каких источников. Пока большая часть сведений, которые правительство собирает о населении — адреса, номера паспортов, история правонарушений, данные операторов сотовой связи, — хранится в разных местах, а в некоторых странах до сих пор даже не оцифрована). Отдельное хранение повышает уровень приватности для граждан, но резко снижает эффективность работы правоохранительных органов.

Это та самая «большая проблема данных», с которой столкнулись власти во всем мире: как спецслужбам, армии и правоохранительным органам интегрировать все свои базы данных в единую централизованную систему, чтобы можно было сопоставлять информацию, не нарушая права граждан на частную жизнь? Так, в США ФБР, Госдепартамент, ЦРУ и другие ведомства пользуются разными базами. Компьютеры определяют зависимости, аномалии и прочие значимые акторы намного эффективнее, чем люди, но объединение различных информационных систем (с паспортными данными, отпечатками пальцев, движением по банковским счетам, результатами прослушки телефонных разговоров, данными авиакомпаний) и создание алгоритмов для эффективной установки перекрестных ссылок, удаления избыточной информации и обнаружения сигналов тревоги является невероятно трудной задачей, требующей огромных затрат времени.

Пугающе высок риск неправомерного использования этой мощи, не говоря уже об опасностях, связанных с человеческими ошибками, неверными выводами по результатам анализа данных и простым любопытством. Возможно, полностью интегрированная информационная система, которая получает данные всеми возможными способами и оснащена программным обеспечением, способным интерпретировать и прогнозировать поведение людей, и при этом управляется человеком, обладает слишком большой мощью, чтобы кто-то мог взять на себя

ответственность за нее? Более того, однажды созданная, такая система никогда не будет уничтожена. Даже если когда-нибудь вопрос безопасности станет менее острым, разве правительство откажется по своей воле от столь мощного средства поддержания общественного порядка? Но что будет, если другое правительство окажется менее осторожным или более безответственным по отношению к информации, которой располагает? Такие полностью интегрированные информационные системы пока находятся в зачаточном состоянии. Конечно же, предстоит преодолеть некоторые недочеты такие как нестабильность сбора данных), ограничивающие их эффективность.

Постепенно такие системы будут развиваться и, вероятно, вскоре получат повсеместное распространение. А единственным лекарством от потенциальной электронной тирании остается укрепление правового поля и развитие гражданского общества, которое должно быть активным и не допускать злоупотребления этой огромной властью[31].

В настоящее время проблематика международной информационной безопасности и глобального управления Интернетом выдвинулась на центральное место в перечне вызовов международной безопасности. Так, поражение объектов иранской ядерной инфраструктуры вирусом Stuxnet было включено российскими и американскими аналитиками в число самых заметных событий в области международной безопасности 2010 года.

В июне 2010 года в компьютерной системе Иранского центра по обогащению урана был обнаружен вирус, получивший название Stuxnet, изменивший скорости вращения центрифуг, что привело к их выходу из строя. Именно этот инцидент вынудил многие развитые страны пойти на укрепление защиты своих жизненно важных промышленных объектов - в частности, в энергетике и водоснабжении. Ведь стало очевидно, что подобные вещи могут происходить и в других странах, и на других объектах. То есть при помощи компьютерного кода можно выводить

[31] Шмидт, Э. Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – С.176.

из строя совершенно не компьютерные объекты. Или, наоборот, приводить их в действие[32].

Успешность решения задачи пресечения деятельности экстремистских и террористических организаций в информационном пространстве во многом зависит от глубокой теоретической проработки данной проблемы. Но до сих пор отсутствуют даже общепринятые определения кибертерроризма и киберэкстремизма как порожденных глобализацией явлений, представляющих особую опасность для личности, общества и государства.

С 80-х гг. XX века в большинстве стран пришли к выводу, согласно которому правовая защита компьютерной информации при помощи общих положений национального уголовного законодательства является недостаточной. Мировое сообщество осознало, что эффективное решение проблемы компьютерной преступности требует согласованных международных действий и сотрудничества.

Перечислим основные факторы, которые осложняют противодействие киберэкстремизму и кибертерроризму.

Во-первых, развитие права и законодательства заметно отстает от процесса формирования новых инфокоммуникационных технологий, которые могут быть использованы террористическими и экстремистскими организациями. Существующее законодательство (как зарубежное, так и российское) носит во многом декларативный характер. Оно ограничивается в основном общими положениями о недопустимости распространения экстремистской и террористической информации в Интернете, но слабо детализирует объективные критерии недопустимых информационных сообщений, механизмы мониторинга Интернета и удаления запрещенного контента.

[32] Повышев, В. Борьба с киберпреступностью и кибертерроризмом. Доклад эксперта. [Электронный ресурс] / В. Повышев // Международная Молодёжная Конференция Тюменская Модель ООН-2012. Совет по правам человека. – Томский государственный университет, 2012. – Режим доступа: http://sartraccc.ru/Pub_inter/cybercrim.pdf, свободный. – Загл. с экрана.

Во-вторых, в условиях повышения приоритета инструментов международного управления необходимо иметь ввиду, что Интернет создан и функционирует, благодаря глобальным принципам построения, а значит и система противодействия интернет-терроризму и экстремизму также должна строится во многом на основе международного сотрудничества. Речь идет о взаимодействии разработчиков специализированных технических средств, правоохранительных органов обмене информацией, взаимном признании тех или иных организаций террористическими или экстремистскими, формировании единых списков таких организаций.

В-третьих, отсутствуют эффективные методики диалектического сочетания механизмов саморегулирования и действующих норм законодательства в данной сфере. По мнению многих экспертов, для соблюдения баланса гражданских прав и свобод, а также ограничительных мер необходимо шире задействовать институты саморегуляции интернет-сообщества с использованием потенциала гражданского общества. В этих целях общественные организации должны с нравственных, социально-политических, национальных (и, возможно, религиозных) позиций участвовать в оценке допустимости контента информационных ресурсов и выработке критериев признания информационных ресурсов террористическими или экстремистскими.

Всё это поможет в осуществлении эффективного противодействия использованию террористами и экстремистами возможностей Интернета, не прибегая к чрезмерному административному вмешательству в развитие Глобальной Сети.

Представляется, что для решения выше обозначенных проблем понадобятся институциональные инновации как законодательные, направленные на

совершенствование законодательных норм, так и организационные, которые нацеленны на улучшение правоприменения[33].

Выводы по главе два.

Задачей данной главы было выявить противоречия, влияющие на процесс разработки и реализации политики противодействия кибертерроризму.

На сегодняшний день требуется разработать правовые механизмы предотвращения и пресечения террористического поведения в киберпространстве.

Однако, существует мнение, что потенциальная опасность кибертерроризма сильно преувеличена и отвлекает от проблем, настоящих связанных кибербезопасностью. Данной точки зрения придерживаются Брюс Шнайер и А. Астахов. По их мнению, крайне редко кибертерроризм может нарушить системы жизнеобеспечения и привести к гибели людей.

Также существует иное мнение, что Кибертерроризм необходимо рассматривать как составную часть компьютерной преступности.

Террористы будут придумывать что-то новое, подразделения по борьбе с террористами – разрабатывать контрмеры. Для того, чтобы ликвидировать террористическую сеть, может оказаться недостаточным заключить в тюрьму её участников. Ведомствам, отвечающим за поиск, выслеживание и поимку опасных лиц, понадобятся для этого очень сложные системы управления данными. Эти организации будут неизбежно получать информацию о людях, которые не имеют к терроризму никакого отношения. Более того, отдельное хранение подобного рода информации резко снижает эффективность работы правоохранительных органов.

[33] Клементьев, А.С. Противодействие кибертерроризму и киберэкстремизму: новая сфера правоохранительной деятельности / А.С. Клементьев, Е.В. Ткач // Противодейтсвие Терроризму Проблемы XXI века. Информационно-аналитический и научно-практический журнал. – 2013. – С.25-30.

Таким образом, появляется "большая проблема данных" - как интегрировать все свои базы данных в единую централизованную систему, чтобы можно было сопоставлять информацию, не нарушая права граждан на частную жизнь?

Кроме всего вышеперечисленного, настораживает риск неправомерного использования мощи данной централизованной системы. Однако, единственным средством от потенциальной электронной тирании остается укрепление правового поля и развитие гражданского общества, которому необходимо быть активным и не допускать злоупотребления такой огромной властью.

