ГЛАВА 1

КИБЕРПРЕСТУПНОСТЬ И КИБЕРТЕРРОРИЗМ

Рассмотрены проблемы, связанные с киберпреступностью и кибертерроризмом. Приведена краткая история кибертерроризма, основные термины и определения, рассмотрены основные способы реализации кибертеракт, основные направления развития, в том числе – особенности кибертерроризма как формы гибридной войны, взаимосвязь кибертерроризма и политического терроризма.

Здесь же рассмотрена и категория «киберпреступность» – приведена классификация типов киберпреступлений, принятая Конвенцией Совета Европы, рассмотрены основные виды киберпреступлений и классификация арсенала используемого киберпреступниками кибероружия, основные стандарты кибербезопасности в этой области. Кратко проанализированы особенности организации структуры и функционирования систем киберзащиты НАТО, в том числе – перечислены основные оперативные киберструктуры НАТО. Приведен с авторскими комментариями детализированный алгоритм реализации типовой кибератаки.

Завершает главу раздел, посвященный «тонкостям профессий» заливщиков, ботоводов, рефоводов и прочих разновидностей кибермошенников – основные методы, способы и средства их детальности, а также рекомендации – как защититься от этих «профессионалов». Приведены примеры такого явления, как «технический симбиоз» киберпреступников и представителей государственных спецслужб.

1.1. Кибертерроризм

1.1.1. Кибертерроризм – определение, способы реализации кибертеракт

В этом разделе, основываясь на работе [1], попробуем дать определения и общие характеристики понятиям ***«киберпреступность»*** и ***«кибертерроризм»***, выделить основные разновидности киберпреступлений и кибертерроризма, кратко описать историю кибертерроризма и попытаться определить основные проблемы борьбы с киберпреступностью и кибертерроризмом.

Развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу электронно-вычислительных машин, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасным социальным явлениям, получившим распространенное название – «киберпреступность» и «кибертерроризм».

Кибертерроризм можно отнести к так называемым ***технологическим*** видам терроризма. В отличие от традиционного, этот вид терроризма использует в террористических акциях новейшие достижения науки и техники в области компью-

терных и информационных технологий, радиоэлектроники, генной инженерии, иммунологии. (Б. Колин ввел этот термин в научный оборот в середине 1980-х гг.)

Основные способы, с помощью которых террористические группы используют Интернет в своих целях:

1. *Создание сайтов* с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени встречи людей, заинтересованных в поддержке террористов.
2. Размещение в Интернете *сайтов террористической направленности*, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также инструкции по их самостоятельному изготовлению. Только в русскоязычном Интернете десятки сайтов, на которых можно легко найти подобные сведения.
3. *Сбор денег* для поддержки террористических и экстремистских движений.
4. Использование Интернета для *обращения к массовой аудитории* для сообщения о будущих или уже спланированных действиях на страницах сайтов или рассылка подобных сообщений по электронной почте.
5. *Вымогательство* денег у финансовых институтов (банков, корпораций) с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
6. Использование Интернета для *информационно-психологического воздействия* на гражданское население и властные структуры.
7. *Вовлечение* в террористическую деятельность ничего не подозревающих соучастников – например, хакеров, которым неизвестно, к какой конечной цели приведут их действия.
8. Использование возможностей электронной почты или электронных досок объявлений *для отправки зашифрованных сообщений* сообщникам.

Как правило, для террористических организаций вроде Аль-Каиды или ИГИЛ Интернет – это прежде всего *место распространения идей, вербовки новых членов и инструмент коммуникации*. Реально за время существования термина «кибертерроризм», а он существует с 80-х годов прошлого века, мир не увидел ни одного достаточно серьезного кибертеракта. Надо сказать, что хотя современные СМИ регулярно сообщают о том, что организация ИГИЛ активно развивает это направление и IT-бойцы халифата готовы наводить ужас на мировую общественность, но получается пока довольно посредственно.

Основная причина этого, по мнению экспертов, – низкий уровень «компьютерной» квалификации специалистов, которыми располагают террористические организации. Им намного проще собрать какую-нибудь бомбу (взрывное устройство) и взорвать, например, с ее помощью самолет, чем взломать электронную систему безопасности этого самолета и устроить авиакатастрофу. Да, ими были взломаны некоторые сайты, например – сайт полиции города Принс-Альберт (Канада). Но здесь большая часть атак осуществлялась *мусульманскими* хакерами, непосредственно никак не связанными с терроризмом вообще и с ИГИЛ в частности. Никаких серьезных последствий это не повлекло. Как обычно в этих случаях, хакерами оставлялись различные «послания», в основном антиизраильские или послания в поддержку ИГИЛ.

Однако отсутствие *совершенных* крупных кибертерактов совсем не означает отсутствие подобного *риска*. Представитель Министерства внутренней безопасности США на одной из ежегодных специализированных конференций ***CyberSat*** рассказал об успешной *реальной* атаке на самолет Boeing 757. И это был не лабораторный опыт, это был самый обычный аэропорт и самый настоящий самолет. А трагедия не произошла лишь потому, что «взломом» занимались эксперты в области безопасности, а не кибертеррористы.

Данная атака не позволяла угнать самолет и управлять им, хотя и это вполне реально при условии высокой квалификации хакеров. Но она позволяет организовать реальную авиакатастрофу при взлете самолета. Это, к сожалению, не шутки и не «теоретические размышления». Помимо самолета, целью может стать ваш автомобиль. Да, мы уверенно идем к эпохе полного автопилота: современные автомобили могут брать на себя функции управления в помощь водителю. И к сожалению, их можно взломать, как было показано в нашей книге (Белоус А.И., Солодуха В.А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – М., Вологда: Инфра-Инженерия, 2020) – в этой книге мы показали как минимум 12 возможных направлений кибератак на бортовые системы управления – от систем управления тормозами и рулевым устройством до электронной системы управления двигателем.

