

Краткий обзор содержания

Введение	28
РАЗДЕЛ 1. ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ	33
Глава 1. Что такое кибербезопасность	35
Глава 2. Знакомство с распространенными кибератаками	51
Глава 3. «Плохие» парни, против которых вы должны защищаться	80
РАЗДЕЛ 2. УЛУЧШЕНИЕ ВАШЕЙ ЛИЧНОЙ БЕЗОПАСНОСТИ	101
Глава 4. Оценка текущего уровня кибербезопасности	103
Глава 5. Укрепление физической безопасности	125
Глава 6. Вопросы кибербезопасности при работе из дома	137
РАЗДЕЛ 3. ЗАЩИЩАЕМ СЕБЯ ОТ СЕБЯ	147
Глава 7. Защита ваших аккаунтов	149
Глава 8. Пароли	168
Глава 9. Противостояние атакам социальной инженерии	186
РАЗДЕЛ 4. КИБЕРБЕЗОПАСНОСТЬ ДЛЯ ПРЕДПРИЯТИЙ, ОРГАНИЗАЦИЙ И ПРАВИТЕЛЬСТВА	209
Глава 10. Защита вашего малого бизнеса	211
Глава 11. Кибербезопасность и крупный бизнес	237
РАЗДЕЛ 5. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ БЕЗОПАСНОСТИ (ВОПРОС НЕ «ЕСЛИ», А «КОГДА»)	253
Глава 12. Идентификация утечки безопасности	255
Глава 13. Восстановление после нарушения безопасности	275

РАЗДЕЛ 6. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ	293
Глава 14. Резервное копирование	295
Глава 15. Сброс устройства к заводским настройкам	324
Глава 16. Восстановление из резервных копий	334
РАЗДЕЛ 7. СМОТРИМ В СВЕТЛОЕ БУДУЩЕЕ	357
Глава 17. Построение карьеры в сфере кибербезопасности	359
Глава 18. Новые технологии – новые угрозы	373
РАЗДЕЛ 8. ПУТЬ ДЕСЯТИ	385
Глава 19. Десять способов прокачать киберзащиту без лишних затрат	387
Глава 20. Чему нас научили крупнейшие киберинциденты	393
Глава 21. Безопасные способы использования публичного Wi-Fi	400
Алфавитный указатель	404
Об авторе	411
Посвящение	412
Благодарности автора	413

Расширенное оглавление

Введение	28
О книге	29
Глупые предположения	31
Иконки, используемые в этой книге	31
Дополнительные материалы	32
Куда идти дальше	32

РАЗДЕЛ 1. ВВЕДЕНИЕ В КИБЕРБЕЗОПАСНОСТЬ

Глава 1. Что такое кибербезопасность	35
Кибербезопасность может восприниматься людьми по-разному	35
Кибербезопасность не стоит на месте	36
Технологический прогресс	37
Социальные изменения	41
Экономические изменения	42
Политические изменения	43
Анализ рисков, которые устраняет кибербезопасность	48
Цель кибербезопасности – триада CIA	49
С точки зрения обычного человека	50
Глава 2. Знакомство с распространенными кибератаками	51
Атаки, наносящие ущерб	51
Атаки отказа в обслуживании (Denial-of-Service attack)	52
Распределенные атаки отказа в обслуживании (Distributed Denial-of-Service attack)	52

Ботнеты и зомби	55
Атаки на уничтожение данных	55
Это действительно ты? Имитация	55
Фишинг	56
Целевой фишинг	56
СЕО-фрод	57
СМС-фишинг	57
Манипуляции с данными	58
Голосовой фишинг	58
Фарминг	58
«Уэйлинг»	58
Атака «человек посередине»	59
Перехват данных	59
Похищение данных	60
Похищение персональных данных	61
Похищение корпоративных данных	61
Утечка данных	62
Скомпрометированные учетные данные	62
Принудительное нарушение политик безопасности	63
Компьютерные вирусы	63
Цифровые бомбы, которые проникают на ваши устройства, – вредоносное ПО	63
«Червь»	64
«Троянский конь»	64
Вирус-вымогатель	64
«Лжеантивирус»	65
Шпионское ПО	66
Майнеры криптовалют	66
Рекламное ПО	67
Вредоносное ПО смешанного типа	67
Вредоносное ПО «нулевого дня»	67
Поддельное вредоносное ПО на компьютерах	68
Поддельное вредоносное ПО на мобильных телефонах	68

