мир электроники

А.И. БЕЛОУС, В.А. СОЛОДУХА

Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения

ТЕХНОСФЕРА

УДК 004.492
ББК 32.85
Б43

Б43 Белоус А.И., Солодуха В.А.
Основы кибербезопасности.
Стандарты, концепции, методы и средства обеспечения
Москва: ТЕХНОСФЕРА, 2021. – 482 с. ISBN 978-5-94836-612-8

Эта книга фактически представляет собой научно-практическую энциклопедию по современной кибербезопасности. Здесь анализируются предпосылки, история, методы и особенности киберпреступности, кибертерроризма, киберразведки и киберконтрразведки, этапы развития кибероружия, теория и практика его применения, технологическая платформа кибероружия (вирусы, программные и аппаратные трояны), методы защиты (антивирусные программы, проактивная антивирусная защита, кибериммунные операционные системы). Впервые в мировой научно-технической литературе приведены результаты системного авторского анализа всех известных уязвимостей в современных системах киберзащиты – в программном обеспечении, криптографических алгоритмах, криптографическом оборудовании, в микросхемах, мобильных телефонах, в бортовом электронном оборудовании автомобилей, самолетов и даже дронов. Здесь также представлены основные концепции, национальные стандарты и методы обеспечения кибербезопасноти критических инфраструктур США, Англии, Нидерландов, Канады, а также основные международные стандарты. Фактически в объеме одной книги содержатся материалы трех разных книг, ориентированных как на начинающих пользователей, специалистов среднего уровня, так и специалистов по кибербезопасности высокой компетенции, которые тоже найдут здесь для себя много полезной информации.

Знания, которые вы получите из этой книги, помогут вам повысить безопасность работы в Интернете, безопасность офисных и домашних устройств, изучить и применять в практической деятельности наиболее эффективные и опробованные на практике политики безопасности.

УДК 004.492
ББК 32.85

ISBN 978-5-94836-612-8

Содержание

Предисловие

Кибербезопасность играет фундаментальную роль в жизни современного информационного общества, в котором большинство работающих занято производством, хранением, обработкой и реализацией различной информации.

Эта книга предназначена для широкого круга читателей – от «начинающих» и пользователей «среднего уровня» подготовки до «продвинутых» пользователей – специалистов по кибербезопасности крупных корпораций и промышленных инфраструктур.

Поэтому материалы всех 9 глав этой книги построены по принципу «от простого к сложному».

Знания, которые вы получите из этой книги, помогут вам повысить безопасность работы в интернете, повысить безопасность домашних и офисных устройств, изучить и применять в своей практической деятельности наиболее эффективные и опробованные на практике политики безопасности.

В общем случае *под кибербезопасностью сегодня понимают совокупность различных концепций, доктрин, стратегий, методов и средств защиты от атак злоумышленников (хакеров) на компьютеры, серверы, информационные системы, сети передач данных, мобильные устройства и т.д.*

Очевидно, что прежде чем изучать эти стратегии, методы и средства кибербезопасности, необходимо хорошо представлять, от каких явлений и угроз надо защищаться (киберпреступность, кибертерроризм, кибершпионаж, кибербразведка), надо хорошо знать основные концепции и методы применения современного кибероружия, надо знать все типовые уязвимости в системах киберзащиты, через которые проникают компьютерные вирусы, программные и аппаратные трояны, а также типовые и перспективные средства защиты от них – антивирусные программы, средства проактивной антивирусной защиты, перспективные кибериммунные и киберфизические операционные системы, методы и средства кибербразведки и киберконтрразведки, методы и средства обеспечения кибербезопасности конечных точек (оконечных устройств) и многое другое.

В свою очередь сегодня активно развиваются многочисленные направления обеспечения безопасности как самих сетей, так и различных приложений. Например, под безопасностью сетей понимают действия по защите компьютерных сетей от различных угроз (целевых атак, вредоносных программ и т.д.). Под безопасностью приложений понимают методы, программные и аппаратные средства защиты от угроз, которые злоумышленники могут «спрятать» в различных прикладных программах. Ведь такое «заряженное» приложение может открыть злоумышленнику доступ к данным, которые это приложение по определению должны защищать от несанкционированного доступа. Поэтому безопасность таких приложений должна обеспечиваться еще на стадии разработки, до появления приложения в открытых источниках.

