Министерство образования и науки Российской Федерации
ФГБОУ ВО «Уральский государственный педагогический университет»
Институт социального образования
Факультет международных отношений и социально-гуманитарных коммуникаций
Кафедра рекламы и связей с общественностью

Политика противодействия кибертерроризму в современной России

ОП ВО «41.03.05 – Международные отношения»

Выпускная квалификационная работа

Выпускная квалификационная работа
допущена к защите
Зав. кафедрой рекламы и связей с
общественностью

_____ _____
дата А.В. Коротун,
канд. пед. наук, доцент

Исполнитель:
Прокопьева Виктория Андреевна,
студент 406 группы
очного отделения

_____ _____
дата подпись

Руководитель ОП ВО:

_____
А.В. Коротун,
канд. пед. наук, доцент

Научный руководитель:
Коротун Анна Валериановна,
кандидат педагогических, доцент
кафедры рекламы и связей с
общественностью

_____ _____
дата подпись

Екатеринбург 2017 г.

Оглавление

Введение

Сегодня интерес к проблемам информационной безопасности проявляется прежде всего в аспекте больших систем, к которым относят особо важные объекты и организации государственного уровня. Если подходить к большим системам как к информационным, в которых обработка информации и их организация в значительной мере зависят от использования ИТ, то такие угрозы информационной безопасности принято характеризовать как проявление кибертерроризма. Внимание к кибертерроризму сильно возросло во всем мире, в том числе и в России, что стимулировало исследования и обмен информацией по проблемам борьбы с ним.

Актуальность исследования политики противодействия кибертерроризму в Российской Федерации вызвано необходимостью глубокого осмысления теоретико-методологических, организационных, политических основ разработки и реализации данного вида политики.

Стоит отметить, что одним из главных факторов развития социально-политической системы является производство и использование информации. В современных условиях она играет ключевую роль в функционировании не только общественных и государственных институтов, но и жизнедеятельности каждого человека. Компьютеры и информационно-коммуникационные системы используются во всех сферах деятельности человека и государства. Это обеспечение национальной безопасности, предоставление государственных услуг в области здравоохранения, образования, ЖКХ, управления аэро- и железнодорожным транспортом, торговли, финансов, а также межличностного общения и др. Влияние глобальных сетей на социально-политическое развитие общества многогранно и противоречиво. С одной стороны, они способствуют развитию потенциала человека через компьютерные игры, обучающие и развлекательные программы, интерактивное телевидение, электронную прессу. Глобальные сети оказывают влияние на электоральное поведение

субъектов политики, процесс организации и проведения избирательных кампаний, механизмы коммуницирования власти и общества, презентацию и отстаивание политическими акторами своих интересов. С другой стороны, стремительное развитие информационно-коммуникационной сферы привело к появлению новых видов преступлений - компьютерной преступности и компьютерного терроризма. От деятельности кибертеррористов в виртуальном пространстве могут пострадать тысячи пользователей сетей, не только отдельные люди, но и целые государства. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей. Современные террористические организации активно используют информационно-коммуникационные технологии, наряду с традиционными средствами. При этом время перехода от угрозы до реального акта кибертеррористов значительно уменьшается.

Объект исследования: кибертерроризм.

Предмет исследования: политика противодействия кибертерроризму в Российской Федерации.

Цель данной работы – изучить основные направления политики противодействия кибертерроризму в РФ и определить дальнейшие уровни развития ситуации по борьбе с данным видом терроризма.

Для достижения цели были поставлены следующие **задачи:**

1. Рассмотреть понятие и причины появления кибертерроризма;
2. Раскрыть кибертерроризм как реальную угрозу национальной безопасности РФ;
3. Изучить нормативно-правовое обеспечение противодействия кибертерроризму в РФ;
4. Определить проблему противодействия кибертерроризму в РФ;
5. Проанализировать пути совершенствования мер противодействия кибертерроризму в РФ в XXI в. и разработать ситуационный анализ.

Степень изученности темы. Теоретический материал по вопросам международных отношений подробно освещен в книгах В. А. Ачкасова, В. Л. Хмылева, П. А. Цыганкова.

Те или иные аспекты данной проблематики исследованы в отечественной и зарубежной политологической, исторической, психологической, социологической, научной и публицистической литературе. Сложность и многогранность феномена кибертерроризма, комплексный характер выработки эффективных мер противодействия ему требуют междисциплинарного подхода и объясняют многообразие возможных ракурсов изучения. В научной литературе теоретическая разработка этого феномена стала активно осуществляться в конце 20 века.

В первую очередь необходимо назвать исследования, связанные с анализом информационного общества, пределов информационной свободы, правовых, социально-экономических и научно-технических аспектов обеспечения национальной безопасности и антитеррористической деятельности. Прежде всего, это работы В.Э. Багдасаряна, В.Н. Галатенко, Е.А. Ерофеева, О.А. Колобова, А.В. Крутских, В.А. Конявского, В.Н. Лопатина, С.В. Лопаткина, Б.Н. Мирошникова, И. Морозова, В. Нерсесяна, С.С. Сулакшина, Ю.С. Уфимцева, В.П. Шерстюка, В.Н. Ясенева и др.

Большой массив литературы посвящен анализу средств массовой информации в противодействии терроризму. Среди исследователей этого направления следует назвать Е.Л. Вартанову, М. Гельмана, А. Евдокимова, А.Н. Курбацкого, М.М. Назарова, И.Н. Панарина, В.Е. Бернатски, П. Вилкинсона, Л.Д. Мартина и др.

Среди российских ученых анализ интересующей нас проблемы представлен в работах Г.К. Варданянца, В.А. Голубева, В. Ибрагимова, Д.Г. Малышенко, Е.А. Роговского, Е.В. Старостиной, Т. Л. Тропиной и др. Важно, что в этих работах немало внимания уделено исследованию политики противодействия кибертерроризму как одной из приоритетных задач не

только государства, но и общества, анализу оценок угроз киберпреступности и предложениям по их нейтрализации.

Кроме того, было обращено внимание к нормативно-правовым документам, федеральным законам Российской Федерации. Среди них важное значение имеют Федеральные законы «Об информации, информатизации и защите информации», «О средствах массовой информации», «О связи», «О безопасности», «О борьбе с терроризмом». Большую помощь в анализе антитеррористической политики государства оказали Доктрина информационной безопасности Российской Федерации, Стратегия развития информационного общества в Российской Федерации и Стратегия национальной безопасности Российской Федерации до 2020 года.

Таким образом, анализ степени изученности темы позволяет сделать следующий вывод: тема противодействия кибертерроризму сегодня изучена достаточно. Однако комплексного исследования, посвященного анализу данной проблемы выявить не удалось, что обусловило новизну темы исследования. Кроме этого, исследователи нередко акцентируют внимание лишь на отдельных аспектах, проявлениях, причинах активизации кибертерроризма. Особое внимание уделено перспективам развития совершенствования мер противодействия кибертерроризму.

Хронологические рамки исследования охватывают XXI век.

Территориальные рамки исследования ограничены административными границами России.

Методологическая основа исследования. Методологической основой исследования послужил подход к определению кибертерроризма ведущих отечественных ученых-международников: Мальгина А., Торкунова А., Цыганкова П.

В работе были использованы как общенаучные, так и специальные методы исследования. Общенаучные методы: анализ, синтез, систематизация, сравнение, обобщение, дедукция и индукция, схематизация. Основные события и процессы на изложены при помощи методов описания и ивент-

анализа. Историко-сравнительный метод использовался для сравнения событий и процессов в разных странах, проблемно-хронологический метод – для изучения эволюции ключевых проблем в проблеме кибертерроризма. Метод сценарного анализа был использован в целях прогнозирования дальнейшего развития ситуации. С помощью ретроспективного метода были исследованы процессы и хронология становления и развития данной угрозы. Кроме этого, был использован метод контент-анализа.

Источниковая база. В исследовательской работе было использованы нормативно-правовые источники, регламентирующие внешнюю политику Российской Федерации. Например, концепция внешней политики Российской Федерации от 12 июля 2008 г. № ПР-1440., концепция национальной безопасности Российской Федерации от 10 января 2000 г., концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г., концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г.

Структура работы обусловлена целью и задачами исследования и состоит из введения, 2 глав, 5 параграфами, построенных по проблемно-хронологическому принципу, заключения, списка использованных источников и литературы и приложений.

Во введении представлена актуальность данной темы, предмет и объект изучения, а также цели и задачи работы.

В первой главе рассматриваются теоретические основы противодействия кибертерроризму в Российской Федерации. Рассмотрено понятие и причины, а также был изучен кибертерроризм как реальная угроза национальной безопасности.

Во второй главе были проанализированы современные проблемы противодействия кибертерроризму в РФ и предложены пути совершенствования мер противодействия кибертерроризму в РФ.

В заключение подводится итог работы, учитывая все вышесказанное.Список использованных источников и литературы.

В приложение находится контент-анализ публикаций по теме: «Кибертерроризм и противодействие ему» за период 2014-2017 гг.

Глава 1. Теоретические основы противодействия кибертерроризму в Российской Федерации

1.1. Кибертерроризм: понятие, причины

В течение последних десятилетий мировая система испытывает значительные общественно – политические и военно-стратегические катаклизмы, связанные с актами терроризма, масштабы и жестокость которых обретают огромный размах. В разных частях мира экстремисты и террористы захватывают самолеты и морские суда, взрывают здания аэропортов и железнодорожных вокзалов, приводят в действие взрывные устройства в административных и жилых зданиях, культурных центрах, автобусах и автомобилях, берут в заложники дипломатов и корреспондентов, бизнесменов и деятелей культуры. На сегодняшний день терроризм оказывает сильное влияние на международные отношения. Для того, чтобы рассмотреть кибертерроризм и его причины, сначала мы рассмотрим понятие международные отношения, а затем влияние кибертерроризма на международные отношения.

Международные отношения – это особый вид общественных отношений, выходящих за рамки внутри общественных отношений и территориальных образований [Хмылёв В.Л., 2010, с.22].

По мнению известного французского философа и социолога Р. Арона, «международные отношения – это отношения между политическими единицами» [А.В. Торкунов., 1999, с. 584].

По мнению французского исследователя М. Мерля, международные отношения – это «совокупность соглашений и потоков, которые пересекают границы, или же имеют тенденцию к пересечению границ» [Цыганков П.А., 1994, с. 56].

Основываясь на определения вышеупомянутых авторов, можно сделать вывод о том, что международные отношения – это система, которая охватывает все международные события. Это механизм, который корректирует государственные и надгосударственные интересы.

Целью международных отношений является создание благоприятных условий для функционирования и развития субъектов взаимодействия (субъектов международных отношений) [Поздняков Э.А., 1976, с. 152].

Причинами развития международных отношений являются:

1. Неравномерность экономического развития различных стран мира
2. Различие в людских, сырьевых, финансовых ресурсах
3. Характер политических отношений
4. Различный уровень научно-технического развития
5. Особенности географического положения, природных и климатических условий [Поздняков Э.А., 1976, с. 152].

Из всего сказанного можно сделать вывод, что международные отношения являются особым видом социальных отношений и на сегодняшний день рассматриваются как система межгосударственных и негосударственных взаимодействий в глобальном, региональном масштабе или на уровне двухсторонних взаимоотношений. Сущность системы международных отношений состоит в том, чтобы найти пути и способы разрешения конфликтов между государствами и странами, возникающих, прежде всего в результате столкновения их реальных и нередко недопонятых национальных интересов. Сегодня в современных международных отношениях наиболее важной и глобальной проблемой является терроризм, и частности, актуальной и наиболее острой проблемой является кибертерроризм. Необходимо подробнее рассмотреть эту проблему и рассказать о том, что такое кибертерроризм, о его виды и опасности.

На сегодняшний день кибертерроризм – это угроза развитию современного глобального информационного общества. Но для того, чтобы

определить понятие «кибертерроризм» – нужно решить довольно трудную задачу, поскольку нелегко установить четкую границу для отличия его от информационной войны и информационного криминала. Еще одна трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма.

Само понятие «кибертерроризм» образовано слиянием двух слов: «кибер» («киберпространство») и «терроризм». В русскоязычной литературе все чаще встречаются термины «виртуальное пространство», «виртуальная реальность», что обозначает моделируемое с помощью компьютера информационное пространство, в котором существуют определенного рода объекты или символьное представление информации – место, в котором действуют компьютерные программы и перемещаются данные [Юркин И. 3., 2007,с. 11-12].

Остановимся на каждом подробнее.

Отметим, что с научной точки зрения терроризм это общественный феномен, заключающийся в противоправном использовании крайних форм насилия или угрозы насилием для устрашения противников с целью достижения конкретных политических целей. Понятием «терроризм» в научной литературе в настоящее время стали обозначать действия оппозиционных организаций, практикующих политические убийства, а понятие «террор» закрепилось за репрессивными действиями государства по отношению к своим гражданам. В этом контексте подразумевается, что терроризм есть осуществление террора [Залиханов М.Ч., Лосев К.С., Шелехов А. М., 2005, с. 216].

Террор – устрашение своих политических противников, выражающееся в физическом насилии, вплоть до уничтожения. Что касается терроризма, то это – деятельность, выражающаяся в устрашении населения и органов власти с целью достижения преступных намерений. Устрашение политических противников характерно для любой формы терроризма, в том числе кибертерроризма [Паненков А. А.,2014,с. 12-19].

Кроме того, *терроризм* – совокупность противоправных действий, связанных с покушениями на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или другими действиями, способствующими нагнетанию страха и напряженности в обществе с целью получения преимуществ при разрешении политических, экономических или социальных проблем. В данном контексте для нас важно «искажение объективной информации», последствия которой могут быть непредсказуемы, в том числе для политического, экономического и социального строя страны.

Террористический акт – это совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека [Юркин И. 3., 2007,с. 11-12].

Теперь перейдем к *виртуальной реальности*. Данный термин обозначает созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие.

Кибернетика – это наука об управлении, связи и переработке информации. Основным объектом исследования кибернетики являются абстрактные кибернетические системы, от компьютеров до человеческого мозга и человеческого общества [Тропина Т. Л., 2003, с.173-181].

Говоря о кибертерроризме, нельзя не отметить и киберпреступность.

Киберпреступность – это незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации через Интернет [Паненков А. А.,2014,с. 12-19].

Попытки же выработки термина «кибертерроризм» были предприняты относительно недавно, в 1997 г., сотрудником ФБР Т. Поллиттом. Кибертерроризм – преднамеренные, политически мотивированные атаки на

информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов. Т. Поллитт задал верный вектор, приняв во внимание политические мотивы, свойственные меры, на которые нацелены атаки, и субъекты этих атак, хотя недостаточно полно. Однако он не описал последствия и не сделал выводов.

Под кибертерроризмом известный исследователь Д. Деннинг понимал, что это противоправная атака или угроза атаки на компьютеры, сети или информацию, находящуюся в них, совершенная с целью принудить органы власти к содействию в достижении политических или социальных целей.

Также данное понятие попытался объяснить украинский ученый Голубев В. По его мнению, кибертерроризм – это преднамеренная атака на информацию, обрабатываемую компьютером, компьютерную систему или сети, которая создает опасность для жизни и здоровья людей или предполагает наступление других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [Голубев А.В. Режим доступа: http://w\v\v.crimc-research.ni/articles/Golubev0804/ (дата обращения: 02.12.2016)].

Еще одно необходимое обозначение данного понятия вывел Кл. Вилскон. Кибертерроризм – использование компьютеров как оружия или объекта атаки политически мотивированными международными или межнациональными группами, или тайными агентами, которые угрожают насилием либо причиняют его, насаждают страх для того, чтобы воздействовать или принудить правительство изменить политику [Тропина Т. Л., 2003.,с.173-181].

Исследователи М. Дж. Девост, Б. Х. Хьютон, Н. А. Поллард определяют кибертерроризм как:

1. Соединение преступного использования информационных систем с помощью мошенничества или злоупотреблений с физическим насилием, свойственным терроризму;

2. Сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов [Тропина Т. Л., 2003,с.173-181].