Поддельные уведомления о продлении подписки на защиту устройства	68
Атака с использованием зараженных веб-сайтов	69
Заражение сетевой инфраструктуры	69
Вредоносная реклама	70
Автоматическая загрузка ПО	71
Похищение паролей	72
Использование недостатков обслуживания	73
«Продвинутые» атаки	73
Оппортунистические атаки	74
Целевые атаки	74
Смешанные (оппортунистические и целевые) атаки	75
Некоторые примеры технических атак	76
Руткиты	76
Атаки методом перебора	76
Инъекционные атаки	77
Межсайтовый скриптинг	77
SQL-инъекция	77
Перехват сессии	78
Атаки с использованием некорректных URL	78
Атаки переполнения буфера	79
 Глава 3. «Плохие» парни, против которых вы должны защищаться	 80
«Плохие» парни и «хорошие» парни – это относительные термины ..	81
Типы «плохих» парней	82
Скрипт-кидди	82
Дети, которые на самом деле уже не дети	83
Террористические и другие преступные группировки	83
«Государственные» хакеры	84
Промышленный шпионаж	85
Преступники	85
Хактивисты	86
Киберпреступники и их «цветные шляпы»	87

Как киберпреступники монетизируют свои действия	88
Прямое финансовое мошенничество	88
Косвенное финансовое мошенничество	89
Прибыль от незаконной торговли ценными бумагами	89
Программы-вымогатели	91
Криптомайнеры	91
Не все опасности исходят от злоумышленников:	
борьба с незлонамеренными угрозами	92
Человеческий фактор	92
Люди как ахиллесова пята в кибербезопасности	92
Социальная инженерия	93
Внешние катастрофы	94
Защита от этих хакеров	99

РАЗДЕЛ 2. УЛУЧШЕНИЕ ВАШЕЙ ЛИЧНОЙ БЕЗОПАСНОСТИ 101

Глава 4. Оценка текущего уровня кибербезопасности 103

Не будьте Ахиллесом: как определить, насколько реальна угроза	103
Ваши домашние компьютеры	104
Ваши мобильные устройства	104
Ваши устройства интернета вещей (IoT)	105
Определение рисков	106
Ваше сетевое оборудование	106
Ваша рабочая среда	106
Защищаемся от выявленных уязвимостей	108
Защита периметра	108
Брандмауэр/маршрутизатор	109
Программное обеспечение безопасности	111
Ваши физические компьютеры и другие конечные устройства	111
Резервное копирование	112
Обнаружение	112
Реагирование	112

Восстановление	112
Улучшение	113
Программное обеспечение	113
Оценка текущих мер безопасности	113
Оборудование	114
Страхование	115
Конфиденциальность 101	116
Образование	116
Думайте, прежде чем делиться информацией	116
Думайте, прежде чем публиковать	117
Основные советы по защите конфиденциальности в Сети	118
Безопасный онлайн-банкинг	120
Как безопасно пользоваться «умными» устройствами	122
Цифровая валюта	123
Глава 5. Укрепление физической безопасности	125
Почему физическая безопасность настолько важна?	126
Проведение инвентаризации	126
Стационарные устройства	128
Мобильные устройства	129
Поиск уязвимых данных	130
Создание и выполнение плана по обеспечению физической безопасности	131
Реализация физической безопасности	132
Безопасность мобильных устройств	134
Осознание того, что инсайдеры представляют самые большие риски	135
Глава 6. Вопросы кибербезопасности при работе из дома	137
Проблемы сетевой безопасности	137
Проблемы безопасности устройств	140
Безопасность местоположения	141
Подглядывание	142
Подслушивание	142

Кража	142
Человеческий фактор	143
Не допускайте попадания личных вещей в поле зрения камеры	143
Безопасность видеоконференций	143
Защите видеоконференции от несанкционированных посетителей	144
Проблемы социальной инженерии	145
Нормативные вопросы	146

РАЗДЕЛ 3. ЗАЩИЩАЕМ СЕБЯ ОТ СЕБЯ 147

Глава 7. Защита ваших аккаунтов 149

Осознание того, что вы являетесь целью	149
Защита внешних учетных записей	150
Защита данных, связанных с различными аккаунтами пользователей	151
Ведите дела только с проверенными людьми	152
Используйте официальные приложения и сайты	152
Не устанавливайте программное обеспечение из сторонних репозиториев	152
Не рутинуйте свой смартфон	153
Не предоставляйте ненужную конфиденциальную информацию	153
Используйте только проверенные платежные системы	153
Используйте одноразовые виртуальные платежные карты	154
Мониторьте свои аккаунты	155
Сообщайте о подозрительной активности как можно скорее	155
Применяйте правильную стратегию для своих паролей	155
Используйте многофакторную аутентификацию	155
Выходите из учетной записи после завершения использования	157
Используйте только свой собственный компьютер или смартфон	157