С 80-х гг. XX века в большинстве стран пришли к выводу, что общих положений национального уголовного законодательства недостаточно для решения проблемы с компьютерной преступностью. Тем самым возросла необходимость согласованных международных действий и сотрудничества.

Однако существуют факторы, осложняющие противодействие киберэкстремизму и кибертерроризму:

§ Развитие права и законодательства сильно отстает от процесса формирования новых инфокоммуникационных технологий;

§ Решение данной проблемы необходимо принимать и осуществлять на международном уровне (речь идет о сотрудничестве, обмене информацией, признание тех или иных организаций террористическими или экстремистскими);

§ Отсутствуют механизмы саморегулирования и действующих норм законодательства в данной сфере.

Было выявлено, что для решения обозначенных выше проблем необходимы институциональные инновации, как законодательные, так и организационные.

3 МЕЖДУНАРОДНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

Успех каждой страны по защите национальных секторов инфраструктуры в значительной степени будет зависеть от усилий всего мирового сообщества по созданию защищенного и безопасного мирового информационного пространства. Только технологии и только внутренняя политика не могут обеспечить эффективную защиту от компьютерной преступности и кибертерроризма. Данное обстоятельство показывает необходимость широкого международного взаимодействия и сотрудничества в решении проблем обеспечения международной информационной безопасности.

Также хотелось бы отметить что, несмотря на принимаемые во всем мире меры безопасности, угроза кибертерроризма остаётся, а в отдельных информационно развитых странах (США, Япония, Великобритания) постоянно обостряется. Поэтому успешное решение этой проблемы возможно лишь с помощью совместных усилий всех информационно развитых стран и с использованием при этом принципов планомерности и системного подхода[34].

То, насколько серьезно люди воспринимают угрозу кибертерроризма, похоже, зависит от их отношения к хакерам. Некоторых образ подростка, взламывающего защиту офисной АТС ради забавы. Однако за последние десять лет хакеры сильно изменились, а взлом систем превратился из хобби в довольно обыденное, хотя и неоднозначное занятие.

Хакеры начнут все чаще объединяться вокруг какой-то общей задачи. Они будут тщательно планировать атаки на тех, кого сочтут подходящей целью, а затем активно делиться информацией о своих успехах. Эти группы окажутся в

[34] Бегишев, И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически-важных и потенциально-опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. – 2010. – №1(6). – С.9-13.

зоне постоянного внимания со стороны органов власти и институтов, становящихся объектами их атак[35].

Помимо использования Интернета для начала кибератаки против национальных государств, террористические организации могут использовать Интернет для проведения хактивизма.

На протяжении многих лет различные ведомства, подобные Агентству передовых оборонных исследовательских проектов США (DARPA) и Агентству национальной безопасности (NSA), набирают талантливых специалистов в ходе таких мероприятий, как серия конференций по компьютерной безопасности Black Hat и съезд хакеров Def Con. В 2011 году DARPA объявило о запуске новой программы Cyber Fast Track (CFT), созданной бывшим хакером, менеджером проектов в DARPA.

Она была направлена на углубление и упорядочение сотрудничества с этими сообществами. В рамках CFT агентство привлекает отдельных специалистов и небольшие компании к работе над краткосрочными целевыми проектами в области сетевой безопасности.

Эта инициатива направлена на работу с мелкими игроками, и ее отличает возможность быстро одобрять выделение грантов. В течение первых двух месяцев после запуска программы DARPA одобрило заключение восьми контрактов — иными словами, оно работает со скоростью света по сравнению с нормальными для государственных ведомств темпами. Это позволяет опытным специалистам, которые иначе вряд ли согласились бы работать на правительство, внести свой вклад в важное дело укрепления кибербезопасности, причем легко и в те временные рамки, которые соответствуют срочности задачи. Программа CFT

[35] Шмидт, Э. Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – С.185.

стала одним из признаков сдвига агентства в сторону «демократических инноваций с использованием краудсорсинга»[36].

Появление компьютерных преступлений транснационального характера сделало очевидным вывод о том, что ни одно государство не может бороться с ними в одиночку. Как следствие появилась необходимость международного сотрудничества[37].

Организационные меры по борьбе с кибертерроризмом принимаются как на международном, так и на национальном уровнях. Впервые вопрос о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности был вынесен на рассмотрение ООН в декабре 1998 г., когда по инициативе Российской Федерации Генеральной Ассамблеей (ГА) была принята первая резолюция, затрагивающая эту проблему. С тех пор Генеральный секретарь ежегодно представляет ГА ООН доклады, в которых государства-члены ООН выражают свое мнение по этому вопросу и подчеркивают необходимость коллективных действий, направленных на практическое сотрудничество в целях обмена передовым опытом и информацией. Кроме того, было создано две группы правительственных экспертов.

Первая из них проводила заседания в 2004 и 2005 гг., но с учетом сравнительной новизны вопросов, связанных с защитой киберпространства, так и не смогла достичь консенсуса в отношении заключительных выводов.

Новая группа начала работу в 2009 г. и к 2010 г. сумела не только завершить обсуждения, но и согласовать доклад, посвященный существующим и потенциальным угрозам киберпространства и изучению возможных коллективных мер по их устранению. В дальнейшем было принято решение продолжить эту работу, чтобы развить данное направление международного

[36] Шмидт, Э., Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – С.189.

[37] Талимончик, В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – ООО «Юридический центр-Пресс», 2011. – С.365.

сотрудничества и, возможно, перевести его из разряда обсуждений в число регулируемых сфер жизнедеятельности.

Также на международном уровне действует Конвенция о компьютерных преступлениях, подписанная государствами-членами Совета Европы в Будапеште 23 ноября 2001 г. Этот документ устанавливает порядок взаимодействия стран в борьбе с преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем, а также всеми видами правонарушений, связанных с использованием компьютерных средств, с содержанием данных и с нарушением авторских и смежных прав. Многие меры, предусмотренные Конвенцией и направленные на недопущение несанкционированного вмешательства в работу компьютерных систем, могут выступить своеобразным заслоном на пути к совершению террористических преступлений[38].

Россия, однако, отказалась подписывать данную Конвенцию, поскольку уполномоченных должностных лиц не устроило содержание пункта «b» ст. 32, которым предусматривается санкционированный доступ одного государства-участника к компьютерным данным, хранящимся на территории другого государства, без предварительного получения согласия последнего.

В приведенной формулировке российская сторона усмотрела возможность нанесения ущерба суверенитету и национальной безопасности государств-участников[39].

Трудно не согласиться с Фрэнком Барнаби, который в монографии «Будущее террора» утверждает, что кибертеррорист с ноутбуком способен нанести больше

---

[38] Конвенция Совета Европы о компьютерных преступлениях [Электронный ресурс] // Бюро договоров. – Совет Европы, 2017. – Режим доступа: http://www.coe.int/ru/web/conventions/search-on-treaties/-/conventions/treaty/185, свободный. – Загл. с экрана.

[39] Капитонова, Е.А. Особенности кибертерроризма как новой разновидности террористического акта / Е.А. Капитонова // Известия ВУЗов. Поволжский регион. Общественные науки. – 2015. – №2 (34). – С. 29-41.

вреда, нежели террорист, вооруженный бомбами и иными взрывчатыми веществами. Именно международный терроризм активно использует компьютерные сети в своей деятельности. Совладать с массовым распространением киберпреступлений сложно, но можно путем принятия всесторонних мер.

Прежде всего, необходима четкая и последовательная международная политика по противостоянию кибертеррору. Нужна высококвалифицированная разведка. Особо важна работа правоохранительных органов и вооруженных сил, нацеленная на предотвращение техногенного и кибернетического террора. Поскольку компьютерный терроризм — уже реальность сегодняшнего дня, необходимо закрепить на законодательном уровне обязанность государственных и частных структур по принятию технических мер, обеспечивающих защиту компьютерных сетей, как одного из наиболее уязвимых элементов современного общества.

Вероятно, в ближайшие годы в России придется применить экстренные меры для обеспечения кибербезопасности. И подобные поручения уже прозвучали из уст Президента России 21 января 2013 года, когда В.В. Путин дал поручение ФСБ создать антихакерскую систему.