Таким образом, исходя из основных понятий кибертерроризма, можно вывести следующее определение, который будет считаться основным, главным термином в данной работе.

Кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта [Юркин И. 3., 2007,с. 11-12].

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

Цель кибертерроризма – это нарушение общественной безопасности, запугивание людей, а также провоцирование военного конфликта.

Для достижения своих целей кибертерроризм использует электронные сети, современные информационно-коммуникационные технологии, радиоэлектронику. Особую опасность представляют посягательства на информационную безопасность критически важных инфраструктур: компьютерных систем управления банковской сферы, обороны, промышленности и др. Реализация таких угроз может привести к чрезвычайным последствиям для общества и государства [Тропина Т. Л., 2003,с.173-181].

Также необходимо отметить объекты кибертерроризма. Объектом кибертерроризма является безопасность людей и различных материальных объектов; жизнь, здоровье, свобода конкретных лиц или их персонально неопределенных групп; нормальное функционирование и физическая целостность тех или иных предметов и сооружений (например, имущества, принадлежащего терроризируемым лицам, учреждениям и т. п.). Это объекты непосредственного насильственного воздействия. Применяя различным образом, насилие или угрожая применить его по отношению к лицам или конкретным материальным объектам, террористические организации, в конечном счете, рассчитывают на достижение выдвинутых ими целей и задач ослабления и подрыва общих объектов терроризма [Возженников А.В., 2007, с.,90 -95].

Согласно версии «Monterey» можно выделить три уровня кибертерроризма [Цыгичко В.Н., 2000]:

1. *Простой – Неструктурированный*

Использование хаков против информационных систем, обычно используются программы созданные кем-то другим (не самими кибертеррористами) Как правило – это самый простой вид атак, потери от него либо минимальны, либо незначительны.

2. *Расширенный – Структурированный*

Возможность вести более сложные атаки против нескольких систем или сетей и, возможно, изменение или создание базовых инструментов взлома. Организация обладает определённой структурой, управлением и прочими функциями полноценных организаций. Также участники таких группировок проводят обучение новоприбывших хакеров.

3. *Комплексный – координированный*

Способность к скоординированной атаке, способны вызвать массовое нарушение систем безопасности страны. Возможность создания сложных инструментов взлома. Имеют строгую структуру, зачастую представляют

собой организации, способные здраво анализировать свои действия, вырабатывать какие-то планы атак и прочее.

Исследователями выделяется следующие причины возникновения кибертерроризма: 1) политические, 2) социальные и 3) экономические.

1. **Политические причины.**

Данные причины подразделяются на внешние и внутренние. К внешним причинам относятся глобализация, углубление разрыва между уровнями благосостояния различных стран, агрессивная политика в отношении другого государства и его оккупация, усиление глобального цифрового противоборства и разрыв в уровне информационного развития стран, столкновение политических интересов различных государств. Внутренними причинами являются политическая нестабильность и обострение политических конфликтов внутри государства, отсутствие механизмов взаимодействия государственной власти и гражданского общества, навязывание правящей элитой несвойственных для данного общества социально-политических реформ и иных нововведений, недовольство граждан страны деятельностью правительств иностранных государств; поощрение кибертерроризма руководством сраны, общественными организациями и в средствах массовой информации [Голубев А.В.Режим доступа: http://w\v\v.crimc-research.ni/articles/Golubev0804/ (дата обращения: 02.12.2016)].

2. Социальные причины.

Исследователи здесь выделяют следующие причины: возросшая социальная дифференциация в обществе, раскол его на группы с различным экономическим положением, заметное снижение качества жизненного уровня людей, слишком медленный процесс формирования среднего слоя общества.

3. **Экономические причины**

Исследователи в возникновение кибертерроризма включают в себя продолжающийся экономический и энергетический кризис, рост цен, инфляции и безработицы [Юркин И. 3., 2007,с. 11-12].

Теперь перейдем к методам и способам кибертерроризма. Одним из главных способов кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Это проявляется в угрозе насилия, поддержании состояния постоянного страха с целью достижения определенных политических или иных целей, принуждении к определенным действиям, привлечении внимания к личности кибертеррориста или террористической организации, которую он представляет [Паненков А. А., 2014,с. 12-19].

При совершении кибератак в информационном пространстве чаще всего используются следующие приемы:

- получение незаконного доступа к личной, коммерческой, банковской информации, к государственным и военным секретам;
- нанесение ущерба физическим элементам информационного пространства (например, создание помех, нарушение работы сетей электропитания, использование специальных программ, которые разрушают аппаратные средства);
- уничтожение информации, программного обеспечения, технических ресурсов путем внедрения вирусов, программных закладок, преодоления систем защиты;
- техническое внедрение в каналы трансляции средств массовой информации с целью распространения слухов, дезинформации, объявления требований террористической организации;
- уничтожение или подавление работы линий связи, перегрузка узлов коммуникации, изменение адресации запросов в сети Интернет;
- проведение информационно-психологических операций, воздействующих на сознание населения и др.

Эти приемы постоянно совершенствуются в зависимости от средств защиты, которые применяют разработчики компьютерных сетей.

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма [Тропина Т. Л., 2003,с.173-181].

На основе анализа научной литературы, международных документов и законодательства ряда стран представляется возможным выделение некоторых отличительных признаков кибертерроризма как социально-политического явления [Паненков А. А.,2014,с. 12-19].

Первым отличительным признаком кибертерроризма является то, что он порождает общую опасность, которая возникает в результате угрозы или совершения общественно опасных действий. Опасность при этом должна быть реальной и угрожать неопределенному кругу лиц.

Вторым отличительным признаком кибертерроризма является то, что акты кибертерроризма должны иметь публичный характер и получать общественную огласку. На сегодняшний день кибертерроризм — это, бесспорно, форма насилия, рассчитанная на массовое восприятие.

Третьим отличительным признаком исследователи кибертерроризма отмечают умышленное создание обстановки напряженности, подавленности, страха на социальном уровне, которая представляет собой объективно сложившийся социально-психологический фактор, воздействующий на других лиц и вынуждающий их к каким-либо действиям в интересах кибертеррористов или принятию их условий.

Четвертым отличительным признаком кибертерроризма является то, что при совершении кибертеррористического акта общеопасное насилие применяется в отношении одних лиц или организаций в целях психологического воздействия и склонения к определенному поведению других лиц.

Пятым признаком кибертерроризма является удаленность от места непосредственного террористического акта, анонимность преступников, небольшие материальные затраты (т. к. не требует оружия, взрывчатых веществ), а также то, что их практически невозможно спрогнозировать и проследить кибертеррористические атаки в реальном времени [Тропина Т. Л., 2003,с.173-181].

Проведенный анализ явления кибертерроризма показывает, что к его особенностям относятся: 1. Является информационным оружием, так как использует компьютерные системы и сети, специальное программное обеспечение и информационные технологии. 2. Носит международный характер, поскольку преступники находятся в одном государстве, а их жертвы за рубежом. 3. Многообразие целей. 4. Характеризуется высоким уровнем латентности и низким уровнем раскрываемости. 5. Требует сравнительно небольших финансовых затрат и наносит огромный материальный ущерб.

Подводя итог, необходимо отметить, что на сегодняшний день существует прямая зависимость между степенью развития информационной инфраструктуры, компьютеризации страны и количеством подобных терактов. В настоящее время проблема кибертерроризма особенно актуальна для стран, лидирующих в использовании систем спутниковой связи и глобальных сетей. По мнению экспертов, кибертерроризм – это серьезная угроза Человечеству, сравнимая по эффективности с оружием массового уничтожения. Действительно, в мире не существует государства, которое полностью было бы защищено от атак кибертеррористов.

1.2. Кибертерроризм как реальная угроза национальной безопасности РФ

Обеспечение внутреннего контура национальной безопасности России невозможно без активизации противодействия терроризму, его финансированию и кибертерроризму. В этой связи важно укрепление международного сотрудничества в борьбе с кибертерроризмом и совершенствование национальных законодательств в этой сфере, что является одним из важнейших направлений деятельности всех государств, их правоохранительных органов и спецслужб, включая Россию.

Кибертерроризм – это реальная угроза, причем существующая, по крайней мере, уже пару десятилетий. Вопрос только в масштабах явления. Конечно, говорить сейчас о глобальной угрозе пока еще, вероятно, рано, хотя, учитывая тот факт, что вычислительная техника (например, компьютеры) постоянно дешевеет (в отличие от военной техники, оружия или взрывчатки), кибератаки становятся все привлекательнее, тем более что очень часто могут иметь большую разрушительную силу. Причем, мишенями могут стать как гражданские, так и военные объекты [Сулакшин С.С., 2010, с. 41].

Сегодня кибербезопасность для России – это стратегическая проблема государственной важности, затрагивающая все слои общества. Государственная политика кибербезопасности служит средством усиления безопасности и надежности информационных систем государства.

Профессиональный компьютерный терроризм представляет собой умышленные преступления, посягающие как на охраняемую законом компьютерную информацию, так и на другие объекты уголовно-правовой охраны, где компьютерные технологии могут выступать орудием преступления. Он характеризуется устойчивой формой своей деятельности, а также высоким уровнем знаний и навыков используемых для достижения преступной цели [Юркин И. 3., 2007,с. 11-12].

Стоит отметить, что общество и государство к нарастающей угрозе кибертерроризма и киберпреступности сегодня относятся без должного внимания.

Что касается киберпреступности, то преступность в сфере высоких технологий не только растет, но и меняет свою форму, она становится все более изощренной и опасной по своим последствиям. Усложняются и вредоносные программы. В будущем следует ожидать создания вирусных программ нового поколения, которые полностью и безвозвратно смогут уничтожать информацию на зараженном компьютере. Появятся также и новые формы кибермошенничества, а благодаря продолжающемуся процессу компьютерной глобализации мошенники не будут испытывать дефицита жертв [Паненков А. А.,2014,с. 12-19].

Для России характерно, что жертвами компьютерного мошенничества все чаще становятся лица, занимающиеся предпринимательской деятельностью. Особая общественная опасность преступлений в данной сфере состоит в том, что помимо причиненного материального ущерба такие действия вносят дисбаланс в денежное обращение. Такое компьютерное мошенничество при определенных условиях может даже стать причиной банкротства.

Уже сейчас стала явной недостаточность законодательного регулирования сети Интернет не только в России, но на международном уровне, так как, ни в одной из стран мира нет кодифицированного законодательства по Интернету. Существующие нормативные акты регулируют частные аспекты функционирования сети, прежде всего вопросы подключения к ней через поставщиков, предоставления соответствующих линий связи и т.д.

Терроризм в сети Интернет представляет собой сложный социальный феномен, обладающий высокой общественной опасностью, и его необходимо изучать как специфический вид преступности, имеющий качественные отличия от иных ее видов, детерминированные особенностями сетевой социальной среды. К таким отличиям можно отнести высокую латентность, транснциональный организованный характер, особые структурные характеристики преступных формирований, дистанционный способ

совершения сетевых преступлений и др. Сетевая преступность имеет тесные связи не только с иными видами преступности, но и с целым рядом негативных социальных отклонений (наркоманией, «теневой» экономикой, и т.п.).

По справедливому утверждению Паненкова А.А,, глобальная информатизация в настоящее время активно управляет существованием и жизнедеятельностью государств мирового сообщества, информационные технологии применяются при решении задач обеспечения национальной, военной, экономической безопасности и др. Вместе с тем, одним из фундаментальных последствий глобальной информатизации государственных и военных структур стало возникновение принципиально новой среды противоборства конкурирующих государств – киберпространства, которое не является географическим в общепринятом смысле этого слова, но, тем не менее, в полной мере является международным [Паненков А. А.,2014,с. 12-19].

Говоря о кибертерроризме, стоит отметить и явление экстремизма.

Экстремизм – приверженность крайним взглядам и, в особенности, мерам (обычно в политике). Среди таких мер можно отметить провокацию беспорядков, гражданское неповиновение, террористические акции, методы партизанской войны. Наиболее радикально настроенные экстремисты никогда не признают какие-либо компромиссы, переговоры, соглашения. Росту экстремизма обычно способствуют: социально-экономические кризисы, резкое падение жизненного уровня основной массы населения, тоталитарный политический режим с подавлением властями оппозиции, преследованием инакомыслия. В таких ситуациях крайние меры могут стать для некоторых лиц и организаций единственной возможностью реально повлиять на ситуацию, особенно если складывается революционная ситуация или государство охвачено длительной гражданской войной — можно говорить о «вынужденном экстремизме» [Башкатов И.П., 2000, с. 25].

Экстремизм весьма динамично развивается и с каждым днем приобретает все новые черты и характеристики. Экстремистские организации все активнее используют достижения компьютерных технологий, внедряя в свою деятельность, прежде всего, те из них, которые достаточно эффективно воздействуют на массовое общественное сознание [Сулакшин С.С., 2010, с. 46].

Статистические данные свидетельствуют о неуклонном росте преступных деяний данной категории в Российской Федерации. За последние 10 лет количество только официально зарегистрированных преступлений экстремистской направленности увеличилось более чем в 5 раз (со 157 фактов в 2005 г. до 896 в 2015 г.). При этом в силу ряда как объективных, так и субъективных причин факты экстремизма зачастую входят в латентную группу преступлений или регистрируются как преступные деяния, совершенные по другим основаниям.

Но стоит учесть, что именно повсеместное распространение web-технологий создает предпосылки для существенного изменения способов совершения преступлений экстремистской направленности. Потенциал и коммуникативные возможности глобальной сети Интернет, социальных, локальных и файлообменных компьютерных сетей используются идеологами экстремизма в качестве своеобразной информационной площадки для популяризации своих идей, вербовки новых сторонников, их интерактивного обучения вопросам идеологии и тактики действий, организации финансовой поддержки деструктивных сил, тем самым «взращивая» кибертерроризм.

На сегодняшний день, по убеждению Колобова О.А., ядром «проблемного поля» информационной безопасности является определение того, каковы природа и деструктивный потенциал информационных угроз [Колобов О.А., 2001, с.176].

Корниш П. из лондонского Королевского института иностранных дел приводит следующую классификацию информационных угроз:

1) деятельность хакеров-одиночек;

2) организованная преступность, действующая в глобальных интернет-сетях;

3) идеологический и политический экстремизм;

4) проводимая государством информационная агрессия [Голубев А.В. Режим доступа: http://w\v\v.crimc-research.ni/articles/Golubev0804/ (дата обращения: 02.12.2016)].

Таким образом, стоит отметить, что связанные с развитием сети Интернет трансформации организованной преступности не только порождают необходимость совершенствования законодательства, изменения организации и тактики борьбы с преступностью, но и требуют новых подходов к комплексному теоретическому осмыслению соответствующих криминологических проблем, уточнения некоторых из сложившихся криминологических представлений о содержании правоохранительной деятельности. На фоне происходящих социальных преобразований и изменения форм деятельности правоохранительных органов особая роль должна отводиться криминологическим исследованиям, которые в итоге должны привести к формированию новой концепции борьбы с преступностью в киберпространстве, обеспечить правоприменительную практику научно обоснованными рекомендациями.

Говоря о кибертерроризме, стоит уделить внимание его влиянию на молодежь. Наиболее массовое и системное воздействие на молодежь преступность в информационной сфере оказывает через Интернет, где молодежь является основным потребителем информации и услуг. Этому способствует тот факт, что жизнь молодых людей, их контакты и действия в виртуальном мире практически неподвластны контролю со стороны семьи, учителей, общественных организаций и государства. При этом преступность рассматривает молодежь, с одной стороны, как потенциальную жертву, учитывая ее высокий уровень виктимности. С другой стороны, преступники смотрят на молодежь, пользующуюся интернетом, как на свой мобилизационный ресурс, негативно воздействуя и понижая уровень ее

правосознания и моральных качеств. Нередко преступники совмещают одно с другим. При этом в любом из этих случаев весьма грамотно используются возможности инфотелекоммуникационной среды, которая предоставляет преступникам свои важнейшие свойства – быстродействие, трансграничность, многообъектность одновременного воздействия, а также анонимность.