То же самое можно сказать и о «безопасности информации» – обеспечении целостности и конфиденциальности данных как в процессе их передачи, так и во время их хранения.

К вопросам кибербезопасности также относятся и методы аварийного восстановления – оперативное автоматические реагирование систем защиты на любые

инциденты (действия злоумышленников), которые могут нарушить работу системы или привести к утечке или потере данных.

Еще одно относительно новое направление кибербезопасности – кибербезопасность оконечных устройств – обеспечение безопасности разных устройств (планшеты, ноутбуки, мобильные телефоны, рабочие станции), находящихся в оконечных точках корпоративных и промышленных сетей.

Особое место в проблеме обеспечения кибербезопасности занимают *стандарты кибербезопасности*. Это вообще особая тема – мало того что на момент выхода этой книги существует великое множество различных международных стандартов, так еще практически у каждой страны (государства) имеются свои собственные многостраничные стандарты, определяющие типовые процедуры и сценарии сбора и обработки информации, оценки рисков, типовых решений и действий.

На темы кибероружия и кибербезопасности уже написаны тысячи статей и сотни книг, этим темам посвящены многочисленные ежегодные конференции, форумы и симпозиумы. Однако большинство этих книг посвящено исследованиям только отдельных направлений и механизмов обеспечения кибербезопасности.

Сложившуюся в этой области информационную ситуацию можно кратко охарактеризовать известной русской пословицей «За деревьями леса не видно» – в этом «информационном лесу» сегодня сложно ориентироваться не только «начинающим» и «продвинутым» специалистам, но даже профессионалам.

Поэтому в предлагаемой вниманию читателей книге предпринята амбициозная попытка систематизации основных наиболее известных из Интернета сведений и опубликованной ранее самими авторами научно-технической литературы описаний и создания описания по возможности наиболее полной картины такого информационного «леса» (основ кибербезопасности), состоящего из описаний отдельных «деревьев» (концепций, методов и средств как организации атак, так и противодействия им).

Образно говоря, все нам известные популярные книги по этой тематике посвящены детальному великолепному описанию только отдельных «деревьев» или их групп (опушки леса). Чтобы стать действительно компетентным специалистом в области такой сложной науки, как «кибербезопасность», необходимо последовательно изучать каждое из многочисленных «деревьев» и при этом «не заблудиться в лесу».

Современная кибербезопасность как новая отрасль науки стремительно развивается (быстро вырастают все новые «деревья»). Например, еще 10 лет назад в работе «Science of Cyber-Security» было предсказано, что эта область науки начнет активно использовать теоретические положения теории игр, криптографии, машинного интеллекта, обфускации, высокоуровневого компьютерного моделирования, что сегодня мы видим уже на практике.

Так вот, наша книга является своего рода «путеводителем» в этом «информационном лесу», позволяя читателю самому легко выбирать именно те «деревья», которые его интересуют, и «в этом лесу не заблудиться».

Особое место в проблеме обеспечения кибербезопасности всегда занимало «военное» направление, этот момент надо рассмотреть более детально.

Как известно, средством ведения любых боевых действий (войн) является оружие, под которым обычно понимаются многообразные устройства, средства и

системы, применяемые для физического поражения (уничтожения) живой силы противника или выведения из строя его техники, сооружений и коммуникаций. Образно говоря, оружие – это специальные средства для борьбы с кем-нибудь или чем-нибудь для достижения поставленных целей.

История создания и развития оружия неразрывно связана с историей развития человечества. Возможно, это звучит странно, но на всех этапах эволюции оружия (от меча, лука до космической ракеты) именно развитие оружия являлось катализатором (ускорителем) прогресса, стимулировало развитие новых технологий, новых материалов, конструкторской мысли – так появилась металлургия, различные технологии изготовления и обработки новых материалов, новые профессии.

