ОБ АВТОРЕ

Баланов Антон Николаевич имеет большой опыт руководства и консультирования в сфере ИТ-технологий. Работал топ-менеджером в крупных компаниях — таких, как Industrial and Commercial Bank of China (КНР), Caravan portal (ОАЭ), Банк ВТБ, Сбербанк России, VK; руководил разработками сервиса Gosuslugi.ru. Имеет степень MBA IT (CIA) и сертификации Microsoft, CompTIA, ISACA, PMI, SHRM, IIBA, HRCI, ISO, Six Sigma (Master Black Belt). Преподавал в следующих вузах и учебных центрах: Российском университете дружбы народов, СберУниверситете, Институте бизнеса и делового администрирования и Центре подготовки руководителей и команд цифровой трансформации (на базе Высшей школы государственного управления РАНХиГС). Автор десятков книг и научно-практических публикаций в профессиональных изданиях. Является советником Российской академии естественных наук.

Широкая эрудиция и глубокие профессиональные компетенции автора в сфере ИТ-технологий позволили ему создать книжную серию «Айтишный университет», один из выпусков которой находится перед вами.

ОГЛАВЛЕНИЕ

Глава 1. Введение в кибербезопасность 10
Введение 10
Определение кибербезопасности и ее роль в современном мире 11
Ключевые понятия и термины в кибербезопасности 13
История развития кибербезопасности и важные моменты 17
Заключение 19

Глава 2. Угрозы и атаки в киберпространстве 21
Введение 21
Основные виды угроз и атак в киберпространстве 22
Известные случаи успешных кибератак и их последствия 24
Анализ трендов и эволюции угроз в современной кибербезопасности 26
Заключение 28

Глава 3. Защита информации и технологии 30
Введение 30
Методы и технологии защиты информации 31
Криптография и шифрование данных 33
Проактивные меры защиты: системы обнаружения вторжений, брандмауэры и прочие 35
Заключение 37

Глава 4. Правовые и регуляторные аспекты кибербезопасности 39
Введение 39
Правовые и регуляторные нормы в области кибербезопасности 40
Законы и политики в сфере кибербезопасности 42
Международное сотрудничество и стандарты в кибербезопасности 43
Заключение 46

Глава 5. Управление инцидентами и реагирование 48
Введение 48
Процесс управления инцидентами в кибербезопасности 49
Методы реагирования на инциденты и минимизации ущерба 51
Восстановление после инцидента и принятие предосторожностей 54
Заключение 57

Глава 6. Сетевая безопасность и защита периметра 59
Введение 59
Защита сетей и сетевая безопасность 60
Проектирование безопасных сетей и защита периметра 63
Идентификация и аутентификация пользователей и устройств 66
Заключение 68

Глава 7. Защита приложений и данных 70
Введение 70
Защита веб-приложений и баз данных 71
Методы обнаружения и предотвращения атак на приложения 73
Резервное копирование и восстановление данных 76
Заключение 79

Глава 8. Безопасность мобильных устройств и приложений 81
Введение 81
Угрозы и уязвимости мобильных устройств и приложений 82
Методы защиты мобильных устройств и данных 84
Управление мобильными устройствами и политики безопасности 87
Заключение 91

Глава 9. Социальная инженерия и человеческий фактор 93
Введение 93
Понимание социальной инженерии и ее влияния на безопасность 94
Обучение и осведомленность сотрудников по вопросам безопасности 96
Проактивные меры по предотвращению атак, основанных на социальной инженерии 99
Заключение 103

Глава 10. Будущее кибербезопасности и вызовы 105
Введение 105
Тенденции и прогнозы развития кибербезопасности 106
Новые технологии и инновации в сфере кибербезопасности 108
Вызовы и вызовы безопасности в современном информационном мире 111
Заключение 114

ГЛАВА 1

ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ

ВВЕДЕНИЕ

Глава 1 посвящена введению в кибербезопасность — область, которая играет важную роль в современном мире. В данной главе мы рассмотрим определение кибербезопасности и ее значимость, а также ознакомимся с ключевыми понятиями и терминами, используемыми в этой области. Также мы ознакомимся с историей развития кибербезопасности и выделим важные моменты, которые сформировали ее сегодняшний облик.