Одним из негативных факторов, отрицательно воздействующим через сеть интернет на молодежь, является противоправный контент, начиная со спама и контрафакта и заканчивая пропагандой экстремизма, в т. ч. крайних его форм. Данный контент направлен не столько на получение прибыли, сколько на разрушение правосознания молодежи и ее психического здоровья. Причем структура контента устроена таким образом, чтобы в полной мере воспользоваться их повышенной внушаемостью и отсутствием житейского опыта [Панарин И.Н., Режим доступа: http://www.panarin.com (дата обращения: 18.04.2017)].

Наиболее опасны с этой точки зрения информационные ресурсы, проповедующие нетерпимость и жестокость, независимо от формы их популяризации: при свободном обмене мнениями на «независимом» блоге или в форме игры. При этом не редко идеологически ориентированные сайты экстремистского толка, контролируемые террористическими организациями, рассматриваются организаторами как площадки для психологической обработки и рекрутирования новых членов боевых групп.

Таким образом, можно констатировать, что современный подход к организации компьютерного обучения и воспитания подрастающего поколения имеет существенные недостатки. Необходим жесткий государственный контроль и цензура. С такой позицией солидарны не только исследователи, но и представители широкой общественности.

Опираясь на труды исследователей кибертерроризма, на современном этапе функционирования кибертерроризма в России как явления, угрожающего национальной безопасности государства, можно выявить

следующие тенденции его развития [Панарин И.Н., Режим доступа: http://www.panarin.com (дата обращения: 18.04.2017)].:

1. Неуклонный рост создаваемой им общественной опасности, который выражается в том, что общий уровень проявления экстремизма и терроризма, как в нашей стране, так и во всем мире, постоянно возрастает.

2. Расширение масштабов воздействия на различные социальные слои. Эта тенденция проявляется в использовании кибертеррористами информационно-коммуникационных сетей и систем, посредством которых происходит воздействие на большие массы людей (например, социальные сети), при слабой цензуре или полном отсутствии какого-либо контроля со стороны государства, а также в быстром и относительно дешёвом распространении информации.

3. Превращение кибертерроризма в долговременный фактор политического процесса. Это обусловлено отсутствием крупных успехов в противодействии ему за последнее десятилетие, формированием новых предпосылок к его дальнейшему распространению (глобализация, научно-технический прогресс), обострением в целом ряде стран многочисленных очагов борьбы за пересмотр государственных границ, межконфессиональных, идеологических и политических противоречий.

4. Повышение уровня его организации, которое включает в себя создание развёрнутой инфраструктуры террористической деятельности в Интернете, координацию идейно-политической позиции, обмен информацией, согласование проводимых акций и атак без внешнего вмешательства со стороны спецслужб и правоохранительных органов.

5. Возрастание изощрённости и антигуманности кибертеррористических актов обусловлено тем, что на сегодняшний день у кибертеррористов есть реальная возможность нарушить нормальное функционирование критически важных объектов государства (ядерные реакторы, биологические и химические лаборатории и т. д.), что повлечёт за собой неисчислимое количество жертв.

6. Улучшение технической оснащённости кибертеррористов. Кибертерроризм относится к технологическим видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компьютерных и информационных технологий, радиоэлектроники.

7. Политизация кибертерроризма, проявляющаяся в стремлении кибертеррористов влиять на принятие государственных решений в целях ослабления деятельности правоохранительных органов, торможения законодательных инициатив посредством насильственных методов (кражи или уничтожения информации, шантажа, угроз, порчи компьютеров).

Выявленные тенденции обусловливают увеличение значимости противодействия угрозам данного типа для государственной системы национальной безопасности.

Суммируя вышесказанное, до недавнего времени информационная инфраструктура России не представлялась сколько-нибудь уязвимой в отношении рассматриваемых террористических актов. Причиной этого, в первую очередь, можно считать низкий уровень её развития, а также наличие значительной доли неавтоматизированных операций при осуществлении процесса управления.

Вместе с тем в последние годы многие государственные и коммерческие структуры приступили к активному техническому переоснащению своих предприятий, организаций.

Информационная составляющая таких организаций реализуется практически исключительно на технических и программных средствах иностранного производства, что в определенной степени повышает угрозу успешных атак со стороны кибертеррористов. Научно-технические достижения и инновации, ускорившие глобализацию, а также рост производительности и благосостояния в мире, могут быть использованы отдельными лицами или группировками как средство террора. Компьютерный террористический акт способен стать действенным орудием

массовой дезорганизации. Уже сегодня кибертеррорист может нанести больший вред, используя в преступном арсенале вычислительную машину, нежели взрывное устройство. Информационные технологии рассматриваются как средство, помогающее террористам объединяться в группировки, действовать скрытно и совершать нападения на элементы национальных инфраструктур. Все более доступными для террористов становятся средства, позволяющие разрушить компьютерные системы и другие электронные устройства.

Особую угрозу мировым информационным системам представляет соединение технологического и научного потенциала развитых стран и особенно России. Ситуация осложнена тем, что нормативная база, на основе которой ведется контроль за экспортом высоких технологий из развитых стран, не в должной мере отвечает серьезности угрозы. Совершать кибертеракты сегодня способна любая из существующих в настоящее время террористических организаций: Ирландская организация «ИРА», «Аль-Кайда», баскская организация «ЭТА», религиозные движения типа алжирских или египетских фундаменталистов, чеченские незаконные вооруженные формирования и т.п. [Роговский Е.А. 2003, с.65]

Таким образом, высокотехнологичные террористические акции новой эпохи способны сегодня продуцировать системный кризис всего мирового сообщества и поставить под угрозу существование отдельных регионов мира, что не было характерно для традиционных террористических актов. В условиях наращивания в мире процессов глобализации и формирования «информационного общества», кибертерроризм может выступать в качестве самостоятельного фактора, способного угрожать отдельным государствам и международному сообществу в целом.

1.3. Нормативно-правовое обеспечение противодействия кибертерроризму в РФ

Модернизация общества и развитие информационных технологий привели к массовому использованию во всем мире Интернета. С появлением глобальной сети возникла одна из наиболее опасных разновидностей киберпреступности – кибертерроризм, который, по сравнению с традиционным терроризмом, при совершении террористических акций прибегает к новейшим достижениям науки и техники.

В последнее время в СМИ все чаще и чаще говорят о проблеме кибертерроризма. Данная проблема была также отмечена на проходившей в конце мая 2016 в городе Грозном VII международной встрече высоких представителей, курирующих вопросы безопасности. Так, участник указанного форума, спецпредставитель президента РФ по вопросам международного сотрудничества в области информационной безопасности, посол МИД РФ по особым поручениям А. Крутских отметил, что кибертерроризм – одно из наиболее страшных явлений, при этом оно совсем новое. Например, «Исламское государство» (запрещенное в России) уже влезло в информационное пространство и занимается кибертерроризмом [Речь А. Крутских от 27.05.2016. Режим доступа: http://www.interfax.ru/russia/520709/ (дата обращения 01.12. 2016)].

Для начала отметим, что за последнее десятилетие во многих государствах мира были приняты меры по защите национального сегмента киберпространства, на государственном уровне разработаны и опубликованы стратегии киберпространства. Основной акцент в этих нормативно-правовых документах делается на то, что «…обеспечение доступности киберпространства, а также целостности, достоверности и конфиденциальности информации в киберпространстве стало одной из важнейших проблем XXI века. Именно поэтому защита киберпространства

становится главной задачей государства, экономики и общества, как на государственном, так и на международном уровне» [Пахарева Е.Н. 2010, с. 78].

Хронологию принятия данных стратегий в европейских государствах можно расположить в следующем порядке.

2008 год – стратегии разработаны, приняты и опубликованы в Словакии, Финляндии и Эстонии.

2011 год – к странам, имеющим стратегии по кибербезопасности присоединились: Германия, Голландия, Литва, Люксембург, Соединѐнное Королевство, Чешская республика, Франция [Усилинский Ф.А., 2014, с.7].

В стратегиях отражено:

- цели и мероприятия, направленные на развитие оборота электронной информации, а также обеспечения ее конфиденциальности, доступности и целостности в киберпространстве;
- обеспечение информационной безопасности рассматривается в качестве необходимого условия нормального функционирования и развития общества;
- информационные системы должны быть способны противостоять событиям в киберпространстве, которые могут отрицательно повлиять на доступность, целостность и конфиденциальность информации.
- определение целей и способов развития государственных возможностей и необходимой законодательной базы для вступления в международную борьбу с киберпреступностью.

Что касается Российской Федерации, то задача нормативно-правового регулирования обеспечения кибербезопасности сегодня является органичным компонентом государственной политики развития национального сектора применения информационных технологий.

Необходимо отметить систему противодействия не только кибертерроризма, но и терроризма в целом.

Система противодействия терроризму – совокупность субъектов, осуществляющих комплексную деятельность по выявлению, предупреждению и устранению причин и условий, порождающих и способствующих терроризму, борьбу с терроризмом, минимизацию последствий террористической активности (рис.1.) [Усилинский Ф.А., 2014, с.7].

Рис.1. Схема координации противодействия терроризму в Российской Федерации

Среди основных документов, определяющих на сегодняшний день фундаментальные подходы к обеспечению информационной безопасности в Российской Федерации, можно выделить, в первую очередь, следующие:

- Закон Российской Федерации 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.
- Доктрина информационной безопасности Российской Федерации.

- Стратегия развития информационного общества в Российской Федерации.

Указанные, а также сопутствующие им ведомственные нормативные документы (в первую очередь это документы ФСТЭК России) на сегодняшний день формируют комплексную систему требований по обеспечению информационной безопасности для информационных систем различного уровня. В то же время вопрос уточнения специфики киберпространства, а также соответствующих угроз и механизмов защиты, безусловно, заслуживает отдельного рассмотрения.

Из современных правовых документов в области безопасности киберпространства следует особо отметить следующие:

- Концептуальные взгляды на деятельность Вооруженных сил РФ в информационном пространстве.
- Проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Указ Президента России 2013г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

Стоит также отметить, что позиция Европы США в отличии от российской, основана на том, что наиболее важной является разработка мер информационной безопасности применительно к угрозам террористического и криминального характера. Перспективу создания информационного оружия, ведения информационной войны американские специалисты считали скорее теоретической. Европа сконцентрировалась на разработке конвенции по борьбе с киберпреступностью, а Соединѐнные Штаты, хотя и уделяют внимание всем аспектам информационного противоборства и в том числе кибернетического, практически не стремились и не стремятся к достижению международных договорѐнностей по их урегулированию [Усилинский Ф.А., 2014, с.7].

Вследствие этого Российская Федерация, не находя поддержки своей позиции на мировом политическом пространстве, перенесла центр своей активности на региональный уровень. Примером тому служит совместная договорѐнность стран ШОС о возможных совместных мерах по устранению информационных угроз, основанная на подписанном 16 июня 2009 г. в Екатеринбурге межправительственном Соглашении государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. В документе впервые на международно-правовом уровне было зафиксировано наличие конкретных угроз в области информационной безопасности, а также определены основные направления, принципы, формы и механизмы сотрудничества в этой сфере. Соглашение стало первым международным нормативно-правовым актом, охватывающим весь спектр проблем международной информационной безопасности – от противодействия кибирпреступности и кибертерроризму до вопросов разоружения. Его ратифицировали: Российская Федерация, КНР, Казахстан, Таджикистан, 2 июня 2011 г. оно вступило в силу [Россия в глобальной политике. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

Кроме этого, на сегодняшний день в Российской Федерации документом, определяющим наиболее фундаментальные подходы к обеспечению кибербезопасности, является Концепция стратегии кибербезопасности Российской Федерации. Документ определяет киберпространство как сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а кибербезопасность, в свою очередь, как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с

нежелательными последствиями [Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г. Режим доступа: http://ww.rg.ru/2009/10/20/ zakon-dok.html (дата обращения: 02.12.2016)].

Также не трудно заметить, что термин «кибертерроризм» употребляется довольно часто, но каждый автор вкладывает в него что-то свое. Ситуацию усугубляет и тот факт, что это понятие нормативно не закреплено ни в Уголовном кодексе, ни в Федеральном законе от 06.03.2006 № 35-ФЗ (ред. 31.12.2014) «О противодействии терроризму», ни в постановлении Пленума Верховного Суда РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности», ни в постановлении Пленума ВС РФ от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам и о преступлениях компьютерной направленности», ни в методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России).

При этом нельзя сказать, что Российское государство не замечает такого явления как кибертерроризм. Так согласно п. 45, пп. «г» «Концепции противодействия терроризму в Российской Федерации» (утв. Президентом РФ 05.10.2009) кадровое обеспечение противодействия терроризму осуществляется по следующим основным направлениям: подготовка специалистов в специфических областях противодействия терроризму (противодействие идеологии терроризма, ядерному, химическому, биологическому терроризму, кибертерроризму и другим его видам). Таким образом, из анализа указанной нормы можно сделать вывод, что под кибертерроризмом в концепции понимается разновидность терроризма [Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г. Режим доступа: http://ww.rg.ru/2009/10/20/ zakon-dok.html (дата обращения: 02.12.2016)].

Известно, что некоторые исследователи выделяют два вида кибертерроризма: совершение с помощью компьютеров и компьютерных сетей террористических действий (то есть терроризм в «чистом виде»), а также использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов [Усилинский Ф.А., 2014, с.7].

Первому виду кибертерроризма можно дать определение с помощью соединения понятий «киберпространство» и «террористический акт».

«Террористический акт (в соответствии со статьей 205 УК РФ в ред. Федерального закона от 27.07.2006 N 153-ФЗ) - 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» [Волеводз А.Г., 2007, с.17-25].

Таким образом, «кибертерроризм в чистом виде» - есть умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Это деяние должно быть совершено в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти. К этому виду терроризма можно отнести также угрозу совершения подобных действий для достижения вышеуказанных целей.

В свою очередь результаты анализа поступающей в Антитеррористический центр государств-участников СНГ информации позволяют сделать вывод об активизации попыток использования террористическими организациями для достижения своих преступных целей возможностей глобальной сети Интернет и о возрастании потенциальной опасности совершения актов так называемого кибертерроризма. К примеру,

спецслужбами России в 2012 году прекращено функционирование около 500 сайтов террористической, экстремистской и иной антиобщественной направленности; выявлена и расследована противоправная деятельность члена радикальной исламской транснациональной партии «Хизб-ут-Тахрир аль-Исламий», причастного к пропаганде экстремизма в сети Интернет, судом он приговорен к 1 году лишения свободы терактов [Усилинский Ф.А., 2014, с.7].

Что касается 2016 года, то количество киберпреступлений экстремистской направленности, зарегистрированных на территории России в первом полугодии 2016 года, на треть превысило аналогичные прошлогодние показатели, а террористических проявлений — почти на 40%. Всего в январе — июне зарегистрировано 752 преступления террористического характера и 741 преступление экстремистской направленности. В МВД отмечают, что рост статистики обусловлен активной борьбой правоохранительных органов с проявлениями экстремизма в интернете, а также уголовными делами в отношении лиц, принимавших участие в вооруженных конфликтах за рубежом, в том числе в Сирии, Ираке и на Украине.

В отличие от иных высокотехнологичных видов террористической деятельности (ядерный, биологический), кибертерроризм не требует привлечения уникальных, высокооплачиваемых, а зачастую находящихся под контролем спецслужб специалистов. Для найма высококвалифицированных специалистов в области информационных технологий, аренды высокоскоростных каналов связи, приобретения необходимых технических и программных средств, требуются сравнительно небольшие финансовые затраты. По мнению исследователей, анализ характера выявленных органами безопасности и правоохранительных органов вредоносных программ свидетельствуют о возможности отнесения некоторых из них к категории информационного оружия. В подтверждение данного тезиса начальник Департамента специальных технических мероприятий МВД России генерал-

полковник милиции Мирошников Б. Н. отмечает, что «информационное оружие может действовать избирательно.