Сегодня существует великое множество типов, видов и разновидностей современного оружия: обычное, высокоточное, химическое, атомное, космическое, лазерное, СВЧ-оружие, гиперзвуковое и т.д. Однако наряду с огромными «поражающими» возможностями, все без исключения виды и типы этого современного оружия обладают и весьма существенными недостатками и ограничениями, в попытках устранить которые военные и ученые прилагают значительные интеллектуальные усилия и на что ежегодно тратятся огромные финансовые ресурсы всех индустриально развитых стран мира.

Сами военные, руководители правительств, здравомыслящие политики всех стран мира хорошо понимают, что использование «на практике» как этих «обычных» типов оружия, так и разрабатываемых в закрытых институтах различных «экзотических» типов (климатическое, сейсмическое, плазменное) в некотором смысле равносильно «самоубийству» для применившей его стороны. Кибернетическое (кибероружие, информационно-техническое) оружие с этой точки зрения является почти «идеальным» оружием, поскольку лишено большинства этих недостатков и ограничений и обладает новыми поистине огромными возможностями.

Но военные также хорошо понимают и тот факт, что использование компонентов кибероружия в современных локальных конфликтах и «сетецентрических» войнах (не путать с «сетевыми войнами») в принципе может обеспечить тот же результат, что и классические виды оружия, но при этом потребуется несоизмеримо меньше затрат материальных и людских ресурсов без риска получить от противника ответный «удар возмездия».

Базисом (технологической платформой) современного кибероружия являются многочисленные вирусы, черви, программные и аппаратные трояны, шпионские программы, использующие различные уязвимости в системах киберзащиты (уязвимости в микросхемах, криптографических алгоритмах, стандартах, протоколах, уязвимости программного обеспечения и т.д.).

Вирусы, черви, программные и аппаратные трояны представляют угрозу практически для всех базовых объектов инфраструктуры современного государства, но прежде всего – для информационных систем обеспечения национальной безопасности, банковских и финансовых структур, систем управления вооружением и военной техникой, навигации и связи, транспортной инфраструктуры и особенно – для объектов топливно-энергетического комплекса (атомные, тепловые

и гидростанции, нефте- и газоперерабатывающие заводы, системы управления нефте- и газопроводами).

Например, внедренные «кем-то» в микросхемы, аппаратные и программные трояны оказались способными творить невероятные вещи. Они могут выполнять по команде своего «хозяина» самые различные несанкционированные и скрытые от разработчика аппаратуры функции – передавать своему «хозяину» любую информацию, изменять режимы функционирования, электрические режимы работы микросхемы (вплоть до ее частичного или полного отказа). Попадая на платы электронных блоков радиоэлектронной аппаратуры, компьютеров, современных информационно-коммутационных устройств, систем энергообеспечения мегаполисов, систем управления высокоточным оружием, систем обеспечения безопасности атомных станций и т.п., такие «заряженные» микросхемы способны не только организовать передачу «хозяину» любой секретной информации, но и полностью «перехватывать» управление этими объектами, вплоть до приведения их в неработоспособное состояние.

Интересно, что в исторической ретроспективе программные и аппаратные трояны первыми начали использовать в своей «работе» национальные криминальные группы (мафиози, гангстеры, русские братки, якудза) для достижения своих чисто криминальных целей без классического применения оружия (незаконные банковские операции, сбор конфиденциальной информации, уничтожение улик в базах данных и т.п.).

Спецслужбы Китая, США, Израиля и России, военные этих стран раньше других оценили как уровень этой новой угрозы, так и поистине неограниченные возможности данного направления, которое уже потом журналисты назвали кибероружием. Так, в составе вооруженных сил практически всех индустриально развитых стран появились специальные подразделения, которые сегодня называют «кибервойсками».

На смену любителям, пишущим вирусы и троянские программы ради развлечений, а потом и киберпреступникам, вымогающим или крадущим деньги, сегодня пришли сообщества людей, воспринимающих современные информационные системы и киберпространство в целом исключительно как «поле боя».

Ниже перечислены ключевые вопросы из области кибербезопасности, на которые читатель этой книги найдет развернутые ответы.