В современном информационном обществе кибербезопасность становится все более важной и актуальной. С развитием информационных технологий и цифровизации нашей жизни возникают новые угрозы и вызовы, связанные с безопасностью данных, систем и сетей. Кибербезопасность занимается защитой информации и обеспечением безопасности в сетевом пространстве.

В рамках этой главы мы познакомимся с основными понятиями и терминами, которые широко используются в кибербезопасности. Это поможет нам лучше понять технические и организационные аспекты безопасности в информационных системах. Мы также изучим историю развития кибербезопасности, отследим важные моменты и события, которые привели к ее становлению и развитию в настоящее время.

Цель данной главы состоит в том, чтобы дать вам общее представление о кибербезопасности, понять ее значение и роль в современном мире. Вы будете ознакомлены с основными терминами и понятиями, чтобы иметь возможность в дальнейшем более глубоко изучать и применять знания в области кибербезопасности.

Далее приступим к рассмотрению основных аспектов и принципов кибербезопасности, чтобы обеспечить безопасность в информационных системах и эффективно противостоять возникающим угрозам.

ОПРЕДЕЛЕНИЕ КИБЕРБЕЗОПАСНОСТИ И ЕЕ РОЛЬ В СОВРЕМЕННОМ МИРЕ

Кибербезопасность — это область знаний и практик, которая охватывает меры и механизмы для защиты компьютерных систем, сетей, данных и информации от угроз, кибератак и несанкционированного доступа. Роль кибербезопасности в современном мире становится все более важной, поскольку с развитием информационных технологий и Интернета возрастает количество киберугроз и киберпреступлений.

Кибербезопасность играет роль в различных сферах нашей жизни, включая

1. *Бизнес и коммерцию*. Кибербезопасность является важным фактором для защиты бизнес-информации, финансовых транзакций и клиентских данных. Нарушение безопасности данных может привести к финансовым потерям, утечкам конфиденциальной информации и негативному влиянию на репутацию компании.

2. *Государственная безопасность*. Кибератаки на государственные инфраструктуры, системы коммуникации и важные государственные данные могут представлять серьезную угрозу национальной безопасности. Кибербезопасность включает защиту государственных сетей и информационных систем от внешних и внутренних угроз.

3. *Личная безопасность*. В современном цифровом мире мы все более зависимы от компьютеров, мобильных устройств и Интернета. Кибербезопасность включает защиту личных данных, паролей, финансовой информации и обеспечение безопасного использования онлайн-сервисов.

4. *Критическая инфраструктура*. Кибербезопасность является неотъемлемой частью защиты критической инфраструк-

туры, такой как энергетические системы, транспортные сети, здравоохранение и другие системы, которые критически важны для функционирования общества. Атаки на эти системы могут иметь серьезные последствия и нанести значительный ущерб.

Теперь рассмотрим примеры кибербезопасности в современном мире.

Пример 1. Атака на крупную компанию

В 2017 году компания Equifax, одно из крупнейших агентств по кредитным отчетам в США, подверглась массовому взлому, в результате которого были скомпрометированы личные данные около 147 миллионов клиентов. Эта атака привела к серьезным последствиям, включая финансовые убытки и повреждение репутации компании.

Пример 2. Распространение вредоносных программ

В 2017 году вирус-вымогатель WannaCry атаковал компьютерные системы по всему миру, зашифровывая данные и требуя выкуп за их восстановление. Эта атака затронула тысячи организаций, включая государственные учреждения и медицинские учреждения, и причинила значительные ущербы.

Пример 3. Фишинг и мошенничество

Фишинговые атаки являются распространенной угрозой в онлайн-мире. Киберпреступники могут отправлять фальшивые электронные письма, притворяясь организациями или банками, с целью получить личные данные и финансовую информацию от пользователей. Это может привести к краже личных средств или идентифичности.

Таблица 1.1

Роль кибербезопасности в современном мире

Сфера	***Роль кибербезопасности***
Бизнес и коммерция	Защита бизнес-информации, финансовых транзакций, клиентских данных и репутации компании

Сфера	***Роль кибербезопасности***
Государственная безопасность	Защита государственных сетей, информационных систем и национальной безопасности
Личная безопасность	Защита личных данных, паролей, финансовой информации и обеспечение безопасности в сети
Критическая инфраструктура	Защита критической инфраструктуры, такой как энергетические и транспортные системы

Кибербезопасность играет критическую роль в современном мире, обеспечивая защиту информации, сетей и систем от киберугроз и киберпреступлений. Эффективные меры по кибербезопасности включают использование современных технологий защиты, обучение пользователей, регулярное обновление программного обеспечения и мониторинг сетевой активности.