Напомним, что большинство развитых стран уже формируют кибервойска и ведут работу по формированию кибербезопасности[40].

Так в 2011 году, Президент США определил 10 экстренных мер необходимых для реализации стратегии кибербезопасности:

1. Учредить подразделения кибер-полиции, которые бы отвечали за обеспечение кибербезопасности.

2. Подготовить обновленную национальную стратегию по обеспечению информационной и коммуникационной инфраструктуры.

[40]Акопов, Г.Л. Хактивизм как неотъемлемый элемент современных информационных войн / Г.Л. Акопов // Национальная безопасность. – 2014. – №3(32). – С.438-444.

3. Передать контроль за кибербезопасностью в прямое управление Президента США и установить показатели, определяющие ее эффективность.

4. Обеспечить конфиденциальность и гражданские свободы в рамках работы национальной секретной службы кибербезопасности.

5. Провести межведомственный нормативно-правовой анализ, по определению приоритетных вопросов в области кибербезопасности.

6. Инициировать национальную информационно-просветительскую кампанию содействия кибербезопасности.

7. Разработать единый международный план действий по обеспечению кибербезопасности и укрепления международных партнеров США.

8. Подготовить ответ кибератакам: инициировать план действий и начать диалог для укрепления государственно-частного партнерства.

9. Разработать основу для исследований применения новейших технологий, которые могли бы обеспечить повышение безопасности, надежности и устойчивости работы цифровой инфраструктуры.

10. Принять протокол кибербезопасности, основанный на стратегии управления и обеспечения конфиденциальности технологий повышения национальной безопасности[41].

Вышеуказанные меры необходимо внедрить во всех цивилизованных государствах, т.к. Интернет дает уникальную возможность применения инновационных технологий в «подрывной» деятельности в целях политического воздействия.

Увеличение масштабов социальной опасности противоправных деяний в информационной сфере обуславливает необходимость повысить защищенность критически важных объектов информационной инфраструктуры, усилить

[41] Cybersecurity 3 апреля 2011 [Электронный ресурс] // Официальный сайт Президента США. – Режим доступа: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity, свободный. – Загл. с экрана.

противодействие угрозе распространения компьютерной преступности и ее крайней формы— кибертерроризма.

Известно, что уже 12 сентября 2001 года, на следующий день после теракта в Нью-Йорке, Национальный центр защиты инфраструктуры при ФБР провел чрезвычайное заседание чтобы оценить возможные угрозы кибертерроризма. Защита объектов критически важных инфраструктур от деструктивных воздействий в террористических целях является одной из актуальных задач современной цивилизации. Осознавая важность ее решения, многие страны координируют свою деятельность в данном направлении с учетом национальных интересов, а также экономических и технологических возможностей.

Надежную гарантированную защиту многочисленных, потенциально уязвимых для такого рода угроз критически значимых для государства объектов возможно обеспечить только при условии существования отлаженной системы национального масштаба. Данная система должна как распознавать возможные угрозы, так и противодействовать разнообразным формам их проявления и реализации, а также минимизировать возможный ущерб от атак. Исследования для решения такой сложной и важной задачи ведутся во многих государствах мира, в том числе и в России.

Характер новых, стратегически значимых угроз информационной безопасности, в том числе — компьютерный терроризм и компьютерная преступность, вызывают необходимость ужесточить политику обеспечения безопасности информационных систем и сетей государства.

Во-первых, данная политика должна ориентироваться на обеспечение безопасного функционирования информационной инфраструктуры государства, в том числе систем управления критических инфраструктур.

Во-вторых, необходимо максимально снизить число присущих таким объектам уязвимостей и угроз, а также минимизировать количество возможных атак и их последствия.

В-третьих, такая политика должна обеспечивать не только непрерывность, адекватность и своевременность мер по противодействию возможным угрозам, но и непрерывный контроль и анализ их защищенности[42].

[42] Шерстюк, В. П. Проблемы противодействия компьютерной преступности и кибертерроризму / В. П. Шерстюк // Материалы Первой всероссийской научно-практической конференции «Формирование устойчивой антитеррористической позиции гражданского общества как основы профилактики терроризма». – М.: МЦНМО, 2009. – 512 с. – С.43-52.

ВЫВОДЫ ПО ГЛАВЕ 3

Задачей данной главы является выявление значения международного опыта противодействия кибертерроризму для разработки и эффективной реализации данного вида политики в современной России.

Несмотря на меры безопасности, принимаемые во всем мире, угроза кибертерроризма не исчезает, а в некоторых странах постоянно обостряется. Данную проблему можно решить только при помощи совместных усилий всех информационно развитых стран.

В рамках данного сотрудничества, многие ведомства набирают талантливых специалистов (хакеров) в ходе конференций по кибербезопасности. Это позволяет опытным специалистам (хакерам), которые иначе вряд ли согласились бы работать на правительство, внести свой вклад в важное дело.

Также стоит отметить принятие резолюций по данной тематике в ООН. Впервые это произошло в декабре 1998 года.

С тех пор Генсек ежегодно представляет ГенАссамблее ООН доклады, в которых государства-члены ООН выражают свое мнение по выделенным вопросам и выявляют необходимость коллективных действий. Помимо этого, были созданы группы правительственных экспертов, которые к 2010-му году смогли согласовать доклад, посвященный угрозам киберпространства и изучению возможных коллективных мер по их устранению.

Кроме того, на международном уровне действует Конвенция о компьютерных преступлениях, от 23 ноября 2001 года, которая устанавливает порядок взаимодействия стран в борьбе с преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем, а также всеми видами правонарушений, связанных с использованием компьютерных средств, с содержанием данных и с нарушением авторских и смежных прав.

Однако, Россия не приняла данную конвенцию в связи с тем, что существует риск нанести ущерб суверенитету и национальной безопасности государств-участников.

Как выяснилось, большинство развитых стран уже занимаются формированием кибервойск и ведут работу по усилению кибербезопасности.

Так в 2011 году в США были обозначены меры для реализации стратегии кибербезопасности.

К тому же, было выявлено, что исследования для создания национальной системы защиты объектов критически важных инфраструктур ведутся во многих странах мира, а также и в России.

4. ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В РОССИИ

Большинство стран в своём законодательстве чётко прописывают, что подразумевается под понятием «терроризм». Зачастую, подобные определения даются в рамках концепций противодействия терроризму. Так, в российском законодательстве в Федеральном Законе «О противодействии терроризму»[43] даётся следующее понятие: Терроризм – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий. Также Уголовный кодекс Российской Федерации даёт более узкое определение, позволяющее точечно классифицировать преступное действие как терроризм. Согласно статье 205 Уголовного Кодекса Российской Федерации, терроризм – это совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях.

Однако в Российской Федерации термин "кибертерроризм" легально не закреплен ни в одном нормативно-правовом акте. Уголовная ответственность за совершение террористического акт предусмотрена ст. 205 УК РФ[44], при этом

---

[43] Федеральный закон от 6 марта 2006 г. N 35-ФЗ О противодействии терроризму [Электронный ресурс] // Российская газета. – 2006. – 10 марта. – №4014(0). – Режим доступа: https://rg.ru/2006/03/10/borba-terrorizm.html. – Загл. с экрана.

[44] Статья 205. Террористический акт [Электронный ресурс] // «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 17.04.2017). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/, свободный. – Загл. с экрана.

квалифицированного признака, связанного с осуществлением данного акта в киберпространстве, российский Уголовный кодекс не предусматривает. Нельзя сказать, что кибертерроризм вовсе отсутствует в нормативном поле Российской Федерации. Так кибертерроризм употребляется в контексте подготовки специалистов для противодействия терроризму.

Также Российская Федерация имеет множество двусторонних договоров о правовой помощи по уголовным делам с иностранными государствами. При наличии между РФ и иностранным государством указанного выше соглашения на основании ст. 453 УПК РФ[45] суд, прокурор, следователь, руководитель следственного органа, дознаватель при необходимости вносит запрос о производстве необходимого следственного или иного действия компетентным органом или должностным лицом иностранного государства в соответствии с международным договором Российской Федерации, международным соглашением или на основе принципа взаимности. Наличие договоров о правовой помощи является полезным элементом сотрудничества в вопросах борьбы преступности, но для борьбы с такой угрозой как кибертерроризм, на наш взгляд, требуется более гибкая структура, т.к. направление и исполнение запросов о правовой помощи довольно долгая процедура.