Оно может быть применено через трансграничные связи, что может сделать невозможным выявление источника атаки. Поэтому информационное оружие может стать идеальным средством для террористов, а информационный терроризм может стать угрозой существованию целых государств, что делает вопрос информационной безопасности важным аспектом национальной и международной безопасности, и роль этого аспекта будет только усиливаться» [Россия в глобальной политике. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

Наибольшую опасность, представляет особая «разновидность» киберпреступников – те, кто распространяет информацию террористического или экстремистского содержания. На таких сайтах вывешивают не только нацистские или ваххабитские призывы, но и подробные инструкции по изготовлению взрывчатых устройств, организации терактов, убийств и даже расчленению трупов. Расследования ряда кровавых преступлений показали, что преступники свои криминальные знания почти полностью почерпнули в Интернете. Помимо этого, со слов главы МВД России Р.Нургалиева, террористические организации оказывают через Интернет «информационно-психологическое воздействие на молодежь в целях распространения радикальных доктрин, формирования антисоциального поведения и, в конечном счете, вербовки новых членов своих группировок, террористов-смертников, одновременно ведя широкую пропагандистскую кампанию по оправданию своих акций и запугиванию населения различных стран».

По данным МВД РФ в Интернете сейчас насчитывается «свыше 4800 сайтов, принадлежащих различным экстремистским организациям, тогда как всего пятнадцать лет назад их было только 12» терактов [Россия в глобальной политике. Электронный ресурс. Режим доступа:

http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

Сегодня очевидно, что количество людей, кто видит в Интернете самый доступный способ для пропаганды экстремизма и призывов к терроризму, увеличивается. Хозяева подобных сайтов понимают, что их деятельность незаконна, поэтому стараются по максимуму обезопасить себя. Для этого они не только стараются скрыть сайт от индексирования поисковыми системами, но и размещают его на заграничных серверах, чтобы следователям было как можно сложнее найти владельца нелегального ресурса. Как отмечают эксперты, в Рунете на сегодня выявлено более 70 сайтов, в США - 49, в Нидерландах – 6, в Германии – 5, в Великобритании – 4, в Канаде – 3, а в Турции – 2 [Россия в глобальной политике. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

Между тем, мировым сообществом в данное время наработан определенный положительный опыт борьбы с кибертерроризмом. На международном и межгосударственном уровне принят ряд нормативных правовых актов, регламентирующих данную проблему. Так, Генеральной Ассамблеей ООН в резолюции 53/70 от 4 декабря 1998 года были затронуты вопросы целесообразности разработки общепринятых международных принципов организации противодействия кибертерроризму, предусматривающих усиление безопасности глобальных информационных и телекоммуникационных систем и борьбу с информационным терроризмом и преступностью [Волеводз А.Г., 2007, с.17-25].

Значительным шагом в формировании международной правовой базы в данном направлении стало подписание 23 ноября 2001 года представителями стран – членов Совета Европы, США, Канады и Японии Конвенции Совета Европы «О киберпреступности». Она определяет приблизительный перечень преступлений, совершенных в информационной сфере, против информационных ресурсов или с помощью информационных средств и

признает их киберпреступлениями. Здесь же предусматривается необходимость решения ряда процедурных вопросов о выявлении и документировании компьютерных преступлений. На сегодняшний день Конвенция подписана 43 членами ЕС и 15 другими странами, включая США.

В последние годы активно прорабатываются вопросы совершенствования нормативной правовой базы стран Содружества в данном направлении. Так, Указ Президента России «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» от 12 мая 2004 года N 611 запрещает госорганам пользоваться Интернетом без средств защиты и регламентирует, какие спецслужбы должны за это отвечать. Как подчеркивала пресс-служба Президента России, Указ направлен главным образом на обеспечение защиты российского сегмента сети Интернет, в первую очередь – сетевых ресурсов государственных органов, от внешних угроз несанкционированного воздействия. При этом речь идет, в первую очередь, о предотвращении возможных попыток компьютерного «взлома» и получения контроля над сетевыми ресурсами органов власти России с террористическим умыслом [Волеводз А.Г., 2007, с.17-25].

Подводя итог, нормативно-правовое обеспечение противодействие кибертерроризму в РФ требует доработки. Важным является то, что требуется добавить в гл. 24 УК РФ новый состав преступления, устанавливающий уголовную ответственность за «кибертерроризм», определив наказание за совершение указанного преступления свыше 10 лет лишения свободы. При этом полагаем возможным внести изменения в ст. 151 УПК РФ и отнести кибертерроризм к подследственности органов ФСБ РФ.

Еще одной проблемой, на наш взгляд, является то, что нормативно не определены формы проявления такого явления как кибертерроризм. Разумно было бы издать соответствующее постановление Пленума Верховного Суда, этот шаг позволил бы излишне не перегружать УК РФ и закон о противодействии терроризму.

Глава 2. Практика борьбы с кибертерроризмом в РФ в XXI в.

2.1. Деятельность РФ по противодействию кибертерроризму

Современный этап развития мирового сообщества характеризуется стремительным развитием научно-технического прогресса, в который включается и сфера высоких технологий. В Окинавской хартии глобального информационного общества отмечалось, что «…информационные телекоммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества XXI в. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества. Информационно-коммуникационные технологии быстро становятся важным стимулом развития мирового сообщества» [Голубев В.А. Кибертерроризм как новая форма терроризма. Режим доступа: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

Вместе с тем, развитие научно-технического прогресса всегда сопровождается всплеском негативных общественных проявлений, в частности таких, как преступность. Одновременно с развитием компьютерной техники появилась преступность, связанная с электронной обработкой информации, в том числе и преступность террористической направленности – «Террористический акт» (ст. 205 УК РФ), «Содействие террористической деятельности» (ст. 205-1), «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма» (ст. 205-2), «Заведомо ложное сообщение об акте терроризма» (ст. 207). По мнению специалистов, терроризм с использованием последних достижений в сфере высоких технологий не менее опасен, чем ядерный или бактериологический терроризм [Голубев В.А. Кибертерроризм как новая форма терроризма [электронный ресурс]. URL: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

Смысл термина «противодействие кибертерроризму» более широк, чем борьба с кибертерроризмом, которая подразумевает непосредственное пресечение теракта или наказание виновных.

Противодействие – это совокупность законодательных, идеологически-информационных, организационных, административно-правовых, воспитательных, в том числе и пропагандистских, мер, призванных упредить появление субъектов кибертерроризма (особенно групп и организаций), воспрепятствовать им, не допустить их перехода к активным действиям, к реализации преступных намерений [Бекяшев К.А.,2004., с.,140].

Опыт многих иностранных государств в борьбе с терроризмом, безусловно, необходимо изучать, а изучив, - использовать во благо обществу. Политическое руководство основных стран европейского Запада и Соединенных Штатов рассматривает противодействие терроризму в качестве одной из важнейших общегосударственных задач [Аксенов А. В., Журнал. 2002. № 4,с.6.].

Таким образом, противодействие – это комплекс мер, благодаря которым не происходит активных действий, для реализации террористических намерений.

Существуют свои цели и задачи, направления и принципы противодействия терроризму.

Основными направлениями в деятельности противодействия терроризма являются:

- совершенствование правовой базы;
- усиление взаимодействия между соответствующими федеральными органами;
- формирование специальных подразделений и увеличение численности сотрудников федеральных структур, занимающихся проблемой терроризма, улучшение их технической оснащенности [Аксенов А. В., Журнал. 2002. № 4. с.6.].

Арсенал компьютерных террористов – различные вирусы, логические бомбы – команды, встроенные заранее в программу и срабатывающие в нужный момент. Современные террористы используют Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие.

Однако можно предполагать, что компьютерный терроризм сегодня уже представляет реальную угрозу обществу. В настоящее время существует весьма мало систем, которые можно назвать надежно защищенными.

Начало активного использования Интернета террористическими и экстремистскими организациями в России можно отнести к началу 2000-х годов. В дальнейшем развитие данного процесса шло в геометрической прогрессии. Только в 2005–2006 гг. было зафиксировано более 2 млн. компьютерных нападений на информационные ресурсы органов государственной власти, в том числе свыше 300 тыс. атак на интернет-представительство президента РФ [Еделев А.Л., 2006, с.192].

Отмеченная негативная тенденция продолжает сохраняться и в настоящее время. Она полностью корреспондируется с развитием криминальной составляющей киберпреступности в Российской Федерации. Так, если 55 % сайтов, противоречащих британских законам, зарегистрированы в США, то 23 % – инициированы из России [Голубев В.А. Кибертерроризм как новая форма терроризма. Режим доступа: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

В российском сегменте Интернета действует более ста интернет-сайтов российских радикальных структур (pn14.info, dpni.org, tor85. livejournal.com и т. д.). Они, как правило, пропагандируют политические идеи, проводят агитационную и вербовочную деятельность, направленную на увеличение числа своих сторонников.

Противостоять компьютерному терроризму, дополняющему обычный терроризм, в настоящее время практически не возможно. Это объясняется тем, что государственное регулирование, цензура и другие формы контроля над информацией, распространяемой в Интернете, отсутствуют. Именно обезличенность и неограниченность в пространстве делают интернет эффективным средством для достижения преступных целей, а шансы обнаружения преступников крайне низкими [Голубев В.А. Кибертерроризм

как новая форма терроризма. Режим доступа: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

С начала 2000-х гг. Российская Федерация принимает активное участие в разработке международных норм, закрепляющих меры борьбы с кибертерроризмом. Однако проводимые меры по борьбе с кибертерроризмом носят скорее формальный характер, и нередко оказываются неэффективными в практической деятельности. Это подтверждают повторяющиеся с каждым годом факты кибератак на крупнейшие компании и государственные органы, как в России, так и за рубежом.

В 2013 году Президент РФ Путин В. В. своим Указом от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» возложил на ФСБ РФ полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

Основными задачами указанной структуры являются:

1)Прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации.

2)Обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3)Осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

4)Установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации

В структуре МВД тоже существует структура, осуществляющая противодействие преступлениям в сфере компьютерной информации. Так основными направления работы МВД России является:

1) Выявление и пресечение фактов неправомерного доступа к компьютерной информации.
2) Борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ.
3) Противодействие мошенническим действиям с использованием возможностей электронных платежных систем.
4) Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет.
5) Выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи.
6) Противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.
7) Противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.
8) Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.
9) Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий. Борьба с международными преступлениями в сфере информационных технологий.

Следует отметить, что общество также оценивает политику России по данному вопросу как не эффективную. По результатам анкетирования, проведенного среди молодежи, лишь 18,42 % опрошенных высказались за эффективность существующих мер по противодействию компьютерному терроризму (опрос проводился в 2016 году в г. Омске среди 97 человек

(студенты и государственные служащие в возрасте от 18 до 30 лет) [Голубев В.А. Кибертерроризм как новая форма терроризма. Режим доступа:: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

В Российской Федерации пока должного внимания указанной выше проблеме не уделяется. Термин кибертерроризм легально не закреплен ни в одном нормативно-правовом акте. Уголовная ответственность за совершение террористического акт предусмотрена ст. 205 УК РФ, при этом квалифицированного признака, связанного с осуществлением данного акта в киберпространстве российский Уголовный кодекс не предусматривает.

В российской юридической литературе проблемы кибертерроризма, его определение рассматриваются весьма слабо. Рядом авторов под кибертерроризмом понимается совокупность противоправных действий, 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 [Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства. Режим доступа: http://www.crime-research.ru/analytics/malishenko (дата обращения: 05.03.2017]

Голубев В.А. под кибертерроризмом понимает преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [Голубев В.А. Кибертерроризм как новая форма терроризма. Режим доступа: http://www.crime-research.org/ (дата обращения: 27.03.2017)].

По мнению Ю.В. Гаврилова и Л.В. Смирнова, сущность кибертерроризма заключается в оказании противоправного воздействия на информационные системы, совершенного в целях создания опасности причинения вреда жизни, здоровью или имуществу неопределенного круга лиц путем создания условий для аварий и катастроф техногенного характера либо реальной угрозы такой опасности [Пахарева Е.Н., 2011, с. 54].

Проблемы кибертерроризма рассматриваются в научных работах А.И. Примакина, В.Е. Кадулина, Ю.И. Жукова, В.И. Антюхова, Е.П. Кожушко, В. Замкового, М. Ильчикова и ряда других. Таким образом, попытки дать понятие компьютерного терроризма многочисленны, однако комплексного анализа не выявлено [Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства. Режим доступа: http://www.crime-research.ru/analytics/malishenko (дата обращения: 05.03.2017].

Обеспечение безопасности от кибертеррористической угрозы становится с каждым годом одним из главных приоритетов национальной безопасности России. Основой же обеспечения борьбы с киберпреступностью является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению таких действий [Пахарева Е.Н., 2011, с. 54].

Российская Федерация осуществляет политику противодействия кибертерроризму в рамках реализации основных принципов построения информационного общества. Это обусловлено необходимостью создания общенациональных систем безопасности информационно-коммуникационной инфраструктуры, обеспечивающих надежную ее защиту от возможных угроз.

Сегодня в России существует некая противоречивость обсуждаемых в обществе взглядов на необходимость или на отсутствие необходимости государственного регулирования национального сегмента сети Интернет. С одной стороны, реализация гражданином конституционных прав на

свободное получение информации и пользование ею, и, с другой стороны, необходимость обеспечения безопасности государства, общества и личности в информационно-коммуникационной сфере.

Использование террористами этих прав и свобод для пропаганды своей деятельности, подрыва государственного строя и причинения иного ущерба, обусловливает необходимость безусловного обеспечения законности и правопорядка, стоящих на защите общества и личности, закрепления права за спецслужбами осуществлять мониторинг виртуального пространства и принятия мер к прекращению деятельности в нем террористических структур.

Главная проблема в противодействии кибертерроризму не в том, что Уголовный кодекс РФ и Уголовно-процессуальный кодекс РФ имеют какие-то изъяны, а в том, что защита чаще оказывается более подготовленной, чем обвинение; в том, что правоохранительные органы на первоначальном этапе расследования, проводя осмотр места происшествия, могут допускать много следственных ошибок, теряется криминалистически значимая информация и, в конечном итоге, уголовное дело, не доходя до суда, может просто «рассыпаться».

Судебных процессов по уголовным делам, связанным с компьютерными преступлениями очень мало, вследствие чего судебная практика не наработана, а судьи не имеют необходимой подготовки [Пахарева Е.Н., 2011,с. 54].

Криминал в интернете все чаще приобретает транснациональный характер. С использованием глобальной сети такие виды преступлений не имеют государственных границ и могут легко совершаться субъектами одного государства в отношение субъектов другого государства. С учетом этого, стратегия борьбы с компьютерной преступностью должна строиться на посылке о том, что данной проблемой необходимо заниматься системно и комплексно, а это, в свою очередь, требует тесного сотрудничества как на национальном, так и на международном уровне.

Следует иметь в виду, что кибертерроризм – это не только хакеры или вирусы. Как известно, на большей части компьютеров во всем мире установлена операционная система Windows 95/98/00/NT, содержимое и внутреннее устройство которой знает лишь очень ограниченный круг лиц на фирме-разработчике. Совершенно не исключено, что эта информация может попасть в руки террористов, которые смогут дать сигнал для переформатирования дисков компьютеров и утери хранящейся на них информации. В России в настоящее время большая часть (несколько тысяч) коммерческих баз данных функционирует с применением минимальных средств защиты и не обеспечивает необходимого уровня защиты. Все это очень опасно и наносит ощутимый вред как государству в целом, так и конкретным владельцам массивов конфиденциальной информации [Тропинина Т.Л. Киберпреступность и кибертерроризм .Режим доступа: http://www.crimeresearch.ru/analytics/ (дата обращения: 05.03.2017)].

