Кто роет яму, сам упадет в нее, и кто ставит сеть, сам будет уловлен ею.

(Книга Премудрости Иисуса, сына Сирахова. XXVII, 29)

«На самом деле, цель энциклопедии – собрать знания, рассеянные по свету, привести их в систему, понятную для людей ныне живущих, и передать тем, кто придет после нас, с тем, чтобы труд предшествующих веков не стал бесполезным для веков последующих, и чтобы наши потомки, обогащенные знаниями, стали добрее и счастливее, и чтобы мы не канули в вечность, не сумев послужить грядущим поколениям...»

Дени Дидро

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.