Используйте защитный пароль на своем компьютере	157
Используйте отдельный компьютер для конфиденциальных задач	157
Используйте отдельный браузер для конфиденциальных веб-задач	158
Обеспечьте защиту всех устройств с доступом в Сеть	158
Регулярно обновляйте свои устройства	158
Не используйте публичные Wi-Fi-сети для работы с конфиденциальными данными	159
Никогда не используйте общественный Wi-Fi в местах повышенного риска	159
Доступ к своим аккаунтам только в безопасных местах	159
Используйте безопасные устройства	160
Установите соответствующие ограничения на устройства	160
Используйте оповещения	160
Периодически проверяйте списки устройств с доступом к учетным записям	161
Проверьте информацию о последнем входе в систему	161
Соответствующим образом реагируйте на любые предупреждения о мошенничестве	161
Никогда не отправляйте конфиденциальную информацию по незашифрованному соединению	161
Остерегайтесь атак с использованием социальной инженерии	162
Установите голосовые пароли	163
Защитите номер своего мобильного телефона	163
Не нажимайте на ссылки в электронных письмах или текстовых сообщениях	164
Защита данных в веб-службах, которыми вы пользуетесь	164
Защита данных в веб-службах, которыми вы не пользуетесь	165
Не подключайте к своему компьютеру или смартфону неизвестные устройства	166
Глава 8. Пароли	168
Пароли: основная форма аутентификации	168
Избегайте простых паролей	169

Мысли по выбору пароля	170
Легко угадываемые личные пароли	170
Не все сложные пароли одинаково полезны	171
Разные уровни конфиденциальности	172
Немного о конфиденциальности паролей	172
Иногда пароли можно повторять	173
Рассмотрите возможность использования менеджера паролей	174
Создаем надежный и запоминающийся пароль	176
Когда следует менять пароль?	176
Изменение паролей после утечки	178
Передача паролей посторонним людям	179
Хранение паролей	179
Передача паролей	180
Хранение паролей для наследников	180
Хранение простых паролей	180
Биометрическая аутентификация	181
Исследуем альтернативы паролям	181
SMS-авторизация	183
Одноразовые генерируемые пароли	184
Авторизация с помощью аппаратного токена	184
Авторизация с помощью USB-устройств	185

Глава 9. Противостояние атакам социальной

инженерии	186
Не стоит всецело доверять технологиям	186
Типы атак в социальной инженерии	187
Шесть уязвимостей человека, которые используются в социальной инженерии	191
Чем не стоит делиться в социальных сетях?	192
Распорядок дня и планы поездок	193
Финансовая информация	194
Личная информация	194
Информация о ваших детях	195
Информация о ваших питомцах	196

Информация о работе	196
Возможные проблемы с цифровой безопасностью	196
Преступления и мелкие правонарушения	196
Медицинская или юридическая информация	197
Информация о местоположении	197
Дата рождения	197
Утечка данных при участии в вирусных трендах	198
Выявление поддельных учетных записей в социальных сетях	198
Ваши «грехи»	198
Фотографии	199
Подтверждение пользователя	200
Список друзей или общих знакомых	200
Посты и публикации в социальных сетях	200
Количество связей	201
Род занятий и местоположение	201
Похожие люди	202
Дублирующий контакт	202
Контактные данные	202
Премиум-статус	202
Список лайков в социальных сетях	203
Активность в группах	203
Относительно равномерное заполнение профиля	203
Действия человека	204
Имя-клише	204
Недостаточное количество контактной информации	204
Компетенции	205
Орфография	205
Возраст аккаунта	205
Подозрительная карьера или жизненный путь	205
Профессиональный уровень или статус знаменитости	206
Использование фальшивой информации	207
Использование защитного программного обеспечения	208
Кибергигиена против социальной инженерии	208