К сожалению, взломы автомобилей – это реальность, и не надо думать, что данная опасность угрожает только самым последним моделям автомобилей вроде Tesla. Конкретный пример – в 2015 году *под отзыв* попали 1,4 миллиона автомобилей марок Jeep, Dodge, Chrysler и Ram. Этот отзыв был вызван обнаруженной «белыми хакерами» уязвимостью в «штатной» мультимедийной системе ***Uconnect***, эксплуатируя которую, злоумышленники получали реальную возможность дистанционно управлять автомобилем. Специалисты по кибербезопасности из Uber Advanced Technology демонстративно «взломали» ***Jeep Cherokee*** 2014 года выпуска и отправили его в кювет – на сайте [book.cyberyozh.com/ru/kibervojna-kiberdiversii-i-kiberterrorizm/] читатели сами могут посмотреть *видеодоказательство* этого эпизода.

1.1.2. Краткая история кибертерроризма

- ***1970-е – начало 1980-х гг.*** – зарождение кибертерроризма;
- ***1983 г.*** – в США была арестована первая группа хакеров под названием «банда 414»;
- ***1993 г.*** – в Лондоне в адрес целого ряда брокерских контор, банков и фирм поступили требования выплатить по 10–12 млн ф. ст. отступных неким злоумышленникам;
- ***1996 г.*** – представители террористической организации «Тигры освобождения Тамил-Илама» провели сетевую атаку, направленную против дипломатических представительств Шри-Ланки;
- ***сентябрь 1997 г.*** – в результате действий неустановленного хакера была прервана передача медицинских данных между наземной станцией НАСА и космическим кораблем «Атлантис»;
- ***январь 1999 г.*** – появление в Интернете первого вируса под названием «Хеппи-99»;

- ***1 мая 2000 г.*** – из пригорода Манилы был запущен в Интернет компьютерный вирус «Я тебя люблю»;
- ***август 1999 г.*** – была развернута широкомасштабная кампания компьютерных атак Китая и Тайваня друг против друга. Кибертеррористы атаковали порталы государственных учреждений, финансовых компаний, газет, университетов;
- ***11 сентября 2001 г.*** – террористический акт против США (по версии спецслужб США);
- ***2004 г.*** – электронные ресурсы правительства Южной Кореи подверглись массированной атаке – вирусом оказались заражены десятки компьютеров, в частности министерства обороны Южной Кореи;
- с ***2005 г. по настоящее время*** в мире ежегодно фиксируется миллионы компьютерных нападений на информационные ресурсы органов государственной власти, банков и крупных компаний.

1.1.3. Основные направления кибертерроризма

Рассмотрим наиболее уязвимые направления, по которым кибертеррористы наносят (или могут нанести) удар. Так, современный *виртуальный терроризм* проявляется в следующих направлениях:

- нанесение материального и экономического урона путем взлома системы безопасности, нарушения работы или полного отключения средств коммуникации, снабжения, общественного транспорта и военных объектов;
- оказание психологического воздействия на широкие массы населения с целью дестабилизации ситуации и распространения хаоса;
- оказание психофизиологического воздействия на отдельные социальные группы, а также людей, задействованных в информационной сфере;
- предоставление провокационной дезинформации с целью нарушения баланса сил на международной арене, разжигания военных, межнациональных и религиозных конфликтов;
- агитация и пропаганда идей радикального и экстремистского толка, вербовка новых членов в действующие террористические организации;
- дезинформация правоохранительных органов конкретного государства о якобы заложенных на его территории взрывных устройствах, готовящихся актах терроризма и т.п.;
- оказание воздействия на принятие решений органами власти путем угрозы совершения террористического акта;
- раскрытие и угрозу опубликования (или опубликование) закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.

Рассмотрим подробнее основные из этих рисков (направлений). Работа современных логистических систем, средств жизнеобеспечения крупных городов, инфраструктуры и коммуникации немыслима без сети Интернет. Эпоха механического управления, основанного на ответственной работе конкретного человека, уходит

в прошлое. Общество уже давно делегировало автоматизированным цифровым электронным системам управления многие полномочия и лишь следит за качеством их работы. Без сети Интернет и соответствующего программного обеспечения современный урбанизированный мир просто немыслим. Упрощая свою жизнь, активно внедряя цифровые технологии в повседневность, современный мир порождает новые проблемы. И пока футурологи спорят относительно вопроса, сможет ли в будущем искусственный разум победить человека и не приведет ли цифровая революция к «восстанию машин», кибертеррористы уже сегодня стремятся перехватить процесс управления.

Если обычный террорист для достижения своих целей использует стрелковое оружие и взрывчатку, то террорист в сфере информационного пространства использует для достижения своих целей современные информационные технологии, компьютерные системы и сети, специальное программное обеспечение, предназначенное для несанкционированного проникновения в компьютерные системы и организации удаленной атаки на информационные ресурсы жертвы – в первую очередь компьютерные программные и аппаратные трояны и вирусы, в том числе и сетевые, осуществляющие съем, модификацию или уничтожение информации [2].

В наши дни наиболее уязвимыми точками инфраструктуры могут быть энергетика, телекоммуникации, авиационные диспетчерские, финансовые электронные и правительственные информационные системы, а также автоматизированные системы управления войсками и оружием. Так, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за собой ядерную катастрофу или прекращение подачи электроэнергии в города и на военные объекты. Искажение информации или блокирование работы информационных систем в финансовой сфере может стать следствием снижения экономических показателей страны, а выход из строя, скажем, электронно-вычислительных систем управления войсками и оружием приведет к непредсказуемым последствиям [3].

Атаки кибертеррористов могут быть направлены на основные объекты национальной информационной инфраструктуры:

- оборудование, включая компьютеры, периферийное, коммуникационное, теле-, видео- и аудиооборудование;
- программное обеспечение военных и гражданских объектов;
- сетевые стандарты и коды передачи данных.

