УДК 323.28:004.056.52(47)
ББК Ф2(2Рос)+Ф4(2Рос),304.1

ГСНТИ 81.93.25
Код ВАК 22.00.04

Прокопьева В. А.
Екатеринбург

ПОЛИТИКА ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В СОВРЕМЕННОЙ РОССИИ

Ключевые слова: национальная безопасность; терроризм; кибертерроризм; киберпреступность; информационное общество; информационные технологии.

Аннотация. В статье анализируется кибертерроризм как угроза национальной безопасности Российской Федерации, причины его возникновения, нормативно-правовое обеспечение противодействия кибертерроризму в России. Особое внимание обращено на пути совершенствования мер противодействия кибертерроризму в современной России.

Prokop'eva V. A.
Ekaterinburg

THE POLICY OF COUNTERACTING CYBERTERRORISM IN MODERN RUSSIA

Keywords: national security; terrorism; cyberterrorism; cybercrime; information community; information technologies.

Abstract. The article analyzes cyberterrorism as a threat to the national security of the Russian Federation, looks at the causes of its emergence and the laws and regulations to counteract cyberterrorism in Russia. Special attention is paid to the ways of improvement of the measures to counter cyberterrorism in modern Russia.

Во все времена обеспечение безопасности являлось одной из важнейших функций государства. Безопасность является важнейшей целью и фундаментальной потребностью, как отдельного человека, так и различных сообществ людей. В настоящее время кибертерроризм является серьезной угрозой для мировой безопасности.

Кибертерроризм приобрел глобальный размах, охватывая при этом многие страны мира. 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 информационных технологий, 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.

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.

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

На сегодняшний день, в общем, 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». 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.

М. А. Залиханов определяет терроризм как 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.

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.

По мнению А. Паненкова, 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 [8].

Попытки 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.

Кл. Вилскон под кибертерроризмом понимает 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 [12, с. 173–181].

Таким образом, исходя из основных понятий кибертерроризма, можно вывести следующее обобщенное определение. 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 [17, с. 11–12].

Цель кибертерроризма – 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 [12, 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

Согласно версии «Monterey» можно выделить три уровня кибертерроризма [16]:

1. Простой – неструктурированный

Использование хаков (взлом) 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 определенной 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 выделяются следующие причины возникновения кибертерроризма: политические, социальные, 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 [2].

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 продолжающийся экономический и энергетический кризис, рост цен, инфляции и безработицы [17, с. 11–12].

В обобщенном виде причины представлены в табл.

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

Таблица

Фактор	Суть
Внешнеполитический	рост числа кибертеррористических проявлений в ближнем и дальнем зарубежье; распространение идей терроризма и экстремизма через информационно-телекоммуникационную сеть; агрессивная политика в отношении другого государства и его оккупация; столкновение политических интересов различных государств
Внутренний	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
Экономический	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	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	вербование новых лиц для террористической деятельности

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.

В подтверждение выше сказанному, стоит отметить хронологию случаев наиболее крупных действий кибертеррористов, направленных на приостановку работы российских банков и финансовых организаций за последние три года.

• 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 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-банкинга 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 [21].

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 [21].

• 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 [21].

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.

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.

С начала 2000-х гг. Российская Федерация принимает активное участие в разработке международных и национальных правовых 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.

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 г.

• 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».

• Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г.

• Указ Президента России 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

В 2013 г. Президент РФ В. В. Путин 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 дипломатиче-

ских 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. Противодействие мошенническим действиям с использованием возможностей электронных платежных систем.

3. Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет.

4. Выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи; Интернет.

5. Противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

6. Борьба с международными преступлениями в сфере информационных технологий. Следует отметить, что общество также оценивает политику России по данному вопросу как не эффективную. В Российской Федерации пока должного внимания указанной выше проблеме не уделяется. Термин кибертерроризм легально не закреплен ни в одном нормативно-правовом акте [10, с. 65].

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.

Противостоять компьютерному терроризму, дополняющему обычный терроризм, в настоящее время практически невозможно. 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.

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, поджога и т. д.), а удаленно и через киберпространство. Кибертеррорист может находиться даже на территории другого государства.

Проанализировав конкретные меры противодействия кибертерроризму и деятельность соответствующих государственных структур, мы приходим к выводу, что в Российской Федерации системного противодействия кибертерроризму не ведется. Существуют разрозненные попытки осуществлять борьбу с данным проявлением терроризма. Отсутствует необходимая нормативно-правовая база. При этом для эффективного противодействия кибертерроризму необходимы совместные усилия всех членов мирового сообщества.