РАЗДЕЛ 4. КИБЕРБЕЗОПАСНОСТЬ ДЛЯ ПРЕДПРИЯТИЙ, ОРГАНИЗАЦИЙ И ПРАВИТЕЛЬСТВА 209

Глава 10. Защита вашего малого бизнеса 211

Назначение ответственного за безопасность 211

Контроль за сотрудниками 212

 Поощрение сотрудников 213

 Разделите уровни доступа 213

 Создавайте отдельные учетные записи 213

 Ограничьте права администраторов 214

 Ограничьте доступ к корпоративным аккаунтам 214

 Внедрение правил для сотрудников 216

 Контроль за использованием соцсетей 219

 Мониторинг сотрудников 219

Работа с удаленными сотрудниками 220

 Использование рабочих устройств и отдельных сетей 220

 Настройка виртуальной частной сети 221

 Создание стандартных протоколов связи 222

 Используйте только проверенные сетевые подключения 222

 Определите стратегию резервного копирования 223

 Будьте осторожны при выборе рабочего места 223

 Будьте особенно внимательны
 к проявлениям социальной инженерии 224

Страхование киберрисков: стоит ли рассматривать? 225

Соблюдение законов и соответствие нормативно-правовой
документации 226

 Защита персональных данных сотрудников 226

 Стандарт PCI DSS 227

 Законы о раскрытии утечек данных 228

 Общий регламент защиты данных 228

 Защита конфиденциальной медицинской
 информации HIPAA 229

 Биометрические данные 229

 Предотвращение «отмывания» денежных средств 229

Управление доступом к сети интернет	230
Международные санкции	230
Сегрегация доступа в интернет для личных устройств	230
Создание политики BYOD (Bring Your Own Device)	230
Защита входящих соединений	231
Защита от DDoS-атак	233
Используйте протокол HTTPS	234
Используйте VPN-сервисы	234
Регулярно проводите проверки на уязвимость	234
Безопасность IoT-устройств	235
Сегментация сети	235
Будьте осторожны с платежными картами	235
Защита серверов и сетевого оборудования	235
Глава 11. Кибербезопасность и крупный бизнес	237
Использование сложных технологических решений	238
Управление нестандартными системами	238
Закон Сарбейнса – Оксли (SOX)	239
Планирование непрерывности бизнеса и восстановление после сбоев	239
Обратимся к законодательству	239
Строгие требования PCI DSS	241
Раскрытие конфиденциальных данных публичных компаний	241
Раскрытие информации о кибератаках	242
Законодательные акты в различных областях	242
Фидуциарные (доверительные) обязанности	242
«Глубокие карманы»	243
«Глубокие карманы» и их страхование	244
Внимание к сотрудникам, подрядчикам и партнерам	244
Внутренние конфликты	245
Обучение сотрудников кибербезопасности	245
Рассмотрим роль директора по информационной безопасности (CISO)	246
Репликация сред	246

Полный контроль над системами безопасности	247
Оценка эффективности системы безопасности	247
Управление человеческими рисками	247
Классификация и контроль информационных активов	248
Операционная безопасность	248
Разработка стратегии информационной безопасности	248
Управление идентификацией и доступом к данным	248
Предотвращение утечек данных	249
Борьба с мошенничеством	249
План реагирования на инциденты	250
Восстановление после аварий и обеспечение непрерывности бизнеса	250
Соответствие законности действий	250
Расследование инцидентов	250
Физическая безопасность	251
Архитектура безопасности	251
Геополитические риски	251
Контроль действий системных администраторов	252
Соответствие требованиям страхования от киберугроз	252

РАЗДЕЛ 5. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ БЕЗОПАСНОСТИ (ВОПРОС НЕ «ЕСЛИ», А «КОГДА»)

Глава 12. Идентификация утечки безопасности	255
Идентификация явных утечек	256
Программы-вымогатели	256
Взлом веб-сайтов	257
Обнаружение скрытых взломов	258
Заявление об уничтожении	258
Ваше устройство работает медленнее, чем раньше	259
Диспетчер задач не запускается	260
Редактор реестра не открывается	260
Устройство выполняет программы с задержкой	261

Устройство демонстрирует буферизацию и теряет связь	261
Настройки устройства изменились без вашего ведома	262
Устройство отправляет или получает подозрительные email ...	263
Устройство отправляет или получает странные сообщения	263
На вашем устройстве появляются новые программы, которые вы не устанавливали	263
Батарея устройства разряжается быстрее, чем раньше	264
Устройство стало нагреваться сильнее, чем раньше	264
Содержимое файлов или папок изменилось	265
Файлы пропали	265
Веб-сайты выглядят не так, как раньше	265
Настройки интернета показывают использование прокси, хотя вы его не настраивали	265
Некоторые программы перестали работать или работают неправильно	266
Защитное программное обеспечение отключено	267
Повышенный расход мобильного трафика или SMS	267
Увеличение сетевого трафика	267
Открыты необычные сетевые порты	268
Устройство часто перезагружается	268
Вы заметили неожиданные списания денег	269
Неизвестные программы запрашивают доступ	269
Внешние устройства подключаются сами по себе	270
Компьютер ведет себя так, будто им управляет кто-то другой	270
Изменился поисковый сервис, установленный по умолчанию в браузере	270
Изменился код доступа к вашему устройству	270
Появляются всплывающие окна	270
В браузере появились новые расширения	271
Изменилась домашняя страница браузера	271
Ваши письма блокируются спам-фильтрами	271
Устройство пытается зайти на сомнительные сайты	272
Необычные проблемы со связью	272