Как показано в одной из глав нашей книги (Белоус А.И., Солодуха В.А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – М., Вологда: Инфра-Инженерия, 2020) наиболее опасными по масштабам разрушений могут быть атаки на систему информационной защиты атомных электростанций.

Первой в истории кибератакой на АС, как мы отметили в цитируемой книге, можно считать инцидент 1994 года на бывшей советской Игналинской атомной электростанции. Тогда электронная вычислительная система «Титан», обслуживающая эту станцию, совершила «ошибку», выдав *неправильную* команду роботам, загружающим ядерное топливо в первый реактор станции. А *неизвестные преступники* сообщили литовским властям, что АЭС будет взорвана, если обвиняемый по делу об убийстве журналиста Б. Деканидзе будет приговорен к смертной казни. Тогда работа

АЭС была остановлена, а руководство станции пригласило специальную шведскую комиссию для расследования. Компьютеры электростанции изучались три месяца при помощи экстренно разработанных специальных *программ-ловушек (наверное, их можно считать первыми программными средствами киберзащиты)*. В результате чего выяснилось, что штатный программист станции записал в неиспользуемые ячейки памяти системы некий «паразитный код», как назвали зловредную программу специалисты комиссии. Он перехватывал управление первым и вторым реакторами станции и дожидался начала загрузки ядерного топлива. После этого менялись параметры скорости ввода урановых стержней в активную зону, что реально могло привести к неконтролируемой ядерной реакции.

Проблема «ядерного терроризма» в странах Запада была осознана еще в 1970-х годах. К настоящему времени в этих странах уже сложилась эффективная, эшелонированная система защиты ядерных объектов и материалов, накоплен значительный опыт борьбы с терроризмом, в том числе и в сфере информационной безопасности [4]. В России, где до начала 1990-х годов проявления терроризма практически отсутствовали, работы в этом направлении начались сравнительно недавно, однако уровень защиты наших атомных объектов остается одним из лучших в мире, чего нельзя сказать про многие другие страны, владеющие технологиями мирного атома. Так, по данным Центра Управления Безопасностью (SOC) для Комиссии по ядерному регулированию США только за 2013 и 2014 годы было зафиксировано увеличение на 18% случаев, связанных с кибератаками на атомные электростанции, что на 9,7% больше зарегистрированных аналогичных угроз в других государственных учреждениях. Были выявлены следующие атаки: несанкционированный доступ к компьютерной сети, инфицирование рабочих компьютеров вредоносным кодом, попытка вмешательства в нормальную работу систем и другие. Согласно результатам другого исследования, проведенного Инициативой по сокращению ядерной угрозы, по всему миру ситуация выглядит еще печальнее: 20 стран с мощными ядерно-энергетическими системами уязвимы к кибератакам.

Из списка 47 стран, имеющих атомные объекты, только 13 странам можно поставить высший балл по кибербезопасности, это такие страны, как: Австралия, Беларусь, Болгария, Канада, Финляндия, Франция, Венгрия, Нидерланды, Россия, Швейцария, Тайвань, Великобритания и США. 20 государств набрали низший балл, как относительно киберворовства, так и киберсаботажа. Это такие государства, как Алжир, Аргентина, Армения, Бангладеш, Бельгия, Бразилия, Чили, Китай, Египет, Индонезия, Иран, Италия, Казахстан, Мексика, Марокко, Северная Корея, Перу, Словакия, Испания и Узбекистан [5].

Новости о кибератаках на систему защиты атомных объектов появляются в СМИ постоянно. Так, летом 2017 года телеканал ABC News сообщал о том, что в США хакеры смогли получить доступ к компьютерной сети как минимум одной американской атомной электростанции. Этот взлом затронул важные операционные данные компьютерной системы. Хакерами были добыты сведения, касающиеся бизнес-контактов и другой важной деловой информации. На первый взгляд, потеря деловой документации крупной компании не является страшным риском для общества, однако следует понимать, что цепочка таких событий могла в конечном итоге привести к куда более серьезным последствиям.

Аналогичный случай произошел в декабре 2014 года в Южной Корее, когда хакеры получили доступ к внутренней сети оператора Hydro and Nuclear Power Co Ltd. Проникнуть в сеть удалось после рассылки сотрудникам компании более 5,9 тыс. зараженных писем. В дальнейшем злоумышленники требовали остановки реакторов на АЭС «Кори» и «Вольсон», а также публиковали схемы, внутренние инструкции и данные о сотрудниках [6].

Англичанин Н. Андерсон сумел взломать компьютерную систему Военно-морского флота США и выкрасть секретные пароли, в том числе и *коды, используемые при ядерных ударах*. А Немец Х. Ландер сумел проникнуть в базу данных Пентагона и получить доступ к 29 документам по ядерному оружию, в том числе, например, к «плану армии США в области защиты от ядерного, химического и бактериологического оружия» [7]. Каким образом могут распорядиться такой информацией террористы, можно только догадываться. Как и обычный терроризм, «кибернетическая агрессия» в наши дни является одним из многих способов достижения своих геополитических интересов.

Под удар кибертеррористов могут попадать и *объекты коммуникации*: линии метрополитена, аэропорты, система водоснабжения в городах или система автоматизированного регулирования дорожного движения в крупных мегаполисах. Даже временная приостановка работы перечисленных жизненно важных элементов непременно приведет к социальной напряженности, панике и хаосу в обществе.

Такая атака позволяет проникать в систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия. Эффективность таких форм и методов кибертерроризма зависит от особенностей информационной инфраструктуры и степени ее защищенности. Такие атаки могут привести к уничтожению или активному подавлению линий связи, неправильной адресации, искусственной перегрузке узлов коммутации и многим другим последствиям. Теоретически подобные атаки могут быть нанесены по работе метрополитена или энергетических систем и привести к их отключению на неопределенное время. Можно только представить, к каким последствиям это может привести во время максимальной нагрузки на эти объекты вкупе с соответствующими информационными вбросами в социальные сети.