Россия предложила на рассмотрение ООН пакет международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и на борьбу с информационным терроризмом и криминалом. В документе зафиксировано право каждого как на получение и распространение информации, так и на защиту своих информационных ресурсов от неправомерного использования и несанкционированного вмешательства. Согласно предложению России, ООН предстоит определить признаки и классификацию информационных войн и информационного оружия, создать систему международного слежения за выполнением взятых на себя государствами обязательств и механизм разрешения конфликтных ситуаций в этой сфере. В документе оговорена также международная ответственность государств за выполнение обязательств и процедура мирного урегулирования споров по информационным проблемам.

В Российской Федерации можно выделить конкретные проблемы противодействия и выявления кибертерроризма. Например, Данильченко Э.

Д. выделяет такие проблемы, как [Россия в глобальной политике. Электронный ресурс. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)]:

1. Отсутствие соответствующих законодательных актов, адекватных современному положению дел в сфере защиты компьютерной информации и регулирующих отношения в сети Интернет.

2. Отсутствие необходимых технических средств у следственных и оперативных органов не способствует своевременной фиксации фактов совершения актов кибертерроризма.

3. Недостаточное количество специально подготовленных кадров, специализирующихся на выявлении и раскрытии компьютерных преступлений, а также специализированных подразделений ПО.

4. Система защиты интернет-серверов и информационно-коммуникационных систем не успевает совершенствоваться вслед за все более совершенными способами и методами совершения актов кибертерроризма.

В случае совершения кибертеррористического акта трудно установить место его совершения, так как данные преступления отличаются своим трансграничным характером. Расположение компьютера, с помощью которого совершается преступление, крайне редко совпадает с местом расположения объекта посягательства и последствиями деяния. Кроме этого, проблему составляет сохранение следов совершения преступления, а также процесс розыска кибертеррористов, что существенно снижает шансы привлечения преступника к уголовной ответственности [Россия в глобальной политике. Электронный ресурс. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

На наш взгляд, основной проблемой, с которой сталкиваются при противодействии кибертерроризму, является его трансграничный характер. Это связано с тем, что отличительной чертой кибертерроризма является

то, что насильственные действия производятся лицом не непосредственно на месте совершения теракта (путем взрыва, поджог и т. д.), а удаленно и через киберпространство. Кибертеррорист может находиться даже на территории другого государства.

Таким образом, в Российской Федерации системного противодействия кибертерроризму не ведется. Существуют разрозненные попытки осуществлять борьбу с данным видом проявлением терроризма. Отсутствует необходимая нормативно-правовая база. При этом для эффективного противодействия кибертерроризму необходимы совместные усилия всех членов мирового сообщества.

2.2. Пути совершенствования мер противодействия кибертерроризму в РФ в XXI в.: ситуационный анализ

Как уголовно-правовой феномен, терроризм носит международный характер и в соответствии с рядом международных документов относится к числу международных преступлений. В полной мере это распространяется и на новые формы его проявления – кибертерроризм или, как его часто еще называют, компьютерный терроризм. Анализ мировых тенденций развития кибертерроризма с большой долей вероятности позволяет прогнозировать, что его угроза с каждым годом будет возрастать [Морозов И.Л. Пределы информационной свободы в российском киберпространстве: как смягчить столкновение интересов государства, гражданского общества, независимой науки? Режим доступа: http://morozov.vlz.ru/library/infsvob.htm (дата обращения 16.04.2017)].

Постоянно растет число пользователей сети Интернет. В США их уже 158 миллионов, в Европе – девяносто пять, в Азии – 90, в Латинской Америке

– четырнадцать, а в Африке – три. В России, по разным оценкам, количество пользователей Интернет составляет от 3,5 до 8 миллионов человек (рис.2.).

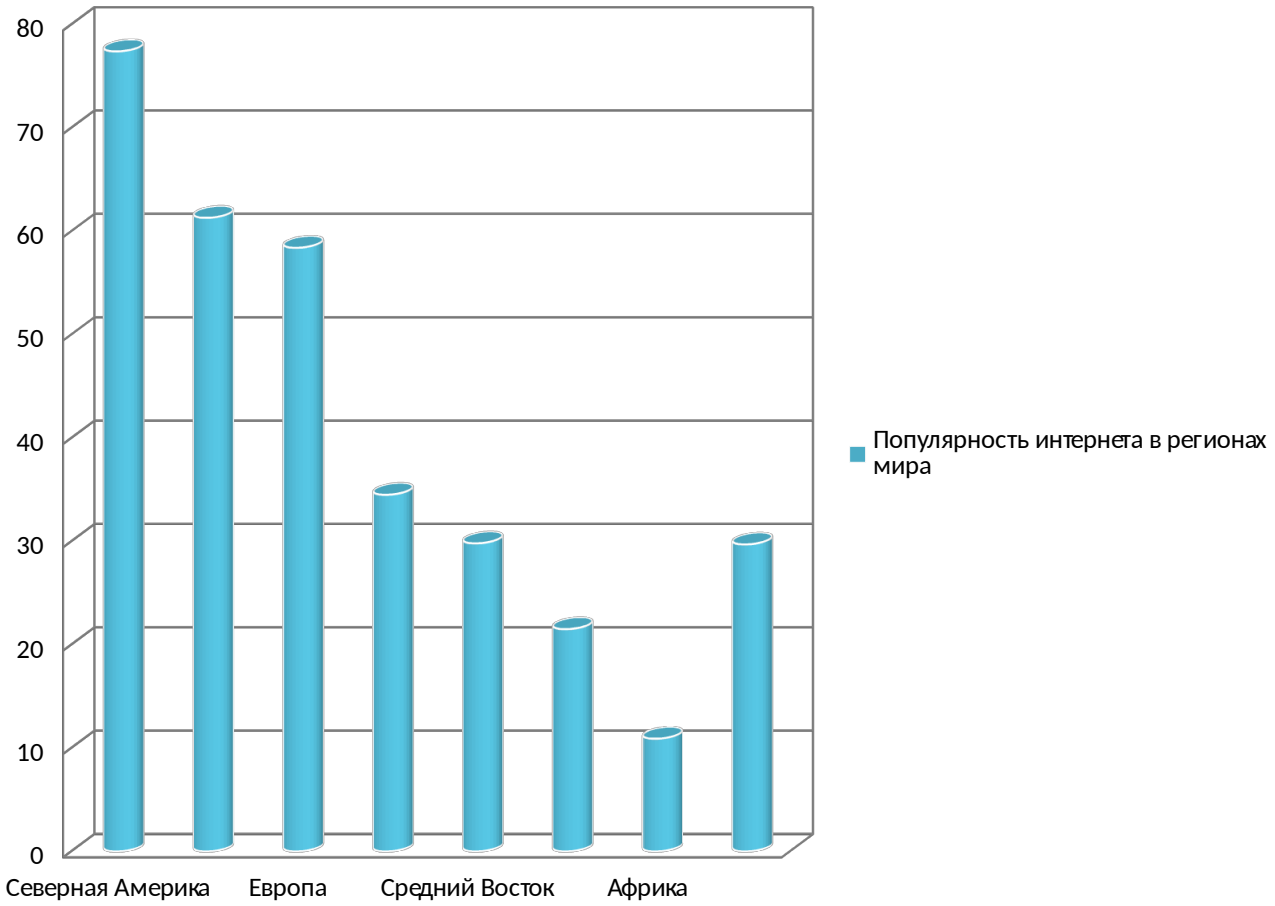

Рис. 2. Популярность интернета в различных регионах мира

Исходя из вышеуказанного рисунка, сегодня можно говорить, что Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира.

Внедрение современных информационных технологий, привело к появлению новых видов преступлений, таких как компьютерная преступность и компьютерный терроризм – незаконное вмешательство в работу электронно-вычислительных машин, систем и компьютерных сетей,

хищение, присвоение, вымогательство компьютерной информации. По своему механизму, способам совершения и сокрытия компьютерные преступления имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости. Кроме этого, компьютерный терроризм способен дестабилизировать обстановку поэтому необходимо рассмотреть те негативные факторы, которые уже сегодня проявляются в связи с широким появлением кибертеррористов и как эти факторы могут повлиять на дальнейшее развитие России.

Цель ситуационного анализа: выявить тенденции развития проблемы противодействия кибертерроризму в Российской Федерации.

Объект исследования: влияние действий кибертеррористов на развитие России.

Сегодня российский сегмент сети Интернет используется кибертеррористами для размещения информации как антигосударственной, антиправительственной, антипрезидентской направленности, так и террористического характера.

В настоящий период террористы ИГИЛ активно используют Интернет как для переписки при подготовке преступлений, так и для пропаганды своих идей и дискредитации Президента, Правительства, существующей власти в России.

Таблица 1

Прямые и косвенные участники

Актор/субъект	**Цель**
Непосредственные участники	

Страны, подверженные кибертеррористическим атакам (Российская Федерация, США, Вьетнам, Индонезия, Индия, Китай)	• Противодействие кибертерроризму; • Уничтожение кибертеррористических группировок.
Кибертеррористические организации (как правило террористические группировки)	• Дестабилизация обстановки в мире; • уничтожение информации, программного обеспечения, технических ресурсов путем внедрения вирусов, программных закладок, преодоления систем защиты; • техническое внедрение в каналы трансляции средств массовой информации с целью распространения слухов, дезинформации, объявления требований террористической организации; • проведение информационно-психологических операций, воздействующих на сознание населения.
Косвенные участники	
Государства – спонсоры кибетерроризма	• Экономические интересы; • Дестабилизация положения стран • Продемонстрировать превосходство своего государственного устройства и мировоззрения над политическими системами и образом жизни других людей.

Для того чтобы выявить проблему противодействия кибертерроризму в Российской Федерации, необходимо сделать краткий экскурс в историю появления данного вида терроризма.

Данная проблема волнует не только Россию, но и Европу, и Северную Америку. Если в 1996 г. в России было выявлено 15 компьютерных преступлений, то в 1997-м – уже 101, причем размер понесенного ущерба достиг 20 млрд. руб. А за пять лет количество подобных преступлений выросло в 33 раза – уже в 2002 г. в России зарегистрировано 3 371 преступление в области компьютерной информации. Об этом в ходе

всероссийской конференции «Информационная безопасность России» в 2002 году сообщил начальник Главного управления специальных технических мероприятий МВД РФ Борис Мирошников. По его словам, из числа зарегистрированных правонарушений в области компьютерной информации, свыше 90% составляли преступления, связанные с незаконным доступом к информационным ресурсам, так называемые «компьютерные взломы». Большая часть киберпреступлений осталась скрытой и не регистрируется правоохранительными органами. Процентное соотношение раскрытых и нераскрытых правонарушений пока установить не удается (табл. 2.).

Таблица 2

Зарегистрированные преступления и выявленные лица в разрезе статей Особенной части УК РФ в России в 2010 и 2015 гг.

Преступления - статьи УК РФ	Зарегистрировано преступлений в течение года		Выявлено лиц, совершивших преступления			
			Всего	В т.ч. по наиболее тяжкому составу преступления	Всего	В т.ч. по наиболее тяжкому составу преступления
Годы	2010	2015	2010			

Продолжение таблицы 2

Раздел 13. Преступления в сфере компьютерной информации						
Годы	2010	2015	2010		2015	
Неправомерный доступ к компьютерной информации - ст. 272	5234	1930	569	368	270	139
Создание, использование и распространение вредоносных программ для ЭВМ - ст. 273	1995	889	390	79	411	222
Нарушение правил эксплуатации ЭВМ, системы	7	1	0	0	0	0

ЭВМ или их сети - ст. 274						
Итого:	7236	2820	878	447	638	361

С начала 2000-х гг. Российская Федерация принимает активное участие в разработке международных норм, закрепляющих меры борьбы с кибертерроризмом. Так, в течение 2001–2005 гг. Россия активно участвовала в разработке проекта Конвенции Совета Европы 2005 г. «О предупреждении терроризма» и первой ратифицировала ее 21 апреля 2006 г.

Кроме того, меры противодействия закрепляются во многих нормативных актах внутреннего законодательства страны: п. 45 Концепции противодействия терроризму в Российской Федерации (утв. Президентом РФ 05.10.2009); Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»; п. 109 Указа Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» (в ред. от 1.07.2014 г.); Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и т. д.

Стоит отметить хронологию случаев наиболее крупных действий кибертеррористов, направленных на приостановку работы российских банков и финансовых организаций за последние три года. В приводимый список не вошли кибертеррористические акты, связанные с похищением средств российских банков [Россия в глобальной политике. Электронный ресурс. Режим доступа: http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)].

- 30 сентября 2013 г. хакерская группировка Anonymous Caucasus опубликовала на видеосервисе YouTube ролик, в котором сообщила о начале

операции против российских банков «в отместку за геноцид кавказских народов». По данным «Лаборатории Касперского», 1 октября 2013 г. DDoS-атаке подвергся сайт Сбербанка, 2 октября - сайт Альфа-банка, 3 октября - сайты Банка России, Альфа-банка и Газпромбанка. Целью нападения было ограничение доступа к публичным сайтам банков, однако к затруднениям в их операционной деятельности атаки не привели. В частности, работа сайта ЦБ была прервана всего на семь минут.

- 24 марта 2014 г. работа сайта Банка России прерывалась на период с 09:45 по 11:00 мск в результате DDoS-атаки, мощность которой более чем в десять раз превышала пропускную способность каналов связи сайта.
- 17 марта 2014 г. российские банки подверглись DDoS-атаке, которая на время вывела из строя сайт и интернет-сервисы банка ВТБ 24 (на работе отделений, банкоматов и пластиковых карт атака не отразилась), а также интернет-сервисов и части банкоматной сети Альфа-банка. Ответственность за атаку взяла на себя группировка Anonymous Caucasus.
- 2 октября 2015 г. «Лаборатория Касперского» сообщила, что с 25 сентября фиксировала крупнейшую с начала года волну продолжительных DDoS-атак на сайты и системы онлайн-анкинга восьми крупных российских банков. Половина атакованных кредитных учреждений получила от организаторов этой DDoS-волны сообщения с требованием заплатить выкуп за прекращение атак в криптовалюте биткойн [Новостные сообщения. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 04.12.2016)].

Это обстоятельство позволило экспертам «Лаборатории Касперского» предположить, что за атаками стоит хакерская группировка DD4BC, которая ранее в 2015 г. также требовала биткойн-выкуп в ходе атак на банки и финансовые учреждения других стран мира. Какого-либо ущерба российским банкам инциденты не нанесли [Новостные сообщения. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 04.12.2016)].

- 10 ноября 2016 г. ФинЦЕРТ (организация Банка России по борьбе с киберпреступлениями) зафиксировал хакерские DDoS-атаки на несколько крупных банков и передал эту информацию в правоохранительные органы. Сообщалось, в частности, что 8 ноября 2016 г. Сбербанк отразил серию мощных DDoS-атак, организованных из нескольких десятков стран. По данным газеты «Ведомости», похожим кибернападениям подверглись Альфа-банк, Банк Москвы (структура ВТБ) и Московская биржа. СМИ сообщали, что под удар попали также банк «Открытие» и Росбанк.
- По информации ФинЦЕРТ, в атаке участвовали бот-сети из так называемых устройств «интернета вещей», нарушений доступности сервисов банков не фиксировалось. По данным «Лаборатории Касперского», злоумышленники атаковали сайты минимум пяти известных финансовых организаций из ТОП-10. Эта серия атак стала первой в 2016 г. масштабной DDoS-волной, направленной на российские банки [Новостные сообщения. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 04.12.2016)].

Стоит также отметить, что огромное количество атак являются не зарегистрированными. Это обуславливаются несколькими причинами, представленными в рисунке 3. (рис.3).