- Что такое киберпреступность и чем она отличается от кибертерроризма.
- «Взлеты» и «падения» самых известных хакеров.
- Этичные хакеры и хактивисты – мифы и реалии.
- Методы работы кибермошенников и способы защиты от них.
- Классификация, концепции, средства, методы и примеры применения современного кибероружия.
- Как определить исполнителей и заказчиков кибератак?
- Основные уязвимости в современных системах киберзащиты – в программном обеспечении, криптографических алгоритмах (стандартах), криптографическом оборудовании, в бортовом оборудовании автомобилей, воздушных судов и дронов.

- Наиболее опасные компьютерные, автомобильные и телефонные вирусы, трояны и шпионские программы.
- Антивирусные программы, методы проактивной защиты, киберфизические и кибериммунные операционные системы.
- SIEM как обязательный элемент в современной архитектуре киберзащиты.
- Что такое кибершпионаж, киберразведка и киберконтрразведка.
- Стратегическая киберразведка как способ управления рисками.
- Почему израильское секретное подразделение 8200 считается лучшим в мире подразделением кибервойск?
- Особенности отбора и обучения специалистов для противостояния в киберпространстве.
- Расследование кибератак как высокоприбыльный бизнес и инструмент политической борьбы.
- Что такое «кибербезопасность конечных точек» и как ее обеспечить.
- Основные политики безопасности-концепции, стратегии и стандарты кибербезопасности ведущих индустриально развитых стран – США, Англии, Канады, Нидерландов, альянса НАТО.
- Что такое «ежегодные отчеты управления контрразведки США о киберугрозах» и зачем их нужно изучать.
- Как обеспечить кибербезопасность критических инфраструктур-энергетических систем, нефте- и газопроводов, атомных и тепловых электростанций?
- А как обеспечить кибербезопасность микросхем, используемых в автоматизированных системах управления военной техникой и производственными процессами?

На эти и многие другие актуальные вопросы вы найдете исчерпывающие ответы в этой уникальной книге.

В книге также использовались отдельные материалы, опубликованные ранее в России в двухтомной монографии (А.И. Белоус, В.А. Солодуха, С.В. Шведов. Программные и аппаратные трояны. Способы внедрения и методы противодействия. Первая техническая энциклопедия), вышедшей в 2018 г.; А.И. Белоус, В.А. Солодуха. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – Инфра-Инженерия, 2020; A. Belous, V. Saladukha. Viruses, Hardware and Software Trojans – Attacks and Countermeasures; A. Belous, V. Saladukha. Handbook of cybersecurity. 3 Books in 1.

При написании этой книги авторы руководствовались следующими принципами, которые было легко сформулировать, но затем очень сложно было их реализовать на практике.

1. Инженерам-разработчикам информационных систем, специалистам по информационной безопасности, студентам и их преподавателям всегда необходимо иметь «под рукой» некий систематизированный сборник справочных материалов по проблемам кибероружия и методам защиты от киберугроз.
2. Чтобы стать достаточно популярным изданием среди широкого круга специалистов по кибербезопасности, ученых, инженеров и студентов, эта книга должна выполнять одновременно интегральные функции и классического учебника, и краткого справочника, да и просто увлекательной книги.

3. Представляя большой объем необходимой справочной информации, в отличие от классических учебников с изобилием математических выражений и физических формул, попытаться максимально простым языком изложить как основные теоретические аспекты проблемы кибероружия, так и основные практические моменты организации противодействия основным видам киберугроз. В книгу должны включаться только те методы, технические и технологические решения, эффективность которых ранее была подтверждена практикой их применения.
4. В тексте необходимо использовать максимально возможное количество графического материала, отражающего эффективность различных рабочих сценариев.

Насколько удалось авторам реализовать эти принципы – судить читателю.

Авторы выражают благодарность рецензентам – академику НАН Беларуси и иностранному избранному члену Академии Наук Российской Федерации Лабунову В.А., профессору кафедры защиты информации БГУИР Лынькову Л.М., чьи критические замечания и полезные советы во многом способствовали появлению книги именно в этом формате, а также Антипенко О.А. за помощь в обработке материалов и подготовке рукописи к печати.

Введение

Материалы книги представлены в виде 9 глав, которые в зависимости от сферы интересов читателя и уровня его подготовки можно читать в произвольном порядке.