В 2006 году В.В. Путин высказал предложение по разработке глобальной стратегии по борьбе с кибертерроризмом. Европейская Конвенция о преступности в сфере компьютерной информации 23 ноября 2001 года до сих пор не распространяется на РФ и страны СНГ, не являющихся участниками (договаривающимися сторонами) по данной конвенции.

[45] Статья 453. Направление запроса о правовой помощи [Электронный ресурс] // «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 N 174-ФЗ (ред. от 07.06.2017). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34481/14b49be9d968092a8e33b246ddbf5950cc6185a5/. – Загл. с экрана.

Для того чтобы обеспечить информационную безопасность РФ 15 января 2013 года Указом Президента РФ № 31-с на ФСБ РФ были возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ[46].

Основными задачами вышеуказанной структуры стали:

1. Прогнозировать ситуации в сфере обеспечения информационной безопасности РФ;

2. Обеспечить взаимодействие владельцев информационных ресурсов РФ, операторов связи, иных субъектов, которые осуществляют лицензируемую деятельность в сфере защиты информации, при решении вопросов по обнаружению, предупреждению и ликвидации последствий компьютерных атак;

3. Контролировать степень защищенности критической информационной инфраструктуры РФ от компьютерных атак;

4. Устанавливать причины компьютерных инцидентов, которые связанны с функционированием информационных ресурсов РФ.

Таким образом, на сегодняшний день в РФ нет основополагающего и соответствующего современным реалиям и вызовам документа, который бы объяснял, как быть с кибербезопасностью на национальном уровне. Вместо структурированной системы регламентов в российской практике есть ряд декларативных документов (Доктрина информационной безопасности, Стратегия национальной безопасности до 2020 года, проект Концепции стратегии кибербезопасности и другие), а также пакеты ограничивающих и запрещающих законов и поправок. Подобных мер недостаточно для создания гибкой и эффективной системы безопасности в киберсреде. Потому перед РФ стоит

[46] Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс] // Российская газета. – 2013. – 18 января. - ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2013/01/18/komp-ataki-site-dok.html. – Загл. с экрана.

большая работа по разработке национальных стандартов и их гармонизации с международными нормами.

Примечательно, что национальные стратегии безопасности в сети появились сравнительно недавно. США как один из лидеров в развитии данного направления обзавелись стратегией национальной кибербезопасности только в 2003 году. К примеру, Франция выработала свои нормы и правила только в 2011 году, а единая стратегия для ЕС появилась только в феврале 2013 года.

В 2014 году в стратегиях информационной безопасности нового поколения значительно сместились акценты. Если раньше государство ориентировалось на защиту граждан и организаций, то теперь – на общество и институты в целом. Это связано с ростом роли Интернета в экономике и государственном управлении, а также с потенциальными угрозами от других стран. Т.е. проблемы кибербезопасности от частных проблем буквально за 20 лет выросли до межгосударственного уровня. Поэтому поощряется межведомственное взаимодействие и государственно-частное партнерство внутри стран и межгосударственное сотрудничество снаружи[47].

Развитие получило сотрудничество в борьбе с криминалом на двустороннем уровне, где общий знаменатель доверия, как правило, более высок. У РФ свыше двух десятков постоянно действующих рабочих групп и иных консультационных механизмов в этой сфере с зарубежными странами, в том числе рабочие группы по борьбе с терроризмом, противодействию незаконному обороту наркотиков в рамках российско-американской Президентской комиссии. А недавно к ним добавилась и подгруппа по кибербезопасности[48].

---

[47] Корнев, М. Суверенная кибербезопасность: как глобальные проблемы влияют на ограничения медиа в интернете? / М. Корнев // Журналист. – 2015. – №02. – ООО Медиагруппа «Журналист», 2017. – Режим доступа: http://mediatoolbox.ru/blog/suverennaya-kiber-bezopasnost-kak-globalnyie-problemyi-vliyayut-na-ogranicheniya-media-v-internete/, свободный. – Загл. с экрана.

[48] Змеевский, А.В. О международном сотрудничестве в борьбе с криминальными вызовами и угрозами [Электронный ресурс] / А.В. Змеевский // Международная жизнь. – 2013. – № 6. –

В ходе интервью заместителя Министра иностранных дел России О.В. Сыромолотова МИА (Международное информационное агентство) «Россия сегодня», 30 сентября 2016 года было заявлено, что «надо создать ответственные правила поведения стран в Интернете. Кроме того, в Интернете должны соблюдаться права граждан всех стран. Соответственно, должны быть установлены суверенитеты государств в своем сегменте сети и право всех стран участвовать в управлении Интернетом. Это основные положения, которые необходимы для того, чтобы существовал относительный порядок в Интернете, чтобы он не служил террористам. Информационная безопасность входит в тематику противодействия новым вызовам и угрозам наряду с терроризмом. Противодействие террору – это не только борьба непосредственно с террористами, это противодействие финансированию терроризма, противодействие наркоугрозе, которая служит ему подпиткой, противодействие организованной преступности и информационная безопасность. Если говорить о сотрудничестве с другими странами, например, у нас (РФ) когда-то существовала с США правительственная комиссия по различным аспектам и, в том числе по информационной безопасности. И сейчас мы (РФ) с США возобновили контакты по информационной безопасности. В Женеве были проведены переговоры по этой проблематике»[49].

Кроме того, в рамках таких международных организаций, как БРИКС и ШОС, в которых Россия принимает активное участие, проходят ежегодные

МИД РФ, Редакция журнала «Международная жизнь», 2017. – Режим доступа: http://www.mid.ru/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/103630, свободный. – Загл. с экрана.

[49] Интервью заместителя Министра иностранных дел России О.В. Сыромолотова МИА «Россия сегодня» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2016. – 30 сентября. – Министерство иностранных дел Российской Федерации, 2017. – Режим доступа: http://www.mid.ru/web/guest/foreign_policy/international_safety/crime/-/asset_publisher/3F5lZsLVSx4R/content/id/2480829, свободный. – Загл. с экрана.

консультации по международной информационной безопасности. В обсуждении со многими странами Евросоюза эта тема также присутствует.

Также в специальной группе АТЭС по борьбе с терроризмом в партнерстве с американским председательством по инициативе России продвигаются такие актуальные вопросы как противодействие отмыванию денег и финансированию терроризма, обеспечение транспортной и международной информационной безопасности. В формате Регионального форума АСЕАН по безопасности (АРФ) Россия совместно с Австралией взяли на себя лидирующую роль в продвижении темы борьбы с кибертерроризмом[50].

В своем интервью заместитель Министра иностранных дел России И.В. Моргулова японскому информагентству «Jiji Press» 17 марта 2017 года ответила, что в последнее время российско-японский диалог по антитеррористической тематике активно развивается на различных уровнях. Эта тема обсуждается в ходе контактов руководителей советов безопасности двух стран, министров иностранных дел, профильных межмидовских консультаций. По отдельным аспектам, в частности, по борьбе с кибертерроризмом, мы (РФ и Япония) уже близки к выходу на более тесные формы координации, в том числе рассматриваем возможность подготовки соответствующих двусторонних документов. У нас также есть успешный опыт совместной реализации под эгидой ООН антинаркотического проекта в Афганистане. Все это создает

[50] Выступление спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в борьбе с терроризмом и транснациональной организованной преступностью А.В. Змеевского в рамках «Дипломатического клуба» на тему «Новые вызовы и угрозы - антикриминальный срез» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2012. – 19 декабря. - Министерство иностранных дел Российской Федерации, 2017. – Режим доступа: http://www.mid.ru/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/129206, свободный. – Загл. с экрана.

хорошую базу для расширения взаимодействия в данной сфере, которое, безусловно, отвечает интересам обеих стран[51].

13 октября 2016 года в Москве прошла крупнейшая в Восточной Европе конференция по кибербезопасности CyberCrimeCon. Представители Интерпола и Европола, а также ведущих европейских компаний и банков рассказали о главных хакерских угрозах для бизнеса и простых пользователей сети[52].