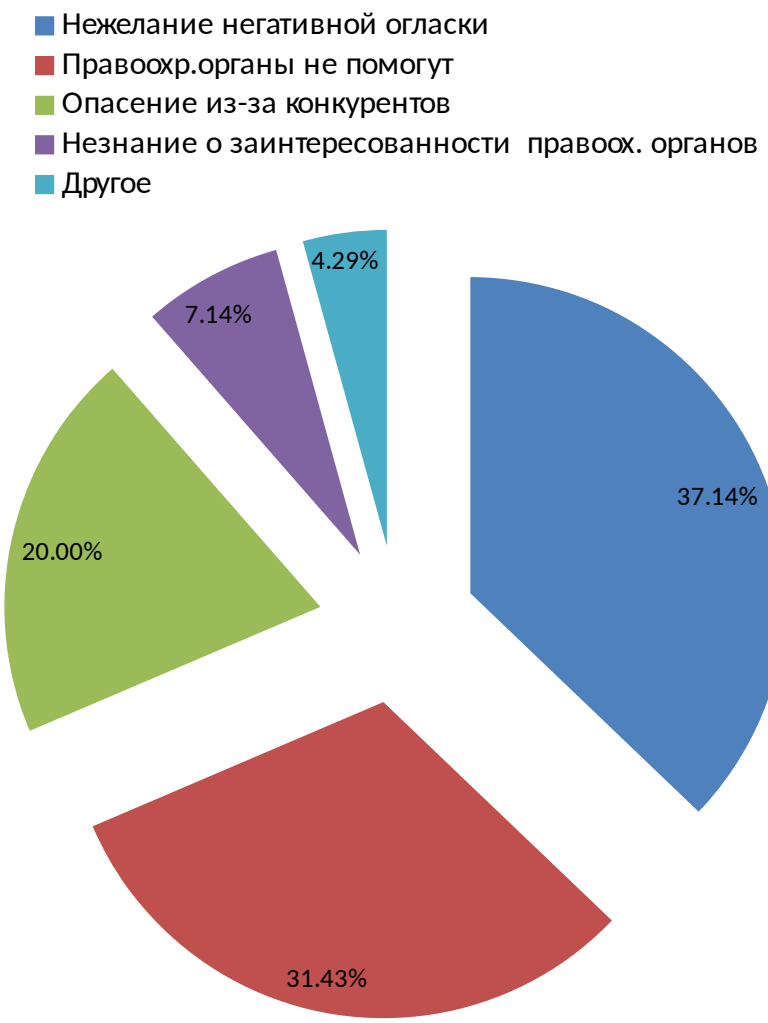

Рис. 3. Причины, по которым организации не сообщают о кибертеррористических действиях

Проанализировав наиболее крупные кибератаки в Российской Федерации, можно выделить следующие **приемы** кибератак [Новостные сообщения. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 04.12.2016)]:

- получение несанкционированного доступа к личной, коммерческой, банковской информации, к государственным и военным секретам;
- нанесение ущерба физическим элементам информационного пространства (например, создание помех, нарушение работы сетей

электропитания, использование специальных программ, которые разрушают аппаратные средства);

- уничтожение информации, программного обеспечения, технических ресурсов путем внедрения вирусов, программных закладок, преодоления систем защиты;
- техническое внедрение в каналы трансляции средств массовой информации с целью распространения слухов, дезинформации, объявления требований террористической организации;
- уничтожение или подавление работы линий связи, перегрузка узлов коммуникации, изменение адресации запросов в сети Интернет;
- проведение информационно-психологических операций, воздействующих на сознание населения и др.

Эти приемы постоянно совершенствуются в зависимости от средств защиты, которые применяют разработчики компьютерных сетей. Так, киберпреступники могут использовать в сетях различного вида атаки, которые позволяют им получить доступ к корпоративной сети, перехватить управление ею или заблокировать информационный обмен в сетях [].

К **средствам** осуществления таких атак относят компьютерные вирусы:

- сетевых червей, модифицирующих и уничтожающих секретную информацию или блокирующих работу вычислительных систем;
- логические бомбы, которые срабатывают при определенных, запланированных преступниками, условиях;
- «троянские кони», отсылающие своему «владельцу» через Интернет различную информацию с зараженного компьютера.

Далее приведём популярность средств осуществления кибертеррористической угрозы, от общего числа инцидиентов (рис.4.)

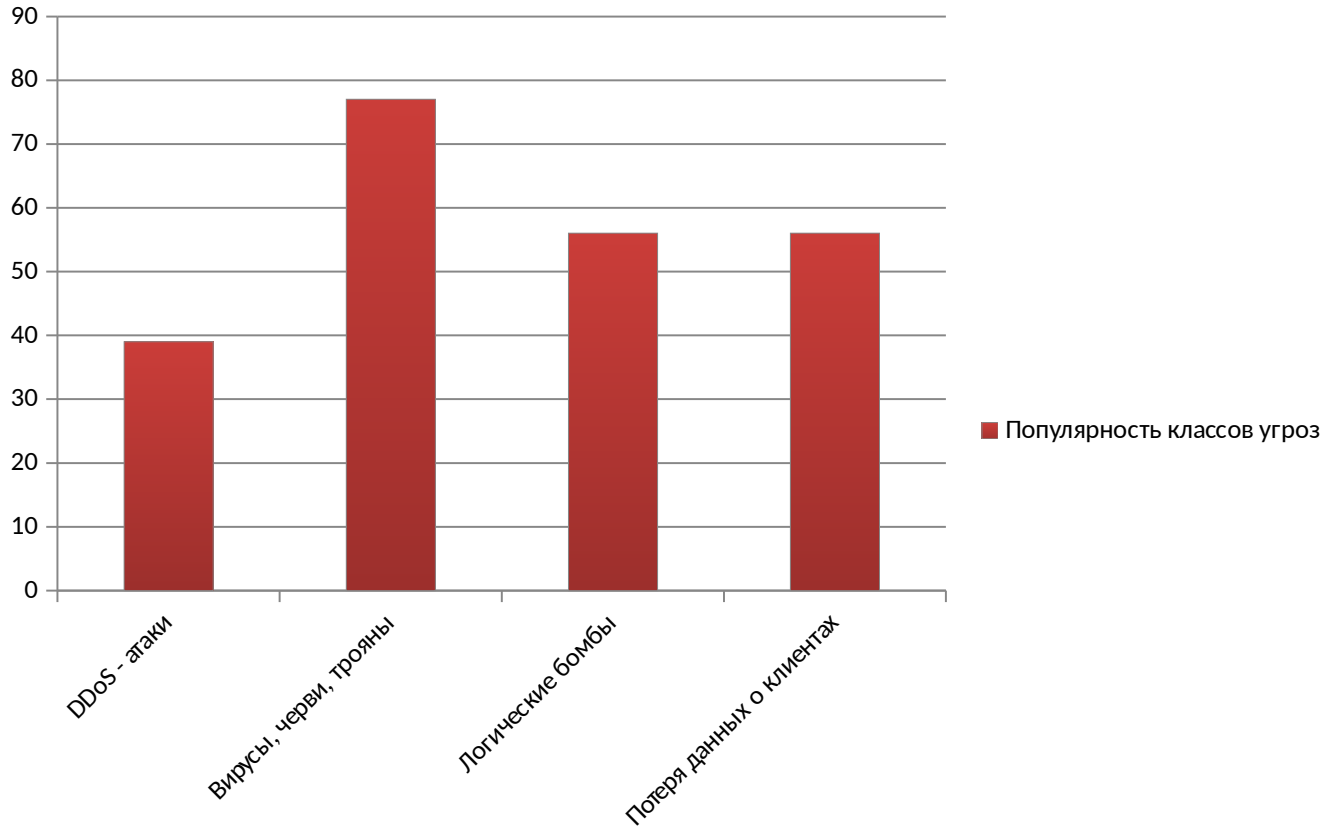

Рис. 4. Популярность классов кибертеррористических угроз, % от общего числа инцидентов, за период с 2013-2016 гг.

Анализ нормативно-правовых актов позволяет выделить следующие причины возникновения кибертерроризма – политические, социальные и экономические.

Политические причины подразделяются на внешние и внутренние. К внешним причинам относятся глобализация, углубление разрыва между уровнями благосостояния различных стран, военная агрессия в отношении другого государства и его оккупация, усиление глобального цифрового противоборства и разрыв в уровне информационного развития стран, столкновение политических интересов различных государств. Внутренними причинами являются политическая нестабильность и обострение политических конфликтов внутри государства, отсутствие механизмов взаимодействия государственной власти и гражданского

общества, навязывание правящей элитой не свойственных для данного общества социально-политических реформ и иных нововведений, недовольство граждан страны деятельностью правительств иностранных государств; поощрение кибертерроризма руководством сраны, общественными организациями и в СМИ.

Среди *социальных причин* возникновения кибертерроризма можно выделить возросшую социальную дифференциацию в обществе, раскол его на группы с различным экономическим положением, заметное снижение качества жизненного уровня людей, слишком медленный процесс формирования среднего слоя общества.

Экономические причины возникновения кибертерроризма включают в себя продолжающийся экономический и энергетический кризис, рост цен, инфляции и безработицы.

Правоохранительные органы стремятся повысить безопасность информационного пространства посредством сведения к минимуму воздействия кибертеррористов на информационные системы. Однако в настоящее время данная проблема уже вышла из сферы контроля правоохранительных органов и переросла в серьезную государственную и международную проблему.

Отметим действующие факторы в данном вопросе:

Действующие факторы

Таблица 3

Фактор	Суть
Внешнеполитический фактор	• рост числа кибертеррористических проявлений в ближнем и дальнем зарубежье; • распространение идей терроризма и экстремизма через информационно-телекоммуникационную • агрессивная политика в отношении другого государства и его оккупация, • столкновение политических интересов различных государств
Внутренний фактор	• политическая нестабильность и обострение политических

Продолжение таблицы 3

	конфликтов внутри государства, • отсутствие механизмов взаимодействия государственной власти и гражданского общества, • навязывание правящей элитой несвойственных для данного общества социально-политических реформ и иных нововведений, • недовольство граждан страны деятельностью правительств иностранных государств
Экономический фактор	• экономический кризис, • безработица молодежи приводит к созданию группировок, желание быстро разбогатеть приводит к террористической деятельности. • получение незаконного доступа к личной, коммерческой, банковской информации, к государственным и военным секретам
Социальные причины	• возросшая социальная дифференциация в обществе, раскол его на группы с различным экономическим положением, • заметное снижение качества жизненного уровня людей, слишком медленный процесс формирования среднего слоя общества
Религиозный фактор	• вербование новых лиц для террористической деятельности

На основе анализа научной литературы, международных правовых документов и законодательства ряда стран можно выделить следующие **особенности** кибертерроризма.

Во-первых, явление кибертерроризма неразрывно связано с информационным оружием, так как для достижения своих преступных целей он использует информационно-коммуникационные технологии, компьютерные системы и сети, специальное программное обеспечение.

Во-вторых, следует признать, что это понятие носит международный характер, поскольку преступники часто находятся в одном государстве, а их жертвы – в другом.

В-третьих, важной особенностью кибертерроризма является многообразие его целей: от умышленного создания обстановки напряженности, подавленности и страха на социальном уровне до совершения с помощью компьютеров и компьютерных сетей террористических действий.

Необходимо отметить также четвертую важную особенность – киберпреступления характеризуются высоким уровнем латентности и низким уровнем раскрываемости, они требуют от исполнителей сравнительно небольших финансовых затрат, однако при этом наносят огромный моральный и материальный ущерб, позволяя достигать политических целей минимальными усилиями.

Проанализировав средства массовой информации за 2014-2017, был проведен контент-анализ по статьям журналов и газет по теме «Кибертерроризм и противодействие ему» (приложение 1). Мнения экспертов имеют общие характерные черты. Например, Демидов О. и Черненко Е. отмечают, что вопрос о необходимости создания правил поведения в киберпространстве именно вокруг глобальной инфраструктуры интернета уже активно обсуждается в экспертном и техническом сообществе. В этом схожи и мнения других исследователей. Кроме того, Касперский Е. отмечает, что наиболее опасная террористическая организация ИГИЛ (запрещенная в Российской Федерации) активно использует методы кибертерроризма. Исследователь Васильев К. отмечает также, что наибольшее количество исследований, посвященных кибертерроризму, проводится в Соединенных Штатах Америки. И необходимо, чтобы противодействие кибертерроризму стало одной из приоритетных задач в борьбе с преступностью в России .

Исходя из характера и особенностей актов кибертерроризма, можно спрогнозировать следующие возможные уровни развития **ситуации по противодействию** с ним.

Научный

Данный уровень должен обеспечиваться организационной и, в первую очередь, финансовой поддержкой научных исследований феномена кибертерроризма.

Работа на этом уровне может развиваться в следующих направлениях:

- разработка единого понятийного аппарата, включая универсальное определение кибертерроризма с целью его дальнейшей кодификации в уголовном законодательстве страны;
- совершенствование критериальной основы оценки безопасности информационно-коммуникационных технологий, разработка новых конструктивных моделей тестирования, верификация средств защиты сложно организованных компьютерных систем, формирование доказательной базы их гарантированной защищенности;
- совершенствование системы подготовки кадров в образовательных учреждениях высшего образования МВД России в области информационной безопасности, причем, как специалистов по техническим аспектам защиты информации, так и обучающихся по специализации «Расследование преступлений в сфере компьютерной информации»;
- участие в разработке международных критериев, определяющих признаки террористических интернет-ресурсов;
- организация финансирования исследований, посвященных выявлению сегментов коммуникационной активности террористов в сети Интернет, и согласование государственных мер противодействия кибертерроризму в рамках отдельного международного документа.

Законодательный

На данном уровне необходимо внесение кибертерроризма в разряд уголовных преступлений и создание всеобъемлющей правовой базы для борьбы с этим явлением.

Можно выделить следующие основные направления работы на законодательном уровне:

- создание нормативной базы, которая будет обеспечивать защиту интересов личности, общества и государства в информационной сфере, в том числе путем установления ответственности провайдеров за

размещение сайтов организаций, официально признанных террористическими, или сайтов, содержащих пропаганду терроризма;

- продолжение работы в рамках международных организаций по унификации национальных законодательств в области борьбы с киберпреступностью и кибертерроризмом.

Организационный

Работа на этом уровне может развиваться в следующих направлениях:

- организация взаимодействия и координация усилий правоохранительных органов, спецслужб, судебной системы в области борьбы с кибертерроризмом, обеспечение их надлежащей материально-технической базой;
- создание национального подразделения по борьбе с кибертерроризмом, а также специального центра по оказанию помощи в нейтрализации последствий кибератак;
- расширение международного сотрудничества в сфере правовой взаимопомощи в области борьбы с кибертерроризмом.

Технический

На данном уровне необходима защита информационной среды от несанкционированных воздействий, осуществляемых посредством использования программно-технических средств.

Можно спрогнозировать следующие основные направления в этой работе:

- содействие государственных структур в разработке программно- аппаратных средств, обеспечивающих высокую степень защиты от кибератак;
- защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов

и вредоносных программ, несанкционированного использования радиочастот, радиоэлектронных атак;

- создание современных качественных технологий обнаружения и предотвращения сетевых атак, а также методов и средств нейтрализации криминальных и террористических воздействий на информационные ресурсы.

Следует признать справедливой следующую точку зрения: благодаря Интернету кибертеррористы могут оказывать на аудиторию серьезное информационно-психологическое воздействие, то есть инициировать «психологический терроризм». Например, с помощью социальных сетей кибертеррористы повышают уровень организации участников этой деятельности, распространяют различные тревожные слухи, сеют панику, вводят пользователей сетей в заблуждение. Также они систематически распространяют среди огромной аудитории информацию о технологии производства взрывчатых веществ и взрывных устройств, ядов и отравляющих газов.

Кибертеррористами часто используется замена содержания сайтов и других интернет-ресурсов, которая заключается в подмене электронных страниц или их отдельных элементов в результате взлома. Этот прием используется в основном для привлечения внимания, демонстрации своих возможностей и является противоправным способом выражения их политических целей и убеждений. Помимо прямой подмены страниц широко используется регистрация в поисковых системах сайтов террористического содержания, которые открываются по ключевым словам легальных сайтов, а также перенаправление (подмена) ссылок на другой адрес, что приводит к открытию специально подготовленных противостоящей стороной интернет-страниц [Новостные сообщения. Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 14.04.2017)].

