

ПЕТР ЛЕВАШОВ

КИБЕРКРЕПОСТЬ

ВСЕСТОРОННЕЕ РУКОВОДСТВО
ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ



Санкт-Петербург • Москва • Минск

2024

КРАТКОЕ СОДЕРЖАНИЕ

Введение	29
Об авторе	30
От издательства.....	32
Глава 1. Введение в компьютерную безопасность	33
Глава 2. Сетевая безопасность	66
Глава 3. Безопасность конечных точек	136
Глава 4. Управление идентификацией и доступом	188
Глава 5. Криптография и шифрование данных.....	293
Глава 6. Реагирование на инциденты и аварийное восстановление.....	352
Глава 7. Соблюдение нормативных требований и юридические вопросы.....	414
Глава 8. Передовые темы и новые технологии	484
Заключение.....	539
Список использованной литературы	540
Список ссылок	542

ОГЛАВЛЕНИЕ

Введение	29
Об авторе	30
От издательства	32
Глава 1. Введение в компьютерную безопасность	33
Обзор области компьютерной безопасности.....	33
Обзор типов угроз.....	34
Виды компьютерной безопасности.....	36
Важность управления рисками	37
Роль стандартов и лучших практик.....	37
Важность реагирования на инциденты	38
Роль сторонних поставщиков услуг безопасности	39
Эволюция компьютерной безопасности.....	40
Первые дни компьютерной безопасности	40
Рост числа киберугроз.....	41
Рост индустрии безопасности.....	41
Современное состояние компьютерной безопасности	42
Тенденции и будущие разработки в области компьютерной безопасности	43
Влияние технологических достижений на безопасность.....	44
Роль правительства и международных организаций в обеспечении компьютерной безопасности.....	44
Роль индивидуальной и корпоративной ответственности в компьютерной безопасности	45
Последствия нарушений компьютерной безопасности.....	46
Виды нарушений компьютерной безопасности	46
Финансовые последствия нарушения безопасности.....	47
Влияние на репутацию и доверие клиентов	48

Воздействие на интеллектуальную собственность и конфиденциальную информацию	48
Воздействие на национальную безопасность и критическую инфраструктуру	49
Соответствие нормативным требованиям и юридические последствия нарушений безопасности	50
Влияние нарушений безопасности на человека	51
Роль реагирования на инциденты в смягчении последствий нарушений безопасности	51
Важность проактивного подхода к компьютерной безопасности	52
Преимущества проактивного подхода к компьютерной безопасности	52
Важность регулярной оценки уязвимостей и тестирования на проникновение	53
Роль обучения сотрудников навыкам безопасности	53
Внедрение надежного плана реагирования на инциденты	54
Роль автоматизации и инструментов безопасности	55
Важность регулярного обновления программного обеспечения и управления исправлениями	56
Роль реагирования на инциденты в проактивной стратегии безопасности	57
Важность мониторинга и обнаружения угроз	57
Роль реагирования на инциденты в проактивной стратегии безопасности	58
Важность проактивного подхода в условиях современных угроз	59
Роль пользователя в компьютерной безопасности	60
Важность надежных паролей и аутентификации	60
Роль обучения и информирования пользователей	61
Влияние социальной инженерии и фишинга	62
Важность безопасного просмотра веб-страниц и электронной почты	62
Роль управления учетными записями пользователей и контроля доступа	63
Важность безопасности персональных устройств	64
Роль пользователей в реагировании на инциденты и составлении отчетов	65
Глава 2. Сетевая безопасность	66
Брандмауэры и системы обнаружения/предотвращения вторжений	66
Типы брандмауэров и случаи их использования	66
Конфигурирование брандмауэров и управление ими	67
Системы обнаружения и предотвращения вторжений	68
Внедрение и обслуживание IDPS	69
Интеграция брандмауэров и IDPS для повышения безопасности	69
Передовая практика и отраслевые стандарты в области брандмауэров и IDPS	70