Вице-президент корпорации ICANN в Восточной Европе и Центральной Азии Михаил Якушев в ходе данной конференции заявил, что с кибероружием необходимо бороться на национальном уровне. Он предлагает применение для этого опыт по регулированию ядерного оружия. По его словам, несколько лет назад эту идею уже озвучивала Россия, но никаких конкретных документов так и не было разработано по данному направлению. В этой связи необходимо актуализировать эту работу[53].

С вице-президентом ICANN согласен гендиректор и основатель компании Group-IB Илья Сачков: «Инструментами, помогающими преступникам красть миллионы у крупнейших банков, теперь интересуются кибертеррористы, которые уже сегодня активно рекрутируют хакеров на закрытых площадках. Только

---

[51] Интервью заместителя Министра иностранных дел России И.В. Моргулова японскому информагентству «Дзи-Дзи Пресс» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2017. – 17 марта. – Министерство иностранных дел Российской Федерации, 2017. – Режим доступа: http://www.mid.ru/web/guest/maps/jp/-/asset_publisher/zMUsqsVU9NDU/content/id/2694158, свободный. – Загл. с экрана.

[52] Гринштейн, Г. Как влияют тренды кибербезопасности на рынок хищений денежных средств [Электронный ресурс] / Г. Гринштейн // Хабрахабр. – 2016. – 15 октября. – «ТМ», 2017. – Режим доступа: https://habrahabr.ru/post/312720/, свободный. – Загл. с экрана.

[53] ICANN выступает за запрет кибероружия на национальном уровне [Электронный ресурс] // Информационное агентство «Rambler News Service (RNS)». – 2016. – 13 октября. – Информационное агентство «Rambler News Service (RNS)», 2017. – Режим доступа: https://rns.online/internet/ICANN-vistupaet-za-zapret-kiberoruzhiya-na-natsionalnom-urovne--2016-10-13/, свободный. – Загл. с экрана.

глобальное соглашение о противодействии высокотехнологичной преступности, имеющее приоритет над национальным законодательством, может помочь предотвратить эту угрозу»[54].

По его словам, необходимо осуществлять борьбу не с конкретными технологиями, а со злоумышленниками, поэтому нет большого смысла в блокировке сайтов, в запрете криптовалюты (разновидность электронных денег с возможностью ограниченной «эмиссии» вне контроля государственных структур какой-либо страны) и в настороженном отношении к блокчейну (способ хранения данных или цифровой реестр транзакций, сделок, контрактов), а киберпреступность можно остановить только совместными действиями всех стран, иначе победить не получится. В вопросе криптовалют не решен вопрос с идентификацией на законодательном уровне – без этого не получится работать с этой разновидностью платежных средств в РФ, объясняет эксперт.

Отвечая на вопрос об обвинениях во вмешательстве в предвыборную борьбу в США хакеров из РФ со стороны ряда американских политиков, Сачков заявил, что киберпреступников в РФ интересует исключительно личная нажива, а тут нет прибыли и слишком много шумихи, поэтому на них это не похоже, либо это глупые люди, которые очень сильно верят в свою безнаказанность. Целью 99% компьютерных преступлений в настоящее время является попытка заработать денег. «На 99% компьютерные преступления связаны с попыткой заработать денег. Пока организованную компьютерную преступность не интересует критическая инфраструктура», – высказался Сачков[55].

---

[54] Шлыгин, И. Специалисты по кибербезопасности из Group-IB рассказали о новых хакерских угрозах [Электронный ресурс] / И. Шлыгин // Журнал «Financial One». – 2016. – 13 октября. – Financial One, 2017. – Режим доступа: https://fomag.ru/news/spetsialisty-po-kiberbezopasnosti-iz-group-ib-rasskazali-o-novykh-khakerskikh-ugrozakh/, свободный. – Загл. с экрана.

[55] Филипенок, А. США заподозрили Россию в передаче украденных данных WikiLeaks [Электронный ресурс] / А. Филипенок // Информационное агентство «РБК». – 2016. – 14

Тем не менее целью оставшихся 1% компьютерных преступлений является шпионаж и кибертерроризм.

Скандальный «пакет Яровой» тоже не остался без комментария со стороны специалистов по кибербезопасности на конференции Cybercrimecon-2016. «Этот нормативный акт имеет своей целью отвлечь внимание общественности от принятия других законов по борьбе с экстремизмом, так как преступники адаптируются к законодательным изменениям за несколько дней, то есть бороться с ними таким путем бессмысленно», – считает директор департамента сетевой безопасности Group-IB Никита Кислицин. В качестве примера он приводит разговоры о запрете ряда мессенджеров для служебной переписки, когда все тут же перешли на другие программы.

По оценкам Group-IB[56], годовой ущерб от кибератак в России вырос на 44% – до 5,5 млрд руб. Наибольший ущерб был нанесен в результате целевых атак на российские банки – он составил 2,5 млрд руб.

При этом сократился ущерб от хищений в интернет-банкинге у юрлиц – на 50%, до 956,2 млн руб., – а также в результате хищений у физлиц с помощью троянов для ПК (вредоносная компьютерная программа, которая используется для заражения системы целевого компьютера, и приводит к вредоносной активности на нем) – на 83%, до 6,4 млн руб. Диаграммы даны в приложении А4.

17 мая 2017 года спецпредставитель президента РФ по международному сотрудничеству в области информационной безопасности, посол по особым поручениям Андрей Крутских заявил, что Россия и США должны срочно начать

октября. – ЗАО «РОСБИЗНЕСКОНСАЛТИНГ», 2017. – Режим доступа: http://www.rbc.ru/politics/14/10/2016/580066c09a7947b21dbf5078, свободный. – Загл. с экрана.

[56] Глава Group-IB связывает 99% киберпреступлений в мире с попыткой заработка [Электронный ресурс] // Информационное агентство «Rambler News Service (RNS)». – 2016. – 13 октября. – Информационное агентство «Rambler News Service (RNS)», 2017. – Режим доступа: https://rns.online/internet/Glava-Group-IB-svyazivaet-99-kiberprestuplenii-v-mire-s-popitkoi-zarabotka-2016-10-13/, свободный. – Загл. с экрана.

диалог по противодействию киберпреступлениям[57]. Речь идет о глобальной атаке вируса WannaCry[58] 12 мая 2017 года. «В каждой стране они выбрали серию объектов критической инфраструктуры и показали всему миру, что в разных странах досягаемо все - и госпитали, и объекты энергоснабжения, и транспорт. Это была атака, показывающая возможность глобальной киберпреступности и кибертерроризма, поэтому ... представителям России и США нужно немедленно встречаться и разрабатывать ответные действия против кибер-ДАИШ (арабское название запрещенной в РФ группировки «ИГИЛ»)».

По его словам, США и РФ должны показать миру пример объединения перед лицом киберугрозы. Также Крутских подчеркнул, что ЦРУ стоило бы сосредоточиться на противодействии хакерским атакам, а не обвинять безосновательно Россию во вмешательстве в американскую президентскую кампанию 2016 года.

В этой связи необходимо создать условия для сотрудничества правоохранительных органов разных стран, обновить законодательную базу, позволяющую преследовать мошенников в киберпространстве. Пользу принесет привлечение к работе бизнеса и современных IT-компаний, специализирующихся на информационной безопасности.

[57] Волков, К. В МИД РФ призвали США начать диалог по кибербезопасности [Электронный ресурс] / К. Волков // Российская газета. – 2017. – 17 мая. – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2017/05/17/v-mid-rf-prizvali-nachat-dialog-s-ssha-po-kiberbezopasnosti.html, свободный. – Загл. с экрана.

[58] Шадрина, Т. Вымогатель атакует [Электронный ресурс] / Т. Шадрина // Российская газета. – 2017. – 14 мая. – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2017/05/14/eksperty-rossijskoe-po-luchshe-zapadnogo-protivostoit-kiberatakam.html, свободный. – Загл. с экрана.

ВЫВОДЫ ПО ГЛАВЕ 4

Цель данной главы является изучение приоритетных направлений государственной политики противодействия кибертерроризма.

Было выявлено, что в Российской Федерации термин "кибертерроризм" легально не закреплен ни в одном нормативно-правовом акте. В связи с этим российский Уголовный кодекс не предусматривает квалифицированного признака, связанного с осуществлением данного акта в киберпространстве, однако, уголовная ответственность за совершение данного террористического акта предусмотрена.