По нашему мнению, для эффективной борьбы с кибертерроризмом в Российской Федерации необходимо разработать государственную программу развития информационно-коммуникационных технологий, обеспечивающих подключение корпоративных сетей к сети Интернет при соблюдении требований безопасности информационных ресурсов. Также необходимо принять меры по совершенствованию технологий своевременного обнаружения и пресечения попыток несанкционированного доступа к информации. Кроме этого, важно законодательно установить исчерпывающий перечень видов сведений, не подлежащих передаче по открытым сетям, и обеспечить контроль над соблюдением установленного статуса конфиденциальной информации.

При этом необходимо продолжать работу по упреждающему выявлению появляющихся новых факторов риска, по созданию и использованию опережающих технологий борьбы с кибертерроризмом.

Большое значение имеет организация системы подготовки и повышения квалификации специалистов по информационной безопасности. Кроме того, необходимо повышать правосознание людей, что позволит им, имея четкое понимание разумности подобных норм, оказывать всемерную помощь правоохранительным органам в выявлении случаев кибертерроризма уже на стадии подготовки преступлений, осуществляемых с использованием информационных систем.

Особую роль в борьбе с киберпреступниками играет осуществление переподготовки и регулярное повышение квалификации кадров, которые специализируются на борьбе с кибертерроризмом, их поиск из числа профессионалов только на конкурсной и контрактной основе. Такое обучение будет побуждать их постоянно самосовершенствоваться, чтобы эффективно противостоять новым видам сетевых атак и компьютерных преступлений.

При этом постоянное техническое и программное переоснащение служб и подразделений, занимающихся противодействием

кибертерроризму, должно стать регулярным, что станет одной из действенных гарантий информационной безопасности государства.

Еще одним важным направлением борьбы с использованием информационных технологий в террористических целях является их профилактика. Особенно важно проводить такую профилактическую работу в среде молодежи, так как именно молодежь в силу ряда психологических и иных факторов является наиболее уязвимой в плане подверженности негативному влиянию разнообразных криминальных групп. Социальная и материальная незащищенность молодежи, частый максимализм в оценках и суждениях, психологическая незрелость, значительная зависимость от чужого мнения, всеобщее увлечение информационно-коммуникационными технологиями, стремление повысить свою самооценку любыми способами, в том числе и противозаконными, такими, как хакерские атаки – это только некоторые из причин, позволяющие говорить о возможности легкого распространения радикальных идей среди российской молодежи и привлекательности кибертерроризма.

В связи с тем, что оружие киберпреступников постоянно совершенствуется, а способы информационных атак становятся все более универсальными и изощренными, в перспективе следует ожидать появления новых «нетрадиционных» видов кибератак и компьютерных преступлений. Однако целенаправленное комплексное решение перечисленных задач и выполнение профилактических мероприятий позволит эффективно противодействовать кибертерроризму, что существенно снизит вероятность реализации террористических угроз в киберпространстве.

Кроме перечисленных выше возможных **уровней развития ситуации по противодействию** с кибертерроризмом можно выделить сценарии, в которых могут быть задействованы не только силы РФ, но и мирового сообщества в целом, приведенные в таблице 4.

Сценарии развития ситуации по противодействию кибертерроризму

Таблица 4

Название	**Условия, при которых сценарий возможен**	**Последствия для основных и косвенных участников**	**Степень вероятности**
Подавление кибертеррористических атак посредством коалиции стран	Сплоченность государств в борьбе с киберпреступниками, и выполнение всех договоренностей.	Ослабление кибертеррористической структуры; Полное уничтожение организаций.	Вероятность полного уничтожения кибертеррористических организаций маловероятна, поскольку не сильна система противодействия, количество организаций ежегодно возрастает
Увеличение числа кибертеррористичесих организаций и информационных технологий	Не способность стран противостоять появлению новых группировок и распространения их в мире	Дестабилизация обстановки в мире; Дезинформирование мирового сообщества; Вербовка в террористические организации.	Вероятность высока, поскольку киберпреступники не остановятся пока не добьются своей цели-дестабилизировать положение всех стран.
Получение важной государственной информации	При создании новых технологий, вирусов, поспособствующих взлому баз данных государства и мирного населения	Изменение мирового порядка	Вероятность высока, поскольку число организаций растет, технологии развиваются, а политика противодействия борьбы не развита, нет четкой стратегии противостояния кибертерроризму.

Таким образом, можно сделать вывод, что проблему кибертерроризма нужно рассматривать как одну из опасных проблем современности, так как данная проблема затрагивает все сферы жизни общества. Для эффективной борьбы с кибертерроризмом необходим системный подход к организации антитеррористической деятельности на государственном уровне. Другие страны мира, так же как и Россия, стремятся решить главную задачу –

эффективно подавить кибертеррористическую деятельность и в процессе борьбы с ней обеспечить строгое соблюдение законности. Создание специальных международных организаций, направленных на борьбу на мировой арене, развитие специальных антикибертеррористических подразделений, которые должны выявлять киберпреступления на стадии возникновения, пресекать кибератаки на стадии планирования и подготовки, могут посодействовать созданию более спокойной обстановке в мире.

Сейчас сложно дать четкий прогноз того, по какому именно сценарию будут развиваться события. Это зависит в первую очередь от политики, которую выберут не только Российская Федерация, так и мировое сообщество в целом.

Заключение

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.

Проблема обеспечения безопасности компьютерной информации и технологий является сегодня одной из самых острых для большинства стран мира. В первую очередь это касается использования информационных систем и сетей в государственном управлении, военной и промышленной сферах, бизнесе. Разработка эффективной политики противодействия кибертерроризму ведется по следующим основным направлениям: определение приоритетных целей (глобальные, региональные, национальные) и средств (ресурсов), выявление возможных кибертеррористических угроз, защита населения, создание и координация международной инфраструктуры противодействия кибератакам, включающей в себя разработку специальных антитеррористических программ, норм международного права и др.

Механизмы политического регулирования в сфере государственной политики противодействия кибертерроризму предполагают учет таких факторов, как наличие у власти экономических, технических, правовых, организационных и иных ресурсов, которые необходимо задействовать в процессе реализации антитеррористических акций и программ, уровень

ответственности граждан, характер освещения данной проблемы в СМИ, последствий совершения кибератак, уровень использования других компьютерных сетей, анализ сайтов, состояние систем защиты собственных сетей, а также объектов повышенной опасности и др.

В противодействии кибертерроризму приоритетное значение должно принадлежать оперативному пресечению кибертеррористических атак на стадии их подготовки (анализ информации, разработка законов, контроль со стороны государства), а также проведению на постоянной основе мониторинга состояния информационно-коммуникационного пространства, донесению необходимой информации до населения, профилактической работе (воспитательная, правовая, организационная) и др. Перечисленные меры должны всегда находится в центре внимания федеральной и региональной власти. Пролонгация кибертеррористических атак в повседневную жизнедеятельность социума обусловила необходимость разработки различных программ и мероприятий по организации разнообразной помощи жителям, пострадавшим от кибертеррористических действий, минимизации наносимого ущерба.

Российская система обеспечения безопасности от угроз кибертерроризма должна представлять собой многоуровневую иерархическую, территориально распределенную систему, в функции которой должны входить: анализ существующей структуры национальной безопасности государственной информационно-коммуникационной инфраструктуры; создание единой, комплексной стратегически ориентированной государственной концепции борьбы с этим явлением; модернизация законодательства в сфере борьбы с терроризмом; взаимодействие всех сил правопорядка и спецслужб в антитеррористической борьбе с выделением головного органа, обладающего необходимыми полномочиями и правами в организации, координации и осуществлении всей борьбы с кибертерроризмом, и возложением на него ответственности за ее результативность.

В заключении необходимо отметить, что поставленная цель достигнута путем решения задач. Таким образом, повышение эффективности борьбы с кибертерроризмом возможно лишь путем принятия всесторонних мер, которые будут в себя включать: четкую и последовательную политику, высококвалифицированную разведку, повышение качества работ правоохранительных органов и вооруженных сил, решение кадрового вопроса в создании ответственной команды профессионалов, а также технические средства предотвращения техногенного и кибернетического террора.

Список использованных источников и литературы

Источники:

1. Государственные стратегии кибербезопасности URL: http://www.securitylab.ru/analytics/429498.php(Дата обращения 02.12.2016 г.)
2. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
3. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № ПР-1895.: URL: http://www.scrf.gov.ru/documents/S.html (дата обращения: 02.12.2016)
4. Закон РФ от 27 декабря 1991 г. N 2124-I «О средствах массовой информации» (с изм. и доп. от 13 января, 6 июня, 19 июля, 27 декабря 1995 г., 2 марта 1998 г., 20 июня, 5 августа 2000 г., 4 августа 2001 г., 21 марта, 25 июля 2002 г., 4 июля, 8 декабря 2003 г., 29 июня, 22 августа, 2 ноября 2004 г. , 21 июля 2005 г., 27 июля, 16 октября 2006 г., 24 июля 2007 г.) // «Российская газета» от 8 февраля 1992 г
5. Интервью с Андреем Крутским. [Электронный ресурс]. URL: http://www.kommersant.ru/Doc/2997208/ (дата обращения 04.12.2016).
6. Концепция противодействия терроризму в Российской Федерации. URL: http://www.rg.ru/2009/10/20/zakon-dok.html(дата обращения 12.04.16)
7. Концепция внешней политики Российской Федерации от 12 июля 2008 г. № ПР-1440. URL: Режим доступа: http://www.moluch.ru/archive/49/6159 (дата обращения: 02.12.2016)
8. Концепция национальной безопасности Российской Федерации от 10 января 2000 г. № 24.URL: http://w4vw.armscontrol.ra/start/rus/docs (дата обращения: 02.12.2016)
9. Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г.URL: http://ww.rg.ru/2009/10/20/ zakon-dok.html (дата обращения: 02.12.2016)

10. Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г.URL: http://www.rg.ru/2009/10/20/zakon-dok.html (дата обращения: 02.12.2016)

11. МИД РФ. Международная безопасность.2016.URL: http://www.mid.ru/ru/foreign_policy/international_safety/regprla(дата обращения 08.04.2017).

12. Новостные сообщения. URL: http://ria.ru/world/20160527/1439834739.html (дата обращения 04.12.2016).

13. Новостные сообщения. URL: http://ria.ru/society/20160603/1442531794.html/ (дата обращения 04.12.2016).

14. Принципы, касающиеся международной информационной безопасности, 12 мая 1999 года: [Подлинный текст на рус. яз.] // Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Доклад Генерального секретаря ООН: A/55/140 / Генеральная Ассамблея ООН: Пятьдесят пятая сессия. 2000. 10 июля.

15. Речь А. Крутских от 27.05.2016.URL: http://www.interfax.ru/russia/520709/ (дата обращения 01.12. 2016).

16. РИАНОВОСТИ. 2016. Россия противник США в киберпространстве.2016.URL: https://ria.ru/world/20161012/1479093276.html(дата обращения 21.05.17).

17. РИАНОВОСТИ.2016.Россия будет привержена борьбе с кибертерроризмом.URL: https://ria.ru/politics/20161012/1479037758.html(дата обращения 11.04.17).

18. РИАНОВОСТИ. Борьба с кибертерроризмом.2016.URL: https://ria.ru/world/20160728/1473086078.html(дата обращения: 12.11.16).

19. РИАНОВОСТИ. Кибертерроризм как оружие.2016.URL: https://ria.ru/analytics/20161108/1480900221.html(дата обращения 5.05.17).

20. Россия в глобальной политике. Электронный ресурс. URL:http://www.globalaffairs.ru/number/Igra-pro-pravila-17640 (дата обращения: 23.04.2017)

21. Стратегия развития информационного общества в Российской Федерации от 7 февраля 2008 г. N Пр-212.

22. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016). [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс»/ (дата обращения 02.12.2016).

23. Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации".URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения: 23.03.2017)

24. Федеральный закон «О борьбе с терроризмом» от 25 июля 1998 года N 130-ФЗ // СЗ РФ. 1998. N 31. Ст. 3808.

25. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // «Российская газета» от 29 июля 2006 г.

26. Федеральный закон от 6 марта 2006 года N 35-ФЗ «О противодействии терроризму» // СЗ РФ. 2006. N 11. Ст. 1146.

Литература:

27. Авцинова Г.И., Пахарева Е.Н. Политическое противодействие кибертерроризму в международном сообществе и в Российской Федерации: управленческий аспект // Научные публикации кафедры политологии и социальной политики РГСУ. Выпуск №1. – М., РГСУ, 2008. – с. 25-44

28. Ачкасов В.А., Ланцов С.А. Мировая политика и международные отношения: Учебник / М.: Аспект Пресс, 2011. 480с.

29. Багдасарян В.Э. Демографические тренды и национальная безопасность России // Мир и политика. 2010. − №7 (46)

30. Багдасарян В.Э. Научится мыслить в парадигме войн нового типа // Научный эксперт. 2011

31. Варданянц Г.К. Терроризм: диагностика и социальный контроль // Социс. 2005

32. Вартанова Е.Л. Современная медиаструктура. // СМИ в постсоветской России. − М., 2002; Гельман А. Русский способ (Терроризм и масс-медиа в третьем тысячелетии). − М., 2003

33. Васильева А.Н. Понятие и проблемы противодействия кибертерроризму // Успехи современного естествознания. – 2011. – № 8.

34. Волеводз А.Г. Конвенция о Киберпреступности: Новации Правового Регулирования // Правовые вопросы связи. 2007. № 2. С. 17–25.

35. Галатенко В.Н. Информационная безопасность: практический подход. − М., 1998.

36. Голубев В. А. Кибертерроризм — понятие, терминология, противодействие.URL: http://w\v\v.crimc-research.ni/articles/Golubev0804/ (дата обращения: 02.12.2016)

37. Голубев В. А. Кибертерроризм - угроза национальной безопасности.URL: http://www.crime-research.ru/articles/Golubev_Cyber_ (дата обращения: 01.12.2016)

38. Голубев В.А. Кибертерроризм как новая форма терроризма [электронный ресурс]. URL: http://www.crime-research.org/ (дата обращения: 27.03.2017);

39. Евдокимов А. Средства массовой информации в противодействии терроризму. // Мировое сообщество против глобализации преступности и терроризма. − М.: «Международные отношения», 2002

40. Еделев А. Л. Борьба с. экстремизмом: вопросы теории и практики. М. : АУ МВД России, 2005. 200 с.

41. Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения. Информационное право, 2013. № 5. С.10-13.

42. Зубков В.А., Осипов С.К. Российская Федерация в международной системе противодействия легализации (отмыванию) преступных доходов и финансированию терроризма: монография. – М.: Городец, 2006. С. 88-89.

43.

44. Иванов С.М. Международно-правовое регулирование борьбы с кибертерроризмом, 2013. Режим доступа: http://elibrary.ru/item.asp?id=22545981 (дата обращения: 02.12.2016)

45. Информационно-психологические аспекты государственного и муниципального управления / В.Г. Кулаков, А.К. Соловьев, В.Г. Кобяшев, А.Б. Андреев, С.В. Скрыль, О.А. Остапенко [и др.]. – Воронеж: Воронежский институт МВД России, 2002. – 52 с.

46. Колобов О.А, Ясенев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решений. − Н. Новгород, 2001

47. Конявский В.А., Лопаткин С.В. Компьютерная преступность. Т.I. − М., 2006

48. Курбацкий А.Н. Роль СМИ в борьбе с международным терроризмом [электронный ресурс]. URL: http://www.economy.bsu.by/library.pdf (дата обращения:18.04.2017)

49. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. − СПб., 2000

50. Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства [электронный ресурс]. URL: http://www.crime-research.ru/analytics/malishenko (дата обращения: 05.03.2017)

51. Международный терроризм: борьба за геополитическое господство: Монография.-М.: Изд-во РАГС, 2005.- 528 С.