Такие акции, направленные на дестабилизацию ситуации в стране, управляемые дистанционно, намного безопаснее организовывать, чем с помощью взрывчатых средств и привлечения смертников.

Однако говоря об угрозах кибертерроризма, необходимо понимать, что мощный потенциал цифровых технологий активно используется не только радикальными группировками, входящими в список запрещенных международных террористических организаций, но и *специальными подразделениями государственных структур – членов «космического клуба»*. Например, возможность захвата систем управления военными спутниками, наведения и запуска ракет или комплексами противовоздушной обороны была убедительно продемонстрирована выводом из строя систем противовоздушной обороны Ирака во время операции «Буря в пустыне». Программные и аппаратные закладки, заложенные в комплексах противовоздушной обороны, стоявших на вооружении Ирака и купленных в основном в Европе, по команде извне блокировали нормальную работу систем, в результате

чего американские воздушные силы смогли практически беспрепятственно проникнуть в воздушное пространство этой страны.

Еще одной из распространенных целей кибертеррористов являются *компьютерные сети оборонных и космических структур*. Так, например, широкую известность в узких кругах специалистов получил инцидент с захватом одного из четырех военных спутников связи из серии Skynet-4D, принадлежащих Министерству обороны Великобритании. По данным СМИ, в распоряжении некой интернациональной хакерской группы еще в конце 1990-х годов находилось «совершенно секретное» программное обеспечение, похищенное у Пентагона, которое позволяло управлять целыми группами военных спутников [8], находящихся на орбите Земли.

Говоря об информационных атаках на гражданские, государственные или военные объекты, необходимо понимать, что под видом кибертеррористов, религиозных фанатиков или неадекватных «талантливых личностей», логика действий которых на первый взгляд не прогнозируема, могут скрываться «вполне вменяемые» профессионалы специальных служб (киберподразделений) иностранных государств. Используя *закамуфлированные под терроризм* кибератаки на иностранные государства, можно достигать тех целей, которые просто немыслимы военными методами, политики и дипломатии. Это может быть *экономическое ослабление* конкурента, расшатывание *политической стабильности*, разжигание *конфликтов* внутри суверенных государств или срывы важных *международных договоренностей* путем вброса *дезинформации*. *Фактически речь идет о комплексном воздействии на противника различными средствами одновременно, который в современной военной науке принято называть* ***гибридной войной***.

Не менее опасно и *психологическое воздействие кибертерроризма* на моральное и психологическое состояние пользователей Интернета. Практически все современные террористические организации имеют десятки и сотни сайтов, интернет-страниц и аккаунтов в социальных сетях, на которых размещаются фото- и видеоматериалы, носящие характер угрозы. Одними из первых применили с этой целью Сеть боевики перуанской организации «Тупак Амару», когда в 1996 году во время приема в японском посольстве они взяли в заложники несколько десятков человек. На созданных их последователями пропагандистских сайтах журналистам предлагалось получить комментарии по поводу происходящего у самих лидеров «Тупак Амару» практически в режиме онлайн, естественно, внимание и активность прессы фактически выполнили задачи террористов. Искомая информация была моментально распространена и растиражирована.

Собственные интернет-публикации с угрозами и предупреждениями о готовящихся терактах первой стала осуществлять организация «АльКаида». Со временем этот метод был использован и другими радикальными группировками. На данный момент практически все известные террористические организации используют мощный арсенал информационно-коммуникативных технологий [9].

Наиболее известными видеороликами, широко растиражированными в Интернете, а также многими телеканалами в разных странах стали показательные казни ИГИЛовцами заложников. Эти фильмы фактически произвели революцию в арабском сегменте Всемирной сети, качество пропагандистских фильмов не уступает Голливуду. В этих фильмах есть все, что хочет увидеть зритель: качественная

операторская работа, диалоги, связный сюжет и, естественно, экстремальное и запретное содержание, которое привлекает многих.

Следует понимать, что показательные казни на камеру работают сразу в нескольких направлениях. Во-первых, это мощная самореклама, привлекающая к себе внимание всего мира. Самый надежный способ обратить на себя внимание – это совершение максимально резонансных и скандальных действий, вызывающих бурю эмоций у зрителя. Создатели роликов умело играют на эмоциях зрителя и нагнетают градус напряженности. После сцены казней с отрезанием головы пропагандисты ИГИЛ выложили видео сожжения иорданского пилота, которое больше похоже на высокобюджетный американский фильм ужасов, чем на реальность. Главная задача таких фильмов – не только напугать зрителя, вселить ему чувство тревоги и страха, но и создать напряженную атмосферу страха или мучительного ожидания чего-либо ужасного.

В сети Интернет существует масса сайтов, на которых подробно излагаются рецепты и схемы изготовления оружия и взрывчатых веществ из подручных материалов, а также способы их использования. Многочисленные чаты и форумы идеально приспособлены для передачи зашифрованных посланий террористов.

Тактика современных кибертеррористов заключается в том, чтобы это киберпреступление имело опасные последствия и стало широко известно населению. Получив большой резонанс, информационный терроризм создает атмосферу угрозы повторения акта без указания конкретного объекта. Таким образом, руководители некоторых радикальных мусульманских организаций Ближнего Востока все чаще и активнее используют современные информационные коммуникативные технологии (ИКТ), рассматривая их в качестве эффективного оружия в борьбе с режимами Израиля, Саудовской Аравии и поддерживающими их западными странами.