Кроме того, РФ имеет множество двусторонних договоров о правовой помощи по уголовным делам с другими странами. Данные договора являются полезным элементом сотрудничества в вопросах борьбы преступности, но для борьбы с такой угрозой как кибертерроризм, как оказалось, требуется более гибкая структура, т.к. направление и исполнение запросов о правовой помощи проходит довольно долго.

В 2006 году Президентом РФ была предложена разработка глобальной стратегии по борьбе с кибертерроризмом. Также в целях обеспечения информационной безопасности России 15 января 2013 года был выпущен Указ, исходя из которого на ФСБ РФ были возложены полномочия по созданию гос. системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В работе были рассмотрены основные задачи данной структуры.

Таким образом, было заключено, что сегодняшний день в РФ нет основополагающего и соответствующего современным реалиям и вызовам документа, который бы объяснял, как быть с кибербезопасностью на национальном уровне.

Развитие на данный момент получило сотрудничество в борьбе с криминалом на двустороннем уровне. Было выявлено, что у России свыше двух десятков

постоянно действующих рабочих групп и иных консультационных механизмов в данной сфере с другими странами.

Россией было заявлено, что «необходимо создать ответственные правила поведения стран в Интернете. Кроме того, в Интернете должны соблюдаться права граждан всех стран. Соответственно, должны быть установлены суверенитеты государств в своем сегменте сети и право всех государств участвовать в управлении Интернетом". Сейчас РФ с США возобновили контакты по информационной безопасности.

Кроме того, в рамках таких международных организаций, как БРИКС и ШОС, в которых Россия принимает активное участие, – проводятся ежегодные консультации по международной информационной безопасности. В обсуждении со многими странами ЕС данная тема также присутствует.

Более того, Россия продвигает тему борьбы с кибертерроризмом в специальной группе АТЭС по борьбе с терроризмом.

Также было выявлено, что на сегодняшний день по отдельным аспектам, в частности, по борьбе с кибертерроризмом, РФ и Япония уже близки к выходу на более тесные формы координации, в том числе рассматривается возможность подготовки соответствующих двусторонних документов.

Было предложено, бороться с кибероружием на национальном уровне, применяя при этом опыт по регулированию ядерного оружия. Было также предложено бороться не с конкретными технологиями, а со злоумышленниками.

Рассмотрению подвергся также ущерб от кибератак в России. Данные по данному вопросу были отображены в приложении А4.

В связи с последними событиями, Россия намерена с США срочно начать диалог по противодействию киберпреступлениям. Так как произошедшая кибератака показала, что досягаемо всё - и госпитали, и объекты энергоснабжения, и транспорт. Она показала возможность глобальной киберпреступности и кибертерроризма. Россия предлагает разрабатывать ответные действия против кибер-ДАИШ совместно с США.

В этой связи было выявлена необходимость создать условия для сотрудничества правоохранительных органов иностранных государств, обновить законодательную базу, которая бы позволила преследовать мошенников в киберпространстве. Также было предложено привлечение к работе бизнеса и современных IT-компаний, которые специализируются на информационной безопасности.

ЗАКЛЮЧЕНИЕ

В результате проведенной работы были изучены приоритетные направления государственной политики противодействия кибертерроризму.

Были выработаны рекомендаций по предупреждению актов кибертерроризма, совершенствованию стратегии борьбы, с этим негативным явлением с учетом российского и зарубежного опыта.

В ходе написания работы были решены такие задачи как систематизация основных научных подходов к изучению феномена кибертерроризм, выявление причин возникновения и активизации кибертерроризма на современном этапе, его особенности и тенденции функционирования. Также были выявлены противоречия, влияющие на процесс разработки и реализации политики противодействия кибертерроризму. Было определено значение международного опыта противодействия кибертерроризму для разработки и эффективной реализации данного вида политики в современной России.

Результаты данной работы могут быть учтены при разработке современной стратегии кибербезопасности Российской Федерации, дальнейшей корректировке государственной политики противодействия кибертерроризму, выявлении наиболее эффективных направлений предупреждения и нейтрализации кибератак. Материалы дипломной работы могут использоваться для подготовки учебных пособий и программ, преподавания спецкурсов в высшей школе, а также системе специальных учебных заведений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Акопов, Г.Л. Хактивизм как неотъемлемый элемент современных информационных войн / Г.Л. Акопов // Национальная безопасность. – 2014. – №3(32). – С.438-444.
2. Астахов, А. Искусство управления информационными рисками / А. Астахов. – М.: ДМК Пресс, 2010. – 312 с.
3. Бегишев, И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически-важных и потенциально-опасных объектов / И.Р. Бегишев // Информационная безопасность регионов. – 2010. – №1(6). – С.9-13.
4. Бочаров, Ю. Киберпреступность и кибертерроризм. Новая глобальная угроза государственному строю [Электронный ресурс] / Ю. Бочаров // International expert Centre for Electoral Systems. – 2011. – Режим доступа: http://www.electionsices.org/russian/publications/region:world/textid:12835/%3, свободный. – Загл. с экрана.
5. Волков, К. В МИД РФ призвали США начать диалог по кибербезопасности [Электронный ресурс] / К. Волков // Российская газета. – 2017. – 17 мая. – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2017/05/17/v-mid-rf-prizvali-nachat-dialog-s-ssha-po-kiberbezopasnosti.html, свободный. – Загл. с экрана.
6. Выступление спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в борьбе с терроризмом и транснациональной организованной преступностью А.В. Змеевского в рамках «Дипломатического клуба» на тему «Новые вызовы и угрозы - антикриминальный срез» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2012. – 19 декабря. – Министерство иностранных дел Российской Федерации, 2017. – Режим доступа:

http://www.mid.ru/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/129206, свободный. – Загл. с экрана.

7. Глава Group-IB связывает 99% киберпреступлений в мире с попыткой заработка [Электронный ресурс] // Информационное агентство «Rambler News Service (RNS)». – 2016. – 13 октября. – Информационное агентство «Rambler News Service (RNS)», 2017. – Режим доступа: https://rns.online/internet/Glava-Group-IB-svyazivaet-99-kiberprestuplenii-v-mire-s-popitkoi-zarabotka-2016-10-13/, свободный. – Загл. с экрана.
8. Григорьев, Н., Террористические действия в виртуальном пространстве опасны [Электронный ресурс] / Н. Григорьев, Э. Родюков // Независимое военное обозрение. – 2016, – Режим доступа: http://nvo.ng.ru/armament/2016-07-22/12_cyber.html, свободный. – Загл. с экрана.
9. Гринштейн, Г. Как влияют тренды кибербезопасности на рынок хищений денежных средств [Электронный ресурс] / Г. Гринштейн // Хабрахабр. – 2016. – 15 октября. – «ТМ», 2017. – Режим доступа: https://habrahabr.ru/post/312720/, свободный. – Загл. с экрана.
10. Змеевский, А.В. О международном сотрудничестве в борьбе с криминальными вызовами и угрозами [Электронный ресурс] / А.В. Змеевский // Международная жизнь. – 2013. – № 6. – МИД РФ, Редакция журнала «Международная жизнь», 2017. – Режим доступа: http://www.mid.ru/web/guest/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/103630, свободный. – Загл. с экрана.
11. Интерактивная Карта Киберугроз [Электронный ресурс]. – ЗАО «Лаборатория Касперского», 2017. – Режим доступа: https://cybermap.kaspersky.com/ru/subsystems/, свободный. – Загл. с экрана.
12. Интервью заместителя Министра иностранных дел России И.В. Моргулова японскому информагентству «Дзи-Дзи Пресс» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2017. – 17 марта. – Министерство иностранных дел Российской Федерации, 2017. – Режим

доступа: http://www.mid.ru/web/guest/maps/jp/-/asset_publisher/zMUsqsVU9NDU/content/id/2694158, свободный. – Загл. с экрана.