Глава 1 посвящена рассмотрению основных проблем, непосредственно связанных с киберпреступностью и кибертерроризмом. Здесь приведена краткая история кибертерроризма, приведены основные термины и определения, рассмотрены основные способы реализации кибертеракторов, основные направления развития и 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, а также основные стандарты кибербезопасности в этой области. В качестве одного из примеров построения эффективных систем кибербезопасности здесь кратко рассмотрены особенности организации структуры и принцип функционирования систем киберзащиты НАТО. Приведен с авторскими комментариями детализированный алгоритм организации типовой кибератаки.

Завершает главу раздел, посвященный «тонкостям профессий» заливщиков, ботоводов, рефоводов и прочих разновидностей кибермошенников – основные методы, способы и средства их детальности, а также практические рекомендации – как обычному пользователю Интернета защититься от этих и ряда других подобных «профессионалов».

Во ***второй главе*** детально рассмотрены концепции, средства, методы и примеры применения кибероружия, приведены научные обоснования, определения (термины) и классификация кибероружия и видов его воздействия на атакуемые объекты.

Здесь кибервоздействия классифицированы по следующим категориям: по виду (одиночные и групповые), по типу (пассивные и активные), по характеру поражающих свойств (высокочастотные и комплексные), по цели использования (атакующие, оборонительные и обеспечивающие), по способу реализации (алгоритмические, программные, аппаратные, физические).

Рассмотрены и особенности многочисленных разновидностей каждого из вышеуказанных типов. Например, анализируются такие типы атакующих кибервоздействий, как «нарушение конфиденциальности информации», «нарушение целостности информации», «нарушение доступности информации», психологические воздействия. Из оборонительных разновидностей кибервоздействий рассматриваются «выявляющие», «противодействующие», «отвлекающие на ложные информационные ресурсы» и т.д.

Третья глава посвящена исследованиям основных наиболее известных типов уязвимостей в системах киберзащиты и по своему содержанию пока не имеет аналогов в мировой и отечественной литературе по проблемам кибербезопасности. Здесь рассмотрены основные типы всех известных уязвимостей в микросхемах, в криптографических алгоритмах и криптографических стандартах, в криптографическом оборудовании, в программном обеспечении информационных систем, а также опасные уязвимости в бортовом оборудовании воздушных судов и совре-

менных робототехнических комплексов. Приведена классификация, термины и механизмы функционирования уязвимостей современных систем информационной безопасности. Например, достаточно подробно рассмотрен механизм работы опасной уязвимости типа «переполнение буфера».

Отдельный раздел главы посвящен новым угрозам – основным уязвимостям в бортовых электронных системах управления мобильной техникой (легковые и грузовые автомобили и электромобили, «беспилотные» транспортные средства). Эта угроза называется «Hackoble» (уязвимости современных автомобилей для кибератак).

Завершает главу раздел, посвященный наиболее эффективным методам выявления вышерассмотренных программных уязвимостей (сертификационные испытания, тестирование безопасности кода и др.), здесь же рассмотрена современная концепция Fiva-Level Problem – пути снижения уязвимостей критических систем.

В ***четвертой главе*** рассмотрены наиболее эффективные антивирусные программы, описаны основные компоненты построения стандартной антивирусной защиты, основные требования к антивирусным программам, их основные технические характеристики, классификация и принципы работы. Приведен краткий обзор наиболее эффективных антивирусных программ, даны конкретные практические рекомендации пользователям от разработчиков антивирусного программного обеспечения. Отдельный раздел посвящен относительно новому направлению – проактивной антивирусной защите – функции, возможности, методы применения. Особенности работы с этими защитными средствами продемонстрированы на конкретных примерах (Behavior Control, Component Control, Removeble Media Protection – защита переносных мультимедийных устройств, Soft-protection и др.). Здесь же рассмотрены типовые потенциально опасные действия и процедуры пользователей корпоративных информационных сетей.

В ***пятой главе*** рассматриваются основные проблемы кибершпионажа, кибер-разведки и киберконтрразведки: классификация, способы, объекты, основные источники угроз, цели, задачи и методы работы «профессионалов». В рамках отдельного параграфа рассмотрены основные особенности применения методов стратегической кибер-разведки как эффективного способа управления рисками. На основании представленного материала сформулированы специфические требования к подготовке нового поколения специалистов по информационной и кибербезопасности.