Такое отношение к ИКТ со стороны радикалов объясняется рядом причин. Во-первых, это достаточно недорогое и в то же время эффективное средство совершения акта терроризма, а во-вторых, Интернет представляет собой сложное пространство для вычисления самого террориста. Наиболее активно методы информационного воздействия использует террористическое движение «Хезболла». Так, например, в структуре этой группировки выделена специальная группа программистов, в задачи которой входит создание и обновление веб-страницы в Интернете для пропаганды проводимых организацией акций и доведения направленной информации до израильтян. Большое внимание «Хезболла» придает таким традиционным методам, как воздействие на аудиторию через средства массовой информации. Для вещания на территории Южного Ливана и Северного Израиля задействованы принадлежащие организации радио- и телевизионный каналы. Помимо материалов агитационного характера, по ним регулярно демонстрируются записи, сделанные при проведении боевых операций против израильских войск и армии Южного Ливана. Трансляция подобных передач способствует снижению боевого духа военнослужащих противника, появлению у них упаднических настроений [10].

Возможность оказать серьезное морально-психологическое воздействие на общество побуждает террористов все чаще прибегать к возможностям Интернета, нежели традиционным методам борьбы с применением летального оружия.

Не менее действенным оказывается психологическое влияние на людей через массовые атаки вредоносных программ на персональные компьютеры пользователей. Весной 2017 года произошла массовая атака червей-вымогателей WannaCry. Более чем 75 000 компьютеров по всему миру, использующих систему Windows, были заражены вредоносной программой. Данное зловредное программное обеспечение не только работало как вымогатель, но и пыталось инфицировать как можно больше систем в сети, сканируя сеть и заражая соседние компьютеры. На экранах мониторов появилось объявление о вирусном нападении с требованием выкупа путем перевода денег на три кошелька криптовалюты Биткоин. Для усиления психологического давления на жертву на экране пораженного компьютера отображался обратный отсчет времени, которое «осталось» у жертвы для выплаты выкупа и спасения информации. Финансовая эффективность нападения сравнительно невысокая, только один из тысячи зараженных компьютеров выплачивал выкуп хакерам, однако это нападение широко освещалось в средствах массовой информации, привлекло внимание правоохранительных органов многих стран и стало ярким примером современного компьютерного терроризма [11, 12].

По своим задачам кибертерроризм ничем не отличается от классических проявлений терроризма, так как его ***главная задача заключается в том, чтобы посеять страх и хаос среди населения***, чувство неуверенности в каждый момент своей жизни, ослабление авторитета государственной власти, которая не смогла своевременно защитить своих граждан от угрозы.

И в этом смысле религиозный фанатик, взрывающий адскую машину в местах большого скопления народа, и хакер, создающий вирусное программное обеспечение, способное нанести удар по критическим элементам национальной инфраструктуры, ничем не отличаются друг от друга. Различными являются лишь *методы* достижения целей террористов, когда преступная *активность переносится из реального мира в виртуальный*.

Современный терроризм в виртуальном пространстве стал одним из ярких примеров симбиоза международной организованной преступности, новейших технологий, спецслужб иностранных стран, а иногда и радикальных фундаменталистских организаций.

Еще одним *направлением кибертерроризма* является оказание психофизиологического воздействия на отдельные социальные группы. Одним из наиболее ярких примеров такого воздействия является ***вирус № 666***, который, по мнению медиков, способен негативно воздействовать на психофизиологическое состояние оператора ПК, ***вплоть до его смерти***. Принцип действия состоит в следующем: он выбирает на экране специально подобранную цветовую комбинацию, погружающую человека в гипнотический транс. Происходит резкое изменение деятельности сердечно-сосудистой системы, и человек может погибнуть. Принцип его действия основан на феномене так называемого 25-го кадра, являющегося весьма мощным средством воздействия на подсознание человека. «Феномен 25-го кадра» связан с тем, что человек имеет не только сенсорный (осознанный) диапазон восприятия, но и субсенсорный (неосознанный), в котором информация усваивается психикой, минуя сознание. Например, если в течение фильма к двадцати четырем кадрам в секунду добавить еще один – 25-й, но с совершенно иной информацией, то глаз человека

его не заметит, однако эта информация неизбежно проникнет в мозг человека и будет им обработана. Многочисленные эксперименты показали, что в течение одной секунды центры головного мозга не успевают принять и обработать 25-й сигнал. Более того, информация, предъявляемая в неосознанном режиме восприятия, усваивается человеком с эффективностью, превышающей обычную норму. Ученые связывают это с тем, что примерно 97% психической деятельности «среднего» человека протекает на уровне подсознания и только 3% – в осознаваемом режиме.

Вирус № 666 выдает на экран монитора в качестве 25-го кадра специально подобранную цветовую комбинацию, погружающую человека в особое состояние транса. Через определенные промежутки времени картинка меняется. По расчетам создателей вируса, подсознательное восприятие нового изображения должно вызывать изменение сердечной деятельности: ее ритма и силы сокращений. В результате появляются резкие перепады артериального давления в малом круге кровообращения, которые приводят к перегрузке сосудов головного мозга человека.

По некоторым данным, за последние несколько лет только в странах СНГ зафиксированы 46 случаев *гибели операторов*, работающих в компьютерных сетях, от подобного вируса [13]. По мнению автора данного исследования, прошедшая в 2019 г. – начале 2020 г. череда *суицидов подростков*, которая произошла в России и странах ближнего зарубежья, была также связана с использованием аналогичных технологий. Большинству участников социальных игр типа «Синий кит» и других предлагалось не только поэтапно выполнять различные задания и выкладывать фотоотчет в Сеть, но и просматривать на первый взгляд нейтральные по своему содержанию видеоролики, в результате чего подростки, не входящие в группу психологического риска, были готовы прыгать с крыш высотных зданий.

Случаи массовых суицидов, подобных «Синему киту», видятся одним из элементов *гибридной войны*, проводимой против нашего государства. В данном случае это *репетиция одного из этапов акций политического протеста*. Так, за несколько лет до кульминационного момента отрабатываются на практике сложнейшие технологии перекодирования сознания подростков, оттачиваются приемы отключения их критического мышления и доведения их до такого состояния, когда они были готовы выполнять любые задания модераторов «игры». К сожалению, использованные технологии оказались слишком эффективными и, вполне возможно, могут быть использованы в качестве различного рода провокаций на массовых мероприятиях.