13. Интервью заместителя Министра иностранных дел России О.В. Сыромолотова МИА «Россия сегодня» [Электронный ресурс] // Министерство иностранных дел Российской Федерации. – 2016. – 30 сентября. – Министерство иностранных дел Российской Федерации, 2017. – Режим доступа: http://www.mid.ru/web/guest/foreign_policy/international_safety/crime/-/asset_publisher/3F5lZsLVSx4R/content/id/2480829, свободный. – Загл. с экрана.
14. Капитонова, Е.А. Особенности кибертерроризма как новой разновидности террористического акта / Е.А. Капитонова // Известия ВУЗов. Поволжский регион. Общественные науки. – 2015. – №2 (34). – С.29-41.
15. Клементьев, А.С., Ткач, Е.В. Противодействие кибертерроризму и киберэкстремизму: новая сфера правоохранительной деятельности / А.С. Клементьев, Е.В. Ткач // Противодейтсвие Терроризму Проблемы XXI века. Информационно-аналитический и научно-практический журнал. – 2013. – С.25-30.
16. Конвенция Совета Европы о компьютерных преступлениях [Электронный ресурс] // Бюро договоров. – Совет Европы, 2017. – Режим доступа: http://www.coe.int/ru/web/conventions/search-on-treaties/-/conventions/treaty/185, свободный. – Загл. с экрана.
17. Корнев, М. Суверенная кибербезопасность: как глобальные проблемы влияют на ограничения медиа в интернете? / М. Корнев // Журналист. – 2015. – №02. – ООО Медиагруппа «Журналист», 2017. – Режим доступа: http://mediatoolbox.ru/blog/suverennaya-kiber-bezopasnost-kak-globalnyie-problemyi-vliyayut-na-ogranicheniya-media-v-internete/, свободный. – Загл. с экрана.

18. Лебедева, М.М. Мировая политика: учебник / М.М. Лебедева. – 4-е изд., стер. – М.: КНОРУС, 2016. – 256 с. – С.131-138.
19. Мазуров, В.А. Кибертерроризм: понятие, проблемы противодействия [Электронный ресурс] / В.А. Мазуров // Доклады ТУСУРа. – 2010. – июнь. – № 1 (21), часть 1. – Режим доступа: http://old.tusur.ru/filearchive/reports-magazine/2010-1/41-45.pdf, свободный. – Загл. с экрана.
20. Новикова, С.А. Процесс артикуляции политической идентичности в контексте политизации интернета : дис….канд. полит. наук : 23.00.02 / С.А. Новикова ; Пермск. Гос. Нац. Исследов. ун-т. – П., 2015. – 150 с.
21. Определение кибертерроризма [Электронный ресурс] / Elcomrevue. – 21 мая 2014. – Режим доступа: http://elcomrevue.ru/opredelenie-kiberterrorizma/, свободный. – Загл. с экрана.
22. Пиджаков, А.Ю. Избранные труды / А.Ю. Пиджаков. – Изд-во «Юридический центр Пресс», 2010. – 574 с.
23. Повышев, В. Борьба с киберпреступностью и кибертерроризмом. Доклад эксперта. [Электронный ресурс] / В. Повышев // Международная Молодёжная Конференция Тюменская Модель ООН-2012. Совет по правам человека. – Томский государственный университет, 2012. – Режим доступа: http://sartraccc.ru/Pub_inter/cybercrim.pdf, свободный. – Загл. с экрана.
24. Рубанов, В.А. О согласовании процессов международного сотрудничества и национальных интересов в сфере информационной безопасности [Электронный ресурс] / В.А. Рубанов. – Agentura.ru, 2011. – Режим доступа: http://archive.is/d2tiJ, свободный. – Загл. с экрана.
25. Сошников, А. WannaCry: как работает крупнейшее компьютерное вымогательство / А. Сошников // Русская служба Би-би-си. – 2017. – 13 мая. – Би-би-си, 2017. – Режим доступа: http://www.bbc.com/russian/features-39905001, свободный. – Загл. с экрана.
26. Статья 205. Террористический акт [Электронный ресурс] // «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 17.04.2017). –

Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/43942021d9206af7a0c78b6f65ba3665db940264/. – Загл. с экрана.

27. Статья 453. Направление запроса о правовой помощи [Электронный ресурс] // «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 N 174-ФЗ (ред. от 07.06.2017). – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34481/14b49be9d968092a8e33b246ddbf5950cc6185a5/. – Загл. с экрана.
28. Талимончик, В. П. Международно-правовое регулирование отношений информационного обмена / В. П. Талимончик. – ООО «Юридический центр-Пресс», 2011. – 490 с.
29. Уварова, А. Опасность и безопасность – гонка виртуальных вооружений [Электронный ресурс] / А. Уварова // Хабрахабр. – 2016. – 26 октября. – «ТМ», 2017. – Режим доступа: https://habrahabr.ru/post/313460/, свободный. – Загл. с экрана.
30. Указ Президента Российской Федерации от 15 января 2013 г. N 31с г. Москва "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" [Электронный ресурс] // Российская газета. – 2013. – 18 января. – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2013/01/18/komp-ataki-site-dok.html. – Загл. с экрана.
31. Федеральный закон от 6 марта 2006 г. N 35-ФЗ О противодействии терроризму [Электронный ресурс] // Российская газета. – 2006. – 10 марта. – №4014(0). – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2006/03/10/borba-terrorizm.html. – Загл. с экрана.
32. Филипенок, А. США заподозрили Россию в передаче украденных данных WikiLeaks [Электронный ресурс] / А. Филипенок // Информационное агентство «РБК». – 2016. – 14 октября. – ЗАО «РОСБИЗНЕСКОНСАЛТИНГ», 2017. – Режим доступа:

http://www.rbc.ru/politics/14/10/2016/580066c09a7947b21dbf5078, свободный. – Загл. с экрана.

33. Хакеры-исламисты заявили о краже данных сотрудников Госдепа США [Электронный ресурс] // Интерфакс. – 2016. – 26 апреля. – Режим доступа: http://www.interfax.ru/world/505598, свободный. – Загл. с экрана.

34. Чернядьева, Н. А. Международный терроризм: происхождение, эволюция, актуальные вопросы правового противодействия. Монография / Н. А. Чернядьева. – «Издательство «Проспект»», 2016. – 336 с.

35. Шадрина, Т. Вымогатель атакует [Электронный ресурс] / Т. Шадрина // Российская газета. – 2017. – 14 мая. – ФГБУ «Редакция «Российской газеты», 2017. – Режим доступа: https://rg.ru/2017/05/14/eksperty-rossijskoe-po-luchshe-zapadnogo-protivostoit-kiberatakam.html, свободный. – Загл. с экрана.

36. Шерстюк, В. П. Проблемы противодействия компьютерной преступности и кибертерроризму / В. П. Шерстюк // Материалы Первой всероссийской научно-практической конференции «Формирование устойчивой антитеррористической позиции гражданского общества как основы профилактики терроризма». – М.: МЦНМО, 2009. – 512 с. – С. 43-52.

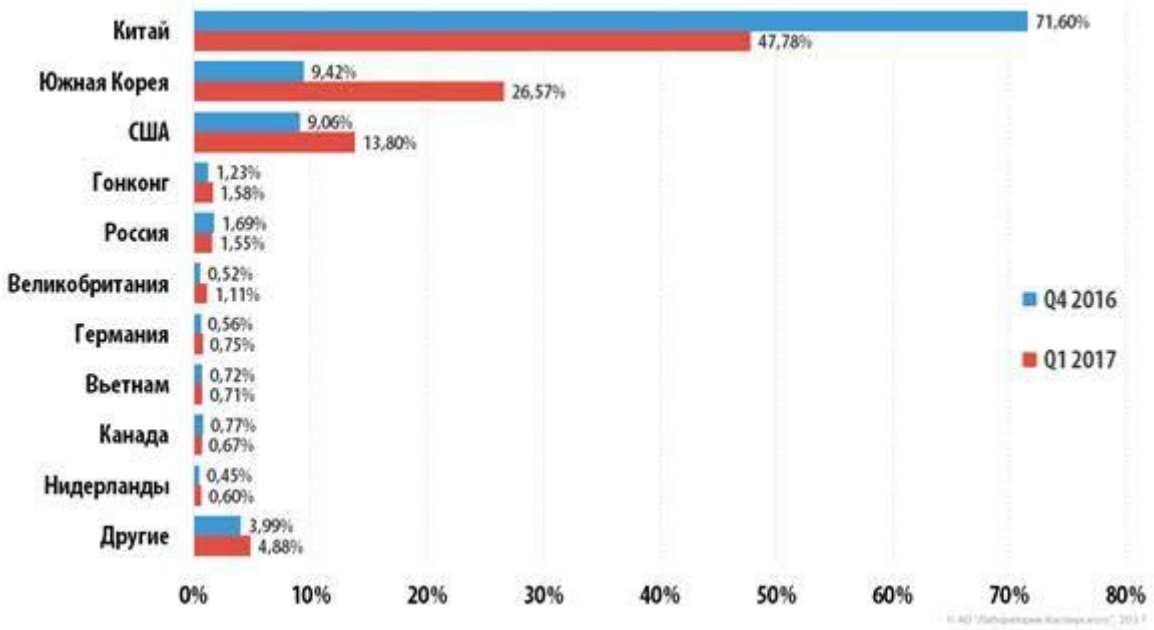
37. Шлыгин, И. Специалисты по кибербезопасности из Group-IB рассказали о новых хакерских угрозах [Электронный ресурс] / И. Шлыгин // Журнал «Financial One». – 2016. – 13 октября. – Financial One, 2017. – Режим доступа: https://fomag.ru/news/spetsialisty-po-kiberbezopasnosti-iz-group-ib-rasskazali-o-novykh-khakerskikh-ugrozakh/, свободный. – Загл. с экрана.