КЛЮЧЕВЫЕ ПОНЯТИЯ И ТЕРМИНЫ В КИБЕРБЕЗОПАСНОСТИ

Кибербезопасность — это область, связанная с защитой компьютерных систем, сетей и данных от угроз, связанных с информационной безопасностью. В кибербезопасности существуют различные ключевые понятия и термины, которые важно понимать и использовать для эффективного обеспечения безопасности информации. Ниже представлены некоторые из наиболее важных понятий и терминов, используемых в кибербезопасности.

I. Основные понятия

1. Угроза (Threat).

Определение. Возможность нарушения безопасности или наступления неблагоприятного события, которое может привести к потенциальным ущербам.

Пример. Вредоносное программное обеспечение, хакерские атаки, фишинг, компьютерные вирусы и т. д.

2. Уязвимость (Vulnerability).

Определение. Слабость или недостаток в компьютерной системе, сети или процессе, который может быть использован злоумышленником для атаки или несанкционированного доступа.

Пример. Отсутствие обновлений программного обеспечения, слабые пароли, недостаточные права доступа и т. д.

3. Атака (Attack).

Определение. Целенаправленное действие или попытка использования уязвимостей в системе или сети с целью нарушения безопасности, кражи данных или причинения ущерба.

Пример. DDOS-атаки, взломы, внедрение вредоносного кода, фишинг и т. д.

4. Идентификация (Identification).

Определение. Процесс определения личности или подлинности субъекта (пользователя, устройства и т. д.) с использованием уникальных идентификаторов или аутентификационных данных.

Пример. Логины, пароли, биометрические данные, сертификаты и т. д.

5. Аутентификация (Authentication).

Определение. Процесс проверки и подтверждения идентификации субъекта с использованием аутентификационных механизмов и данных.

Пример. Ввод пароля, использование двухфакторной аутентификации, смарт-карты и т. д.

6. Авторизация (Authorization).

Определение. Процесс предоставления определенных прав доступа и разрешений субъекту на основе его идентификации и аутентификации.

Пример. Назначение ролей и разрешений, определение уровней доступа и т. д.

7. Шифрование (Encryption).

Определение. Процесс преобразования информации в зашифрованный формат с использованием криптографических алгоритмов для обеспечения конфиденциальности и целостности данных.

Пример. Использование SSL/TLS протокола для защиты передачи данных по сети, шифрование файлов и т. д.

II. Термины и понятия в кибербезопасности

1. Фаервол (Firewall).

Определение. Устройство или программное обеспечение, которое контролирует трафик в сети, фильтрует пакеты данных и обеспечивает защиту от несанкционированного доступа.

Пример. Сетевые файерволы, периметральные файерволы, межсетевые экраны и т. д.

2. Инцидент безопасности (Security Incident).

Определение. Нарушение безопасности или событие, которое может представлять реальную или потенциальную угрозу для информационных ресурсов, систем или сетей.

Пример. Утечка данных, взлом системы, вирусная атака и т.д.

3. Управление уязвимостями (Vulnerability Management).

Определение. Процесс и методология для обнаружения, анализа, оценки и устранения уязвимостей в системах и сетях с целью повышения безопасности.

Пример. Сканирование уязвимостей, исправление уязвимостей, патч-управление и т. д.

4. Сетевая безопасность (Network Security).

Определение. Область кибербезопасности, относящаяся к защите компьютерных сетей от несанкционированного доступа, атак и утечки данных.

Пример. Межсетевые экраны, виртуальные частные сети (VPN), обнаружение вторжений (IDS/IPS) и т. д.

5. Социальная инженерия (Social Engineering).

Определение. Манипулятивные методы и техники, используемые злоумышленниками для обмана людей и получения несанкционированного доступа или информации.

Пример. Фишинг, подделка электронных писем, мошенничество по телефону и т. д.