В 2015–2017 гг. несовершеннолетние участники подобных социальных игр прыгали с крыш высотных зданий, теперь их могут призвать совершить публичный суицид во время митинга или бросить бутылку с зажигательной смесью в представителей правопорядка.

Информационно-коммуникативные технологии находятся на таком уровне развития, что позволяют эффективно и латентно воздействовать на подсознание здорового человека, превращая его в добровольного смертника. Объединение подобных киберугроз с технологиями «цветных революций», к которым привлекаются массы протестующих, может вызвать катастрофические последствия. Что в очередной раз подтверждает *возможность использования кибертерроризма в геополитических целях*.

Не менее важным направлением действий кибертеррористов является *предоставление провокационной информации* с целью нарушения баланса сил на международной

арене и разжигания межнациональных конфликтов. Первые проявления подобного рода кибертерроризма проявили себя еще двадцать лет назад. Так, в начале 1999 года в посольства более 20 стран (Великобритании, США, Австралии, Израиля и др.) были разосланы электронные письма от имени офицеров российской ракетной воинской части, имеющей на вооружении стратегические ракеты шахтного базирования. Письма содержали сведения о недовольстве унизительным положением России, а также *угрозу самовольного пуска ракет по целям, расположенным в западных странах*.

В результате проведенного расследования ФСБ России были задержаны два жителя города Калуги, не имевшие никакого отношения к военной службе. Судом данные действия квалифицированы как сообщение о заведомо ложном акте терроризма [14].

В феврале 2000 года армянские хакерские группы «Liazor» предприняли компьютерную атаку против 20 сайтов правительственных организаций и средств массовой информации Азербайджана. Причем действия осуществлялись одновременно с территории нескольких стран: Армении, России и США. Армянские хакеры также создали и внедрили специальную компьютерную программу «Synergy Internet Systems» обеспечивающую негласный перехват и снятие информации с компьютеров.

И это лишь некоторые примеры вмешательств кибертеррористов в процесс *международных отношений*. Подобные действия не только подрывают международный авторитет государств, но существенно мешают установлению стабильных дипломатических отношений на международной арене. А иногда, воруя и обнародовав секретную информацию, а порой предоставив *качественную дезинформацию*, кибертеррористам удается полностью сорвать международные договоренности.

Многие кибертеррakты стали связываться с определенными политическими заказами. Например, 9 мая 2014 года всемирно известная хакерская группа «Anonymous» фактически парализовала работу официального портала Президента Российской Федерации «Kremlin.Ru». В течение нескольких часов официальный сайт президента России был заблокирован [15].

Специалисты по кибербезопасности также обращают внимание на то, что популярная технология видеоконференций, получившая широкое применение в государственном управлении является весьма уязвимой, поскольку с помощью современных технических средств видеоизображение может быть *полностью сфальсифицировано*. Так, инженеры Массачусетского технологического института с помощью средств компьютерной графики и искусственного интеллекта, продемонстрировали публике неотличимые от реальных видеозаписи известных публичных деятелей, говорящих то, что *они заведомо не могли бы сказать в реальности* [16].

Вполне возможно, что в ближайшее время подобные технологии могут оказаться в руках террористов или тех политических сил, которые, прикрываясь террористической организацией или группой анонимных хакеров, попытается таким образом вмешаться в ход международных отношений.

В январе 2013 года «Лаборатория Касперского» опубликовала первый аналитический отчет об исследовании масштабной кампании, проводимой киберпреступниками с целью шпионажа за дипломатическими, правительственными и научными организациями в различных странах мира. Действия злоумышленников

были направлены на получение конфиденциальной информации, данных, открывающих доступ к компьютерным системам, персональным мобильным устройствам и корпоративным сетям, а также сбор сведений геополитического характера [17].

Все чаще кибертеррористы пытаются вмешиваться в международные политические процессы, совершая как одиночные атаки, так и проводя долговременную агрессию против конкретных стран. Так, например, «хакерская группа GhostShell заявила о начале кибервойны с Россией и опубликовала данные около 2,5 миллиона аккаунтов и различных записей государственных, правоохранительных, образовательных, финансовых, медицинских и других учреждений. Свои действия хакеры назвали Project BlackStar и заявили, что они направлены именно против российского правительства.

Несколько ранее аналогичную кибервойну эта же организация развернула против Китая [15]. Страны, претендующие на собственную исключительную роль в однополярном мире, уже давно используют не только военную и экономическую мощь, но все чаще прибегают к методам информационного воздействия. В начале октября 2014 года в США была обнародована новая оперативная концепция сухопутных американских войск «Победа в сложном мире. 2020–2040». При этом в концепции выделяют пять полей противоборства: суша, море, воздух, космос и киберпространство.

Киберпространство становится важным полем боя за политические симпатии граждан внутри страны, а на международной арене глобальная сеть становится мощнейшим рычагом влияния на геополитические процессы. Цифровая информация становится мощнейшим оружием политических экстремистов, тесно сотрудничающих со спецслужбами иностранных стран.

Еще одним новым направлением, в котором активно себя проявляет кибертерроризм, – это ведение агитации и распространение радикальной информации и набор в свои ряды новых членов. Сейчас практически все известные террористические организации имеют свои сайты в Интернете и активно пытаются проникать в социальные сети. Так, например, террористы ИГИЛ активно используют аккаунты в наиболее популярных социальных сетях (Facebook, Twitter, Instagram, Friendica «ВКонтакте» и «Одноклассниках» и др.), через которые распространяется информация об этой организации, ведется пропаганда и вербовка новых сторонников. По некоторым данным, только в Twitter зарегистрировано более 45 тысяч аккаунтов «Исламского государства», что превращает их в мощный винтик пропагандистской машины террористов [18].