Исходя из характера и особенностей актов кибертерроризма, можно спрогнозировать следующие возможные пути развития ситуации по борьбе с ним.

Научный. Такой путь развития 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;

• 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. Работа в данном пути развития предусматривает 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 в данном пути развития может проходить в таких 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 пути развития необходима защита информационной среды от несанкционированных воздействий, осуществляемых посредством использования программно-технических средств.

Можно спрогнозировать следующие основные направления:

• содействие государственных структур в разработке программно-аппаратных средств, защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ,

• создание современных качественных технологий обнаружения и предотвращения сетевых атак.

По нашему мнению, для эффективной борьбы с кибертерроризмом в Российской Федерации необходимо разработать государственную программу развития информационно-коммуникационных технологий, обеспечивающую 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 переподготовка 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 крими-

нальных 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.

Библиографический список

1. Багдасарян, В. Э. Демографические тренды и национальная безопасность России / В. Э. Багдасарян // Мир и политика. – 2010. – № 7 (46).
2. Голубев, В. А. Кибертерроризм – угроза национальной безопасности [Электронный ресурс] / А. А. Голубев. – Режим доступа: www.crime-research.ru/articles/Golubev_Cyber_ (дата обращения: 01.12.2016).
3. Ефремова, М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения / М. А. Ефремова // Информационное право. – 2013. – № 5. – С. 10–13.
4. Иванов, С. М. Международно-правовое регулирование борьбы с кибертерроризмом [Электронный ресурс] / С. М. Иванов. – 2013. – Режим доступа: http://elibrary.ru/item.asp?id=22545981 (дата обращения: 02.12.2016).
5. Концепция противодействия терроризму в Российской Федерации от 20 октября 2009 г. [Электронный ресурс]. – Режим доступа: www.rg.ru/2009/10/20/ zakon-dok.html (дата обращения: 02.12.2016).
6. Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин. – СПб., 2000.
7. Нерсесян, В. Национальная безопасность и формирование информационного общества в России / В. Нерсесян // Власть. – 2003. – № 9.
8. Паненков, А. А. Кибертерроризм как реальная угроза национальной безопасности России / А. А. Паненков // Право и кибербезопасность. – 2014. – № 1. – С. 12–19.
9. Пахарева, Е. Н. Влияние кибертерроризма на молодежную среду: особенности и тенденции развития / Е. Н. Пахарева // Ученые записки Российского государственного социального университета. – 2011. – № 2. – С. 51–56.
10. Роговский, Е. А. Кибербезопасность и кибертерроризм / Е. А. Роговский // США – Канада. Экономика, политика, культура. – 2003. – № 8.
11. Торкунов, А. Современные международные отношения : учебное пособие / А. Торкунов, А. Мальгин. – М. : Аспект Пресс, 2012. – 688 с.
12. Тропина, Т. Л. Киберпреступность. Понятие, состояние, уголовно-правовые меры борьбы : моногр. / Т. Л. Тропина. – Владивосток, 2009. – 237 с.
13. Усилинский, Ф. А. Кибертерроризм в России: его свойства и особенности / Ф. А. Усилинский // Право и кибербезопасность. – 2014. – № 1. – С. 6–11.
14. Федеральный закон «О борьбе с терроризмом» от 25 июля 1998 г. № 130-ФЗ // СЗ РФ. – 1998. – № 31. – Ст. 3808.
15. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. –2006. –29 июля.
16. Цыгичко, В. Н. Информационное оружие – новый вызов информационной безопасности / В. Н. Цыгичко, Д. С. Вотрин, А. В. Крутских [и др.]. – М., 2000.
17. Юркин, И. З. Кибертерроризм: вызов XXI века / И. З. Юркин // Газета Исполнительного комитета СНГ «Республика». – 2007. – 5 апр. – С. 11–12.
18. Cohen, F. Terrorism and Cyberspace / F. Cohen // Network Security. – 2002. – Vol. 5.
19. Convey, M. Terrorist use of Internet and Fighting Back / M. Convey // Materials of the conference Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities. – Oxford, 2005.
20. 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.
21. Новостные сообщения [Электронный ресурс]. – Режим доступа: http://ria.ru/society/20160603/1442531794.html/ (дата обращения: 04.12.2016).

Статью рекомендует Ю. Р. Тагильцева, кандидат филологических наук, доцент