Рассмотрена организационная структура, основные функции, цели и задачи главного управления киберконтрразведки США – мирового лидера в этом направлении киберпротивостояния. Для корпоративных специалистов по кибербезопасности могут представить практический интерес приведенные в этом разделе типовые ежегодные отчеты главного управления о киберугрозах.

На конкретных примерах здесь также продемонстрирован тот факт, что расследование кибератак сегодня превратилось как в высоко прибыльный бизнес, так и в важный инструмент политической борьбы. Понятно, что решать задачи кибер-разведки и тем более киберконтрразведки «вручную» уже становится невозможным даже с помощью «талантливых личностей». Поэтому здесь детально рассмотрены как коммерческие (приобретаемые за «большие деньги»), так и некоммерческие (бесплатные open sourse) автоматизированные программно-аппаратные платформы:

в частности – практические особенности автоматизации этих процессов с помощью наиболее популярной в среде специалистов Threat Intelligence Platform: основные этапы алгоритма реализации, стандартный цикл процесса контрразведки и др.

Шестая глава посвящена важным теоретическим и практическим особенностям решения всегда актуальной задачи обеспечения кибербезопасности конечных точек инфраструктурных систем. Конечные точки – рабочие станции, серверы, ноутбуки и даже корпоративные мобильные телефоны сегодня для злоумышленников в большинстве случаев являются достаточно простыми и популярными «точками проникновения», что повышает значимость контроля за ними со стороны служб кибербезопасности.

Остроту проблемы усугубляет тот очевидный для экспертов факт, что изощренные целевые атаки все чаще применяют сочетание распространенных угроз, уязвимостей нулевого дня, уникальных нестандартных схем вообще без использования вредоносного программного обеспечения, «бесфайловых» методов и т.п.

Присутствующие сегодня в инфраструктурах большинства организаций платформы защиты конечных точек EPP (Endpoint Protection Peatform) отлично защищают от массовых, ранее известных угроз, но они не способны, например, определить, что поступающие предупреждения могут быть составными частями более сложной и опасной атаки, которая может повлечь за собой существенный ущерб для организации.

Здесь в качестве примера будет рассмотрено одно из наиболее эффективных «защитных» решений – это платформы типа EDR (Endpoint Detection and Response), которые должны автоматически взаимосвязываться с предыдущим поколением EPP.

В этой главе более детально будут рассмотрены тенденции развития киберугроз, направленных именно на конечные точки (в том числе бесфайловых filless-атак), а также технические характеристики и особенности эксплуатации таких основных платформ EDR-решений, как Gamet, Forresher, The Radicati Group.

Седьмая глава посвящена более детальному рассмотрению основных направлений обеспечения кибербезопасности. Напомним, что наиболее часто используемое общее определение кибербезопасности – это действия стратегического характера, направленные на защиту информации и коммуникаций при помощи ряда передовых инструментов, политик и процессов. Учитывая постоянно усложняющийся ландшафт киберугроз, направления, концепции, методы также совершенствуются, реагируя на изменение видов и характера возникающих все новых киберугроз.

Но если такое направление, как «пентест», достаточно широко освещается в научно-технической печати и в социальных сетях (Codeby и др.), то, например, редтайммингу и блютайммингу здесь уделяется гораздо меньше внимания, хотя методы RedTeam и BlueTeam появились намного раньше пентеста. Еще древние китайские императоры использовали такой метод: для того чтобы организовать наилучшую защиту от противника, нужно разнообразными методами самим атаковать собственные войска, чтобы не только найти «слабые места» в обороне, которые затем можно было бы защитить лучше, но и тренировать атакующие навыки своих воинов.

В начале главы приведены базовые определения основных терминов кибербезопасности, особенности организации редтайминга, блютайминга и других «разноцветных» команд, концепции и сценарии «цветного» противостояния,

особенности организации «киберучений» – имитации целевых атак как метода оценки безопасности.

Подробно рассмотрено относительно новое и стремительно развивающееся направление обеспечения кибербезопасности – «охота за угрозами» (Theat Huating) как проактивный метод киберзащиты. Представлен анализ как концепции этого метода, так и наиболее часто используемых программно-аппаратных инструментов.