Современный мир диктует новые правила и законы жизни. С появлением цифровых технологий, тесной интеграцией человечества и информационно-коммуникативных систем, которые стали частью повседневной жизни человека, появились новые виды рисков и угроз. В силу колоссальных технических возможностей, которыми обладает кибертерроризм, это новое явление моментально превратилось в одну из важнейших угроз мирового масштаба. А в условиях обострения международных отношений, разрушения системы однополярного мира, возвращения на мировую арену России и появления нового лидера – Китая, ***кибероружие становится действенным рычагом глобального противостояния***. От того, кто быстрее сможет освоить эти технологии, создать мощную систему защиты от

кибертерроризма, зависит не только национальная безопасность отдельно взятой страны, но и в целом миропорядок на планете.

1.1.4. Кибертерроризм как форма гибридной войны

1.1.4.1. Кибертерроризм и политический терроризм

Если еще совсем недавно бескрайние просторы Интернета активно использовались различного рода мошенниками, которых интересовала исключительно финансовая выгода, то теперь возможности виртуального пространства оказались в руках более опасных игроков, преследующих в первую очередь политические цели.

Как уже было отмечено выше – в мировой обществоведческой науке пока не существует единого мнения о том, какие же угрозы считать кибертерроризмом, хотя сам термин появился практически сразу с появлением серийных компьютеров еще в конце прошлого века. Так, термин «кибертерроризм» впервые был использован старшим научным сотрудником Калифорнийского института безопасности и разведки Барри Коллином еще в далеком 1980 году. В то время сеть Управления перспективных разработок Минобороны США ARPANET, которая являлась предшественницей Интернета, объединяла всего лишь несколько компьютеров на территории одного государства. Однако исследователь утверждал, что уже достаточно скоро возможности киберсетей будут взяты на вооружение террористами.

В 1997 году сотрудник ФБР Марк Поллитт ввел в обиход новый юридический термин, предложив считать «кибертерроризмом» *любую «умышленную, политически мотивированную атаку на информацию, компьютерные системы, программы и данные, которая приводит к насилию в отношении невоенных целей, групп населения или тайных агентов»* [19].

Проблемы в определении понятия «кибертерроризм» связаны с одной стороны с тем, что порой трудно отделить сам *терроризм* такого вида от *информационной войны* и факта использования *информационного оружия*. Не менее трудным представляется разграничить его с информационным криминалом и преступлениями в сфере цифровой информации.

С другой стороны трудности возникают при попытке выявить специфику данной формы терроризма. Так, экономический и психологический моменты кибертерроризма тесно переплетены, и невозможно однозначно определить, какой из них имеет *большее* значение. Такие авторитетные в этой области исследователи, как Дж. Девост, Б.Х. Хьютон, Н.А. Поллард, определяют кибертерроризм как сознательное злоупотребление цифровыми системами, сетями или их компонентами в целях, которые способствуют осуществлению террористических операций или актов [20].

Ключевым отличительным признаком киберпреступности принято считать корыстный характер действий злоумышленника. Кибертерроризм же отличается от вышеприведенных преступлений в первую очередь своими целями, которые остаются схожими с привычным *политическим терроризмом*. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала.

Важно понимать, что кибертеррорист существенно отличается от хакера, компьютерного хулигана или компьютерного вора, которые действуют в корыстных или хулиганских целях. Главная задача виртуального терроризма состоит в том, чтобы совершенный террористический акт имел не только опасные последствия, стал широко известен населению, но и получил большой общественный резонанс [21]. Как правило, требования кибертеррористов сопровождаются угрозой повторения акта без указания конкретного объекта, что также отличает это явление от информационного криминала.

Говоря о современном кибертерроризме, следует понимать, что это многогранное явление, которое выражается в политически мотивированной атаке на виртуальное пространство, создающее опасность для жизни или здоровья людей либо наступления других тяжких последствий, часто такие действия связаны с нарушением общественной безопасности, запугивания населения, подрывом инфраструктуры и провокациями военного характера.

Отличительной чертой кибертерроризма является непосредственное воздействие на общество с целью его устрашения, парализации воли членов социума, распространения панических настроений, чувства незащищенности. Это достигается путем тиражирования информации об угрозах насилия, поддержания состояния постоянного страха с целью достижения определенных политических или иных целей, принуждения к определенным действиям, а также привлечения внимания к самой террористической организации. Конечной целью кибернетической атаки террориста является не только демонстрация своих технических возможностей (что характерно для хакеров-хулиганов), но и попытка с помощью их оказывать влияние на политическую власть в стране. Сравнивая кибертерроризм с другими виртуальными преступлениями, необходимо отметить, что *информационные террористы* используют одинаковые технические средства наравне с *киберпреступниками*, однако имеют *отличные цели*.

По характеру воздействия на социум кибертерроризм имеет универсальный характер, так как охватывает практически все сферы жизни общества, что также отличает его от других видов информационной преступности. В силу практически стопроцентной интеграции общества развитых стран с цифровыми технологиями, когда виртуальное пространство не только постоянно существует в жизни человека, но иногда играет большую роль, чем реальная реальность, кибертерроризм получает колоссальный веер возможностей.

Угроза, которая исходит от кибертерроризма, огромна, а в некоторых случаях она может иметь необратимый характер. Современному обществу еще только предстоит выработать эффективную систему противодействия и борьбы с этим информационным злом современности, а следовательно, требуется тщательный его анализ.

1.1.4.2. Перспективы кибертерроризма

Привлекательность использования киберпространства для современных террористов связана с тем, что для совершения кибертеракта не нужны большие финансовые затраты – необходим лишь персональный компьютер, подключенный к сети Интернет, а также специальные программы и вирусы.