38. Шмидт, Э., Новый цифровой мир: как технологии меняют жизнь людей, модели бизнеса и понятие государств / Э. Шмидт, Д. Коэн. – М.: Манн, Иванов и Фербер, 2013. – 368 с.

39. Fantz, A. Who is Anonymous? Everyone and no one [Электронный ресурс] / A/ A. Fantz // CNN. – 2012. – 9 February. – Cable News Network, 2017. – Режим доступа: http://edition.cnn.com/2012/02/09/world/anonymous-explainer/index.html, свободный. – Загл. с экрана.

40. Cyber Operations and Cyber Terrorism [Электронный ресурс] // Handbook. – 2005. – 15 Aug. – No. 1.02. – Threats For Leavenworth, 2005. – Режим доступа: http://handle.dtic.mil/100.2/ADA439217, свободный. – Загл. с экрана.
41. Cybersecurity 3 апреля 2011 [Электронный ресурс] // Официальный сайт Президента США. – Режим доступа: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity, свободный. – Загл. с экрана.
42. Denning, D. E. Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy / D. E. Denning // Networks and netwars: The future of terror, crime, and militancy. – 2001. – P. 239-288.
43. Eliot Che Securing a network society cyber-terrorism, international cooperation and transnational surveillance / Eliot Che // Research paper. – 2007. – September. – No. 113. – Research institute for European and American Studies (RIEAS), 2007. – 31 p.
44. ICANN выступает за запрет кибероружия на национальном уровне [Электронный ресурс] // Информационное агентство «Rambler News Service (RNS)». – 2016. – 13 октября. – Информационное агентство «Rambler News Service (RNS)», 2017. – Режим доступа: https://rns.online/internet/ICANN-vistupaet-za-zapret-kiberoruzhiya-na-natsionalnom-urovne--2016-10-13/, свободный. – Загл. с экрана.
45. De Arimatéia da Cruz, J. Terrorism, War, and Cyber (In)Security [Электронный ресурс] / J. de Arimatéia da Cruz // Small Wars Journal. – 2013. – October 27. – Режим доступа: http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity, свободный. – Загл. с экрана.
46. Khalimonenko, A. DDOS attacks in Q1 2017 [Электронный ресурс] / A. Khalimonenko, O. Kupreev // SecureList. – AO Kaspersky Lab., 2017. – Режим доступа: https://securelist.com/ddos-attacks-in-q1-2017/78285/, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А1



Распределение DDoS-атак по странам, четвертый квартал 2016 года по сравнению с первым кварталом 2017 года

Источник: Khalimonenko, A. DDOS attacks in Q1 2017 [Электронный ресурс] / A. Khalimonenko, O. Kupreev // SecureList. – AO Kaspersky Lab., 2017. – Режим доступа: https://securelist.com/ddos-attacks-in-q1-2017/78285/, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А2

20 стран по наибольшему количеству киберугроз на 21 января 2017 года (ч. 1)

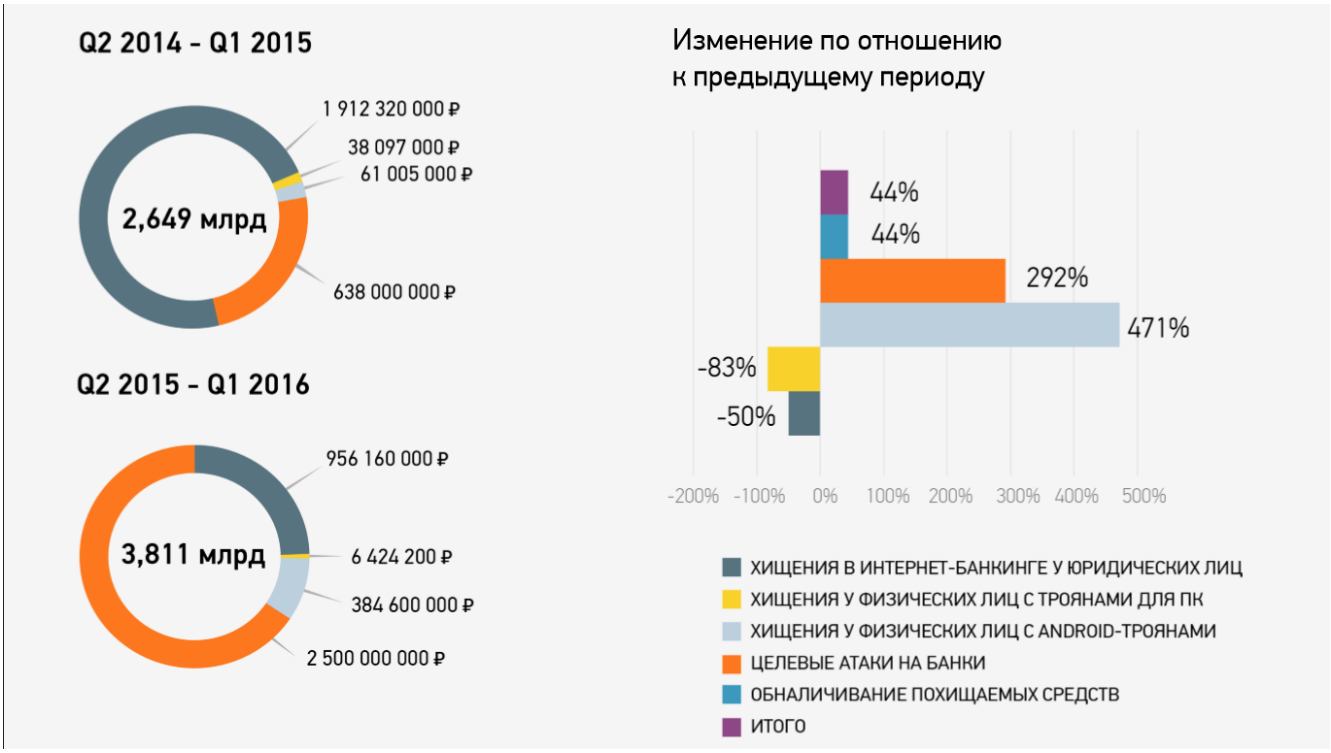
Источник: История кибертерроризма – Кибертерроризм XXI века [Электронный ресурс] // Парламентская газета. – 2017. – «Парламентская газета», 2017. – Режим доступа: https://www.pnp.ru/politics/istoriya-kiberterrorizma-kiberterrorizm-xxi-veka.html, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А3

20 стран по наибольшему количеству киберугроз на 21 января 2017 года (ч. 2)

Источник: История кибертерроризма – Кибертерроризм XXI века [Электронный ресурс] // Парламентская газета. – 2017. – «Парламентская газета», 2017. – Режим доступа: https://www.pnp.ru/politics/istoriya-kiberterrorizma-kiberterrorizm-xxi-veka.html, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А4



Общий объем хищений за 2015-2016 финансовый год в России

Источник: Гринштейн, Г. Как влияют тренды кибербезопасности на рынок хищений денежных средств [Электронный ресурс] / Г. Гринштейн // Хабрахабр. – 2016. – 15 октября. – «ТМ», 2017. – Режим доступа: https://habrahabr.ru/post/312720/, свободный. – Загл. с экрана.