Здесь же рассматривается и наиболее популярная у специалистов по кибербезопасности база знаний MITRE ATT&CK – парадигма построения, описания типовых проектов, ее использующих.

Завершает главу раздел, посвященный SIEM как важному элементу в стандартной архитектуре современной киберзащиты: цели, задачи основных и дополнительных функций, сравнительные характеристики наиболее популярных SIEM. Особое внимание уделено корреляции как важному процессу сопоставления событий и логов. Рассмотрены принципы построения и примеры «магического квадранта» Gartnet.

Восьмая глава посвящена вопросам обеспечения кибербезопасности современных критических инфраструктур. Здесь детально рассмотрены основные тенденции развития и особенности реализации на практике процессов цифровизации современных промышленных инфраструктур, включая анализ причин и следствий эволюции парадигмы информационной безопасности современного промышленного производства.

Основное внимание в этой главе уделено анализу основных угроз для электроэнергетических структур, наиболее известным уязвимостям промышленных информационно-коммуникационных систем, а также различным эффективным методикам оценки рисков безопасности в таких электроэнергетических системах. Детально рассматриваются конкретные типовые сценарии процессов анализа так называемых рейтингов рисков для электроэнергетических систем, а также наиболее эффективные международные стандарты и методы, направленные на уменьшение величин их (рисков) численных значений.

Большая часть материалов этой главы посвящена описанию нормативно-технической базы обеспечения кибербезопасности энергетических структур ведущих мировых индустриально развитых стран. В частности, здесь детально рассмотрены стандарты авторитетного американского общества приборостроителей (ISA), международной организации по стандартизации в области промышленной безопасности (ISO), стандарты национального института стандартов и технологий (NIST), специальные публикации NIST 800, руководство по обеспечению безопасности промышленных систем управления (KS), руководство по управлению рисками для информационно-телекоммуникационных систем (NIST 800-30), руководство по обработке инцидентов в сфере компьютерной безопасности (NIST 800-61), наиболее интересные стандарты Североамериканской корпорации по надежности электроснабжения (NERC), а также – национальная стратегия по защите киберпространства в США (DHS).

Заключительная ***девятая глава*** посвящена вопросам обеспечения безопасности элементно-компонентной базы (ЭКБ), используемой в аппаратной части АСУТП объектов топливно-энергетического комплекса (ТЭК).

Во вступительной части главы показаны причины эволюции классической «пирамиды безопасности» от «пирамиды происшествий» Дюпона до «пирамиды кибербезопасности», краеугольным камнем которой и является ЭКБ. Здесь также приведена классификация, механизмы активации, способы внедрения аппаратных троянов в микросхемы, приведены основные методы их выявления. Детально рассмотрены основные положения современной технологии обеспечения безопасности каналов поставки ЭКБ для систем и объектов критических инфраструктур.

Правильная организация защиты секретной информации от несанкционированного доступа – важный компонент кибербезопасности. Поэтому здесь в качестве примера приведен краткий сравнительный анализ принципов и форм защиты секретной информации в Министерствах энергетики и обороны США.

Таким образом, в систематизированных материалах девяти глав авторы попытались представить читателям подробную информацию по достаточно широкому кругу основных способов и путей обеспечения кибербезопасности как рядовых пользователей, так и современных критических инфраструктур.

Однако необходимо учитывать тот очевидный факт, что на момент выхода этой книги кибератаки становятся все более сложными, все более «скрытыми». То, что называют в СМИ термином *«киберпреступность»*, становится чрезвычайно прибыльным *бизнесом*. Хотя среди киберзлоумышленников все еще можно встретить немногих и любителей, сегодня в основном это профессионалы высшего уровня со специализированной подготовкой и огромными финансовыми и материальными ресурсами, которые они получают от определенных компаний или даже от государственных структур. Поэтому очень важно, чтобы противостоящие им специалисты по кибербезопасности были хотя бы на одном уровне (а желательно – выше) с современными киберпреступниками.

Авторы надеются, что предоставленные в этой книге обобщенные и систематизированные материалы позволят читателю более глубоко вникнуть в проблемы кибербезопасности и использовать хотя бы часть из них в своей профессиональной деятельности.

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.