52. Мирошников Б.Н. Борьба с киберпреступлениями одна из составляющих информационной безопасности Российской Федерации

[электронный ресурс] / Б.Н. Мирошников. URL: http//www.crimeresearch.ru/articles/Mirosh1 (дата обращения: 16.04.2017)

53. Морозов И.Л. Пределы информационной свободы в российском киберпространстве: как смягчить столкновение интересов государства, гражданского общества, независимой науки? [электронный ресурс]. URL: http://morozov.vlz.ru/library/infsvob.htm (дата обращения 16.04.2017)

54. Назаров М.М. Массовая коммуникация в современном мире: методология анализа и практика исследований. − М., 2003

55. Национальная безопасность: научное и государственное управленческое содержание. Под ред. Сулакшин С. С.,Соловьев А. И.,Багдасарян В. Э.,Вилисов М. В.,Зачесова Ю. А.,Мешков Ю. Е. – М. 2009, 424 С.

56. Нерсесян В. Национальная безопасность и формирование информационного общества в России // Власть. 2003. − №9

57. Панарин И.Н. СМИ и терроризм [электронный ресурс]. URL: http://www.panarin.com (дата обращения: 18.04.2017)

58. Паненков А. А. Кибертерроризм как реальная угроза национальной безопасности России. Право и кибербезопасность, 2014. № 1. С. 12-19.

59. Пахарева Е.Н. Политика противодействия кибертерроризму как задача международной политики государства // Научные исследования кафедры политологии и социальной политики РГСУ. Сборник научных трудов. Выпуск 3. / Отв. ред. Г.И. Авцинова. М.:РГСУ, АПКиППРО, 2010. 172 с.

60. Пахарева Е.Н. Влияние кибертерроризма на молодежную среду: особенности и тенденции развития // Ученые записки Российского государственного социального университета. − М.: РГСУ, 2011. − №2 с. 51-56

61. Пахарева Е.Н. Защита пользователей от распространения контента террористического характера в сети интернет: политологический аспект

проблемы // Социальная политика и социология: междисциплинарный научно-практический журнал. − М.: РГСУ, 2010. − №2(56). с. 80-94.

62. Пахарева Е.Н. Кибертерроризм как технология воздействия намолодежную среду: причины и пути минимизации // Ученые записки Российского государственного социального университета. − М.: РГСУ, 2009. − №4 (67). с. 77-81

63. Пахарева Е.Н. Угрозы кибертерроризма в современном информационном обществе // Инновационные подходы в исследованиях молодых ученых: Материалы выступлений на Аспирантских чтениях 20 апреля 2010 года/ под ред. А.В. Гапоненко. – М.: АПКиППРО, 2010. 480с.

64. Роговский Е.А. Кибербезопасность и кибертерроризм // США – Канада. Экономика, политика, культура. 2003, − №8

65. Саитов И.А. Противодействие кибертерроризму – важнейшая задача обеспечения информационной безопасности / И.А. Саитов, А.Е. Миронов, А.В. Королёв // Вестник национального антитеррористического комитета. – 2012. – № 2 (07). – С. 72–79.

66. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики : дис. … канд. юрид. наук. Иркутск, 2006. С. 109–112.

67. Старостина Е.В., Фролов Д.Б. Защита от компьютерных преступлений и кибертерроризма. − М.: 2005

68. Сулакшин С.С. Категория «безопасность»: от категориального смысла до государственного управления // Научный эксперт. 2010

69. Сулакшин С.С. Национальная безопасность страны и качество национального образования // Родная Ладога. 2010. − №4

70. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера : дис. … канд. юрид. наук. Красноярск, 2010. 210 с.

71. Торкунов А., Мальгин А. Современные международные отношения: учебное пособие. М.: Аспект Пресс, 2012. 688 с.

72. Тропина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате. Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. Киев: Национальная академия наук Украины, 2003. С. 173-181.

73. Тропина Т.Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : монография. Владивосток, 2009. 237 с.

74. Тропина Т. Л. Киберпреступность и кибертерроризм [электронный ресурс]. URL: http://www.crimeresearch.ru/analytics/ (дата обращения: 05.03.2017).

75. Усилинский Ф. А. Кибертерроризм в России: его свойства и особенности. Право и кибербезопасность, 2014. № 1. С. 6-11.

76. Уфимцев Ю.С., Ерофеев Е.А. и др. Информационная безопасность России. − М., 2003

77. Хмылёв В. Л. Современные международные отношения: учебное пособие. 2010. URL: http://window.edu.ru/resource/136/ 71136/files.pdf (дата обращения: 11.06.2014).

78. Цыганков П. А. Международные отношения: Учебное пособие. М.: Новая школа, 1996. 320 с.

79. Цыганков П. А. Теории международных отношений. М.: Гардарики, 2003. 590 с.

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

81. Шагинян Г.А. Антитеррористическая информационная политика Российского государства: автореф. дис. … канд. полит. наук. – Краснодар: ГОУ ВПО «Кубанский государственный университет», 2006.

82. Шерстюк В.П. Проблемы правового обеспечения информационной безопасности в Российской Федерации // Право-Информация- Безопасность. Альманах российского юридического журнала. 2002. − №1

83. Юркин И. 3. Кибертерроризм: вызов XXI века // Газета Исполнительного комитета СНГ «Республика». 2007. 5 аир. С. 11-12.

84. Biernatzki W. E. Terrorism and Mass Media. // Center for the Study of Communication and Culture. − London. 2002. Vol. 21. − N.1

85. Cohen F. Terrorism and Cyberspace // Network Security, 2002, Vol.5; Convey M. Terrorist use of Internet and Fighting Back // Materials of the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. Oxford, 2005

86. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks/ P. Cornish; Directorate-General for External Policies of the Union, Policy Department. - Brussels : European Parliament, 2009. - 34 p.

87. Cyber Security Strategy for Germany URL: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (дата обращения 02.14.2017 г.)

88. Fowler, R. Language in the News: Discourse and Ideology in the Press / R. Fowler. -L.; N.Y.: Routledge, 1991. 184 p.

89. Goffman, E. Frame Analysis: An Essay on the Organization of Experience / E. Goffman. New York: Harper and Row, 1974. - P. 575.

90. Grunebaum, von G. E. The Search for Cultural Identity / von G. E. Grunebaum. N. Y., 1962. - P. 40.

91. Heit, G. Neural Encoding of Individual Words and, Faces by the Human Hippocampus and Amygdala / G. Heit, M. Smith, E. Halgren // Nature. -1988. Vol. 333, no. 6175. - P: 773-775.

92. Laqueur, Walter. Interpretations of Terrorism Fact, Fiction and Political Science / W. Laqueur // Journal of Contemporary History. January 1977. — P.3.

93. Lewis, P. Alternative media in a'contemporary social and theoretical context / P. Lewis // Alternative Media: Linking Global and Local / Unesco Paris, 1993.-P. 12.

94. Martin L.J. The Media’s Role in international Terrorism [электронный ресурс]. URL: http://www.pegasus.cc.ucf.edu~surette/mediasrole.html (дата обращения: 18.04.2017)

95. Pollitt M., CYBERTERRORISM – Fact or Fancy? FBI Laboratory [электронный ресурс]. URL: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (дата обращения 08.04.2017)

96. Weimann, G. How Modern Terrorism Uses the Internet. Release Date: March 2004 No. 116 [электронный ресурс]. URL: http://www.usip.org/pubs/specialreports/srl16.html (дата обращения: 08.04.2017)

97. Wilkinson P. The Media and Terrorism: A Reassessment. // Terrorism and Political Violence. − London. 2001. Vol. 9. − N.2.

98. Wilson C. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress [электронный ресурс]. URL: http://www.fas.org/sgp/crs/terror/index.html (дата обращения: 08.04.2017).

Приложения

Приложение 1

Контент – анализ публикаций по теме: «Кибертерроризм и противодействие ему» за период 2014- 2017 гг.

Сведения об авторе статьи	**Название статьи, выходные данные**	**Оценка эффективности противодействия кибертерроризму**
Демидов Олег, *консультант ПИР-Центра* Черненко Елена, *кандидат исторических наук, руководитель международного отдела газеты «*Коммерсантъ»	Игра про правила // Россия в глобальной политике, № 4, 2015	- Невозможность сдвинуть диалог о глобальном договоре по киберпространству с мертвой точки, вероятно, способствовала тому, что за прошедшие годы российская позиция по этому вопросу стала более гибкой, а «тактика малых шагов» более не рассматривается как уступка западному подходу. - Впрочем, «малые шаги» на пути к выработке правил поведения государств в киберпространстве не ограничены лишь соглашениями, затрагивающими банковский сектор. Уже некоторое время параллельно обсуждается идея активизации международного сотрудничества в обеспечении кибербезопасности объектов мирной атомной индустрии. Дискуссия о востребованности новых международных, в том числе международно-правовых инструментов для борьбы с киберугрозами ядерным объектам, конечно же, получила начальный импульс после обнаружения в 2010 г. вируса Stuxnet и продолжает набирать обороты. - Вопрос о необходимости создания правил поведения в киберпространстве именно вокруг глобальной инфраструктуры

		интернета уже активно обсуждается в экспертном и техническом сообществе. Ничто не мешает России включить их в свой спектр инициатив и подходов к выстраиванию режима ответственного поведения государств в информационном пространстве. Наряду с защитой банков и объектов атомной отрасли от кибератак одобрение такой инициативы полностью соответствовало бы российским национальным интересам и стало бы шагом вперед в международном сотрудничестве в сфере кибербезопасности.
Диденко Александр, *Дальневосточный федеральный университет, г. Владивосток*	Режим доступа: http://elibrary.ru/download/elibrary_27346057_26941964.pdf	- Определенная обеспокоенность угрозой кибертерроризма возникает у президента РФ. Еще в 2006 году президент РФ Путин В. В., выступая в Москве на конференции генеральных прокуроров европейских стран, предложил разработать глобальную стратегию по борьбе с кибертерроризмом . В 2009 году появляется утвержденная президентом РФ «Концепции противодействия терроризму в Российской Федерации».
Касперский Евгений	Режим доступа: http://www.interface.ru/home.asp?artId=38057	- Раньше все было просто. Вот Windows, у которого есть домашняя версия и корпоративная версия. Это было в эпоху становления киберпреступности. Потом появились шпионские атаки, потом усложнились криминальные атаки, потом прибежала традиционная преступность и начала атаковать SCADA-системы. Например, была такая история: латиноамериканские наркоторговцы стали пересылать наркотики морскими контейнерами. Открывают, догружают его. На том берегу открывают, разгружают. Морским портом Антверпен управляет автоматическая SCADA-система, людей там нет. С корабля снимают

		базу данных контейнеров - и за два часа их выгружают. И вот эту систему взломали наркокартели: они научились отдельно разгружать контейнеры с кокаином. Еще уголь с шахт воруют. На Украине зерно с элеваторов: тонну приняли, тонну отгрузили. А на самом деле не тонну они отгрузили (смеется). Поменялся пейзаж, и это меняет и нашу индустрию. Если у нас раньше было две категории продуктов - домашние и корпоративные, то теперь появилась третья: защита индустриальных систем. - Судя по сообщениям СМИ, ИГИЛ (запрещенная в России организация) крайне активно в социальных сетях, и в первую очередь они используют интернет для коммуникации, вербовки сторонников и т. д. У нас нет никакой достоверной информации о каких-то хакерских группах, действующих в интересах ИГИЛ. Я читал в СМИ про «кибер-халифат», что ИГИЛ рекрутирует хакеров, но пока о возможностях этой террористической организации в киберсфере судить трудно. Однако потенциально ИГИЛ - это очень серьезная угроза и в интернете тоже. Продвинутые технологии взлома компьютеров и сетей доступны на черном рынке, и из рук криминала они вполне могут попасть в руки террористов. Вероятно, существуют хакерские группы наемников, атакующие цели под заказ. Угроза кибертерроризма - это, к сожалению, сегодня печальная реальность. И самый кошмарный сценарий - это возможная террористическая атака на критическую инфраструктуру.
Васильев Кирилл	Молодой учёный №17 (97) сентябрь-1 2015 г.	- Наибольшее количество исследований, посвященных кибертерроризму, проводится в Соединенных Штатах Америки, что

		напрямую связано с обширной правовой базой, регламентирующей процесс обеспечения информационной безопасности, где рассматриваемое явление отнесено к угрозам военно-политического характера, которые проявляются во враждебном использовании информационно-коммуникационных технологий для достижения политических, экономических, военных целей. - противодействие кибертерроризму должно стать одной из приоритетных задач в борьбе с преступностью в России. При этом следует исходить из дифференцированного понятия кибертерроризма, включающего в себя совершение атак на телекоммуникационные, компьютерные сети и средства связи (технический аспект) и информационно-психологическое воздействие с использованием подконтрольных террористам СМИ. Поставленная проблема актуализирует проведение широкомасштабных научных исследований с целью выявления отдельных факторов пропагандистского воздействия кибертеррористов и восприимчивости аудитории. Весьма показательным в этом отношении является опыт Германии и Голландии. Учитывая трансграничный характер кибертерроризма, чрезвычайно важно международное сотрудничество в сфере противодействия ему, содействующее выработке взаимосогласованных решений и единого понятийного аппарата.
Голубев Владимир, Доктор юридических наук	Кибертерроризм как новая форма терроризма Режим доступа: http://www.crime-	В качестве рекомендаций, направленных на противодействие опасным тенденциям и повышение эффективности борьбы с кибертерроризмом, предлагаем следующее:

	research.ru/library/Gol_tem3.htm	1. Организация эффективного сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, а также международными организациями, в задачу которых входит борьба с кибертерроризмом и транснациональной компьютерной преступностью. 2. Создание национального подразделения по борьбе с киберпреступностью и международного контактного пункта по оказанию помощи при реагировании на транснациональные компьютерные инциденты. 3. Расширение трансграничного сотрудничества в сфере правовой помощи в деле борьбы с компьютерной преступностью и кибертерроризмом. 4. Принятие всеобъемлющих законов об электронной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы о борьбе с киберпреступностью.
Шерстюк Владислав, *директор Института проблем информационной безопасности МГУ имени М.В. Ломоносова*	Киберпреступность – самая опасная угроза информационной безопасности Режим доступа: https://ria.ru /world/20150422/933965574.html	- Важно противодействовать угрозам превращения интернета в театр военных действий или идеологических сражений и обеспечить информационную безопасность каждого государства мира; - Сформировалось общее понимание того, что наиболее опасными угрозами международной информационной безопасности на данном этапе являются продолжающийся рост масштабов компьютерной преступности, подготовка и осуществление актов компьютерного терроризма, а также использование информационных и коммуникационных технологий для "силового" разрешения

		межгосударственных противоречий; - Актуальность проблемы обусловлена потребностью общества в нейтрализации негативных последствий злоупотребления свободой информации во вред общественной нравственности и социальной стабильности. Реальная практика современной жизни такова, что в той или иной степени механизмы фильтрации интернет-контента используются многими государствами мира, в том числе и теми, которые относят себя к демократическим;
Дубов Дмитрий, *заведующий отделом исследований информационного общества и информационных стратегий Национального института стратегических исследований при Президенте Украины*	Киберпреступность – угроза для бизнеса Режим доступа: http://internetua.com/kiberprestupnost---ugroza-dla-biznesa	Сегодня киберпространство, это «Дикий Запад». В нем царит тотальное беззаконие. Как и любое другое пространство, киберсреда постепенно превращается в поле битвы различных интересов, представленных в форме государств, глобальных корпораций и пр. Пока, от массовых кибератак Украину защищает не соответствующий мировым темпам, уровень информатизации. Но мы уже сегодня дожны задуматься над тем, как защитить государство и бизнес от киберугроз мирового масштаба.