Терроризм в глобальной компьютерной сети развивается динамично: интернет-сайты появляются внезапно, часто меняют формат, а затем и свой адрес. Если в 1998 г. около половины из тридцати террористических групп, внесенных США в список «Иностранных террористических организаций», имели свои сайты, то сегодня почти все террористические группы присутствуют в Интернете.

Среди них – перуанские террористы из организаций «Сендеро Луминосо» и «Тупака Амару», боевики афганского движения «Талибан», грузинские националисты из группы «За свободную Грузию», «Тамильское движение сопротивления» и многие другие террористические структуры, функционирующие на различной организационной и идеологической основе.

«Аль Кайда», «Хезболла», «Хамас», «Организация Абу Нидаля», «Черные Тигры» (связанные с «Тиграми Освобождения Тамил Илама») не только используют киберпространство для пропаганды своих взглядов, но и в качестве оружия для нанесения ударов по объектам национальной инфрастуктуры, для атак на иностранные сайты и серверы.

Интернет-аудитория террористических сайтов используется для активизации потенциальных и реальных сторонников террористов; для влияния на международное общественное мнение, непосредственно не вовлеченное в конфликт; для деморализации «врага» – граждан, организаций и государств, против которых борются террористы.

К настоящему времени кибертерроризм стал суровой реальностью. Общее количество происходящих в мире кибератак очень трудно подсчитать, так как в силу разных причин не все они становятся достоянием гласности.

В этой связи некоторые *эксперты предлагают перейти на новую систему Интернета,* радикально отказавшись от его изначальной концепции полной открытости.

Основной смысл новой модели состоит в *отказе от анонимности пользователей Сети,* что позволит обеспечить ее большую защищенность от преступных посягательств. Компания Microsoft, к примеру, объявила о готовности выплачивать премию за выявление каждого кибертеррориста в размере 50 тыс. долл.

В качестве рекомендаций, направленных на противодействие опасным тенденциям и повышение эффективности борьбы с киберпреступностью и кибертерроризмом, большинство экспертов предлагает следующее.

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 первую очередь с Россией) 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.

Уголовно-правовая борьба с киберпреступностью и кибертерроризмом – глобальная проблема в силу того, что киберпреступность носит трансграничный характер.

Поэтому для эффективной борьбы с киберпреступлениями необходимо не только принятие соответствующих уголовно-правовых норм на *национальном* уровне, но и выработка единых *международных* стандартов, таких как определение круга деяний, подлежащих криминализации, выработка единого понятийного аппарата и единой терминологии, пересмотр существующих уголовно-правовых норм с учетом стандартов, установленных международно-правовыми документами.

Итак, киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. Поэтому с ростом использования информационных технологий в различных сферах деятельности человека растет и будет расти и вероятность использования их в целях совершения преступлений.

Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных «мастей» кибертеррористов. Об обеспечении безопасности надо думать сегодня, в этом и заключается одна из главных целей этой книги.

1.2. Киберпреступность

1.2.1. Классификация типов киберпреступлений согласно Конвенции Совета Европы

Конвенция Совета Европы выделяет 4 типа компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- ***незаконный доступ*** – ст. 2 конвенции (противоправный умышленный доступ к компьютерной системе либо ее части);
- ***незаконный перехват*** – ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
- ***вмешательство в данные*** – ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- ***вмешательство в систему*** – ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

1.2.2. Основные виды киберпреступлений, представленные в Конвенции Совета Европы

- Незаконный доступ в информационную среду;
- нелегальный перехват информационных ресурсов;
- вмешательство в информацию, содержащуюся на магнитных носителях;
- вмешательство в компьютерную систему;
- незаконное использование телекоммуникационного оборудования;

- мошенничество с применением компьютерных средств;
- преступления, имеющие отношения к деяниям, рассматриваемым в содержании Конвенции;
- преступления, относящиеся к «детской» порнографии;
- преступления, относящиеся к нарушениям авторских и смежных прав.

Надо отметить, что в зарубежном законодательстве понятие кибертеррорист часто трактуется как хакер.

1.2.3. Классификация арсенала используемого киберпреступниками «кибероружия»

Арсенал используемого кибертеррористами и киберпреступниками «оружия» включает в себя:

- ***различные виды кибератак***, позволяющие проникнуть в атакуемую сеть или перехватить управление сетью;
- ***компьютерные вирусы***, в том числе – сетевые (черви), модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем;
- ***логические бомбы*** – наборы команд, внедряемые в программу и срабатывающие при определенных условиях, например по истечении определенного отрезка времени;
- ***«троянские кони»***, позволяющие выполнять определенные действия без ведома хозяина (пользователя) зараженной системы;
- ***средства подавления информационного обмена в сетях.***

1.2.4. Стандарты кибербезопасности

Глобальный масштаб киберугроз неминуемо привел мировое информационное сообщество к разработке единой системы критериев ИБ. Так были введены стандарты кибербезопасности (Cybersecurity standards), описывающие методологию защиты информационной среды пользователя или организации: всего ПО, данных, информационных систем, сетей, хранилищ, серверного и коммутационного оборудования, рабочих станций, разнообразных гаджетов с подключением к сети и т.п. Эти стандарты разрабатываются с 1990-х годов и непрерывно актуализируются с учетом меняющейся обстановки в сфере информационной безопасности. Они используются как в глобальном, так и локальном контексте, формируя унифицированный подход к защите информационных систем в каждой стране.

Наиболее известные международные стандарты: ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO 15408, немецкий стандарт IT Baseline Protection Manual – Standard security safeguards (Руководство по базовому уровню защиты информационных технологий) от German Information Security Agency, британские стандарты IASME, BS 7799-1:2005, BS 7799-2:2005 и BS 7799-3:2006, американские NERC и NIST.

Эти документы максимально подробно описывают процессы и процедуры ИБ, раскрывают терминологию, включают в себя различные инструменты защиты от киберугроз, концепции безопасности, политики, руководства пользователя, меры