Таблица 1.2

Примеры ключевых понятий и терминов в кибербезопасности

Понятие	***Определение***	***Пример***
Угроза	Возможность нарушения безопасности или наступления неблагоприятного события	Вредоносное программное обеспечение, хакерские атаки, фишинг
Уязвимость	Слабость или недостаток в компьютерной системе, сети или процессе	Отсутствие обновлений программного обеспечения, слабые пароли
Атака	Целенаправленное действие или попытка использования уязвимостей	DDOS-атаки, взломы, фишинг
Идентификация	Процесс определения личности или подлинности субъекта	Логины, пароли, биометрические данные
Аутентификация	Процесс проверки и подтверждения идентификации субъекта	Ввод пароля, двухфакторная аутентификация
Авторизация	Процесс предоставления прав доступа и разрешений субъекту	Назначение ролей и разрешений
Шифрование	Процесс преобразования информации в зашифрованный формат	Использование SSL/TLS протокола для защиты передачи данных
Фаервол	Устройство или программное обеспечение, контролирующее трафик в сети	Сетевые файерволы, периметральные файерволы
Инцидент безопасности	Нарушение безопасности или событие, представляющее угрозу для информационных ресурсов	Утечка данных, взлом системы

Понятие	***Определение***	***Пример***
Управление уязвимостями	Процесс обнаружения и устранения уязвимостей в системах и сетях	Сканирование уязвимостей, исправление уязвимостей
Сетевая безопасность	Область кибербезопасности, связанная с защитой компьютерных сетей	Межсетевые экраны, VPN, IDS/IPS
Социальная инженерия	Манипулятивные методы для обмана людей и получения несанкционированного доступа или информации	Фишинг, подделка электронных писем

Важно иметь хорошее понимание этих понятий и уметь применять соответствующие меры и технологии для обеспечения безопасности информации и защиты от киберугроз.

ИСТОРИЯ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ И ВАЖНЫЕ МОМЕНТЫ

История развития кибербезопасности является важным аспектом современного информационного общества. Начиная с появления первых компьютеров, развитие кибербезопасности прошло длительный путь, соответствуя развитию технологий и изменению угроз. Рассмотрим основные этапы и важные моменты в истории развития кибербезопасности.

Этап 1. Ранние годы компьютеров (1940–1950 годы)

В начале развития компьютеров вопросы безопасности не привлекали большого внимания, так как компьютеры использовались преимущественно в научных и военных целях. Однако уже в эти ранние годы были известны некоторые случаи несанкционированного доступа к компьютерам и нарушения безопасности.

Пример.

В 1943 году американские военные обнаружили, что некий Генрик Куттербек взломал систему управления ракетами и получил доступ к конфиденциальной информации.

Этап 2. Появление Интернета и вирусы (1960–1980 годы)

С развитием Интернета и распространением компьютерных сетей стали появляться новые угрозы безопасности. В этот период появились первые компьютерные вирусы, которые могли наносить серьезный ущерб компьютерным системам.

Пример.

В 1971 году инженер Роберт Томас создал первый компьютерный вирус Creeper, который распространялся через ARPANET (предшественник Интернета) и отображал на зараженных компьютерах сообщение «I'm the creeper, catch me if you can!» («Я — крипер [ползун, проныра], поймай меня, если сможешь!»).

Этап 3. Профессиональное развитие кибербезопасности (1990–2000 годы)

В 1990-е годы с появлением коммерческого Интернета и распространением компьютеров в повседневной жизни стала возрастать важность кибербезопасности. В этот период были созданы первые специализированные организации и стандарты, направленные на обеспечение безопасности информационных систем.

Пример.

В 1998 году был создан Координационный центр по реагированию на компьютерные чрезвычайные ситуации (CERT), который занимается координацией и анализом уязвимостей в компьютерных системах и разработкой методов и инструментов по предотвращению и реагированию на инциденты безопасности.

Этап 4. Развитие современных угроз и защитных технологий (2000 год — настоящее время)

В современной эпохе кибербезопасности наблюдается постоянное развитие новых угроз и соответствующих методов защиты. Киберпреступность, хакерские атаки, кибершпионаж и другие формы атак стали все более сложными и масштабными. Вместе с тем, разрабатываются и совершенствуются инструменты и методы киберзащиты.

Пример.

В 2017 году компания WannaCry стала известна во всем мире после крупномасштабной атаки с использованием вы-