Брандмауэр и IDPS в облачных и виртуализированных средах.....	71
Брандмауэр и IDPS в IoT и мобильных сетях	71
Роль брандмауэра и IDPS в реагировании на инциденты.....	72
Будущее брандмауэров и технологий IDPS	73
VPN и безопасность удаленного доступа	73
Типы VPN и случаи их использования	73
Протоколы VPN и методы шифрования	74
Конфигурирование и управление VPN.....	75
Передовые методы обеспечения безопасности VPN и отраслевые стандарты	77
VPN в облачных и виртуализированных средах.....	78
VPN для удаленного доступа и удаленной работы	79
Интеграция VPN с другими мерами безопасности	80
Будущее технологии VPN.....	80
Сегментация сети и микросегментация	82
Сегментация сети и ее преимущества.....	82
Реализация сегментации сети в физических и виртуальных средах	82
Преимущества микросегментации.....	83
Интеграция сегментации сети с другими мерами безопасности.....	84
Мониторинг и обслуживание сегментации сети.....	85
Будущее сегментации сети и технологии микросегментации.....	85
Безопасность беспроводных сетей.....	85
Понимание рисков безопасности беспроводных сетей	85
Внедрение протоколов и стандартов безопасности беспроводных сетей	86
Конфигурирование беспроводных точек доступа и контроллеров и управление ими	87
Методы шифрования и аутентификации беспроводных сетей	88
Мониторинг беспроводных сетей и реагирование на инциденты	89
Интеграция безопасности беспроводной сети с другими мерами безопасности.....	90
Лучшие методы обеспечения безопасности беспроводных сетей на предприятии	91
Будущее технологии безопасности беспроводных сетей.....	92
Мониторинг сети и поиск угроз.....	93
Введение в тему	93
Типы мониторинга сети	94
Инструменты и технологии мониторинга сети	95
Реализация мониторинга сети.....	96
Передовые методы мониторинга сети и отраслевые стандарты.....	97
Охота за угрозами	99

Мониторинг сети в облачных и виртуализированных средах	100
Автоматизация реагирования на инциденты с помощью мониторинга сети	101
Безопасность в облачных и мультиоблачных средах	102
Введение в тему	102
Типы облачных услуг и их последствия для безопасности.....	103
Внедрение средств контроля безопасности в облаке	103
Управление безопасностью облачных вычислений и их мониторинг.....	105
Лучшие методы обеспечения безопасности облачных вычислений на предприятии	106
Стратегии безопасности мультиоблачных сред	106
Интеграция облачной безопасности с локальными мерами безопасности	108
Безопасность облачных вычислений	109
Соблюдение нормативно-правового соответствия и нормативные аспекты в облаке	110
Роль шифрования в сетевой безопасности	111
Введение в шифрование и его значение для сетевой безопасности.....	111
Типы алгоритмов шифрования и случаи их применения.....	111
Реализация шифрования в протоколах сетевого взаимодействия.....	112
Шифрование данных в состоянии покоя	114
Управление ключами шифрования и их администрирование	115
Нормативные требования к шифрованию и соответствие им	117
Будущее технологии шифрования в сетевой безопасности.....	118
Лучшие методы шифрования на предприятии	119
Обеспечение безопасности устройств интернета вещей в Сети.....	120
Введение в безопасность IoT.....	120
Идентификация и инвентаризация устройств IoT в сети	121
Защита коммуникаций и данных устройств IoT	122
Управление безопасностью устройств IoT и мониторинг	123
Лучшие методы обеспечения безопасности устройств IoT на предприятии	124
Будущее технологий безопасности IoT.....	125
Соответствие нормативным требованиям и нормативные аспекты безопасности устройств IoT	127
Сетевая безопасность и соответствие нормативным требованиям и требованиям регуляторов	127
Введение в тему	127
Требования к сетевой безопасности в соответствии с отраслевыми нормами	128
Соответствие нормативным требованиям и нормативно-правовые аспекты для облачных и мультиоблачных сред.....	129

Роль шифрования в обеспечении соответствия нормативным и регулирующим требованиям.....	130
Правила сетевой безопасности и конфиденциальности данных.....	131
Нормативные требования к безопасности устройств IoT и соответствие им	132
Передовые методы достижения и поддержания соответствия требованиям сетевой безопасности.....	133
Будущее соответствия нормативным требованиям к сетевой безопасности.....	134
Лучшие методы реагирования на инциденты при нарушениях сетевой безопасности.....	134
Глава 3. Безопасность конечных точек	136
Введение в тему	136
Основа безопасности конечных точек и их роль в сетевой безопасности	136
Определение различных типов конечных устройств и их уникальных потребностей в безопасности.....	137
Важность защиты конечных точек в ходе предотвращения кибератак и утечки данных.....	137
Эволюция технологии защиты конечных точек и ее влияние на безопасность сети	138
Передовые методы внедрения и поддержания безопасности конечных точек на предприятии	139
Будущее технологии защиты конечных точек и ее роль в сетевой безопасности.....	140
Типы решений для обеспечения безопасности конечных точек и случаи их использования.....	141
Антивирусное программное обеспечение.....	141
Брандмауэры.....	142
Управление мобильными устройствами.....	142
Платформа защиты конечных точек	143
Полное шифрование диска.....	144
Управление исправлениями.....	144
Контроль доступа к сети.....	145
Контроль приложений и составление белых списков	146
Системы обнаружения и предотвращения вторжений на базе хоста.....	147
Аналитика поведения пользователей	148
Облачная защита конечных точек.....	149
Биометрическая аутентификация.....	150
Виртуальная частная сеть	150
Решения для удаленного доступа.....	151
Управление информацией о безопасности и событиях.....	152
Аварийное восстановление и планирование непрерывности бизнеса	153

Внедрение антивирусного программного обеспечения и брандмауэров на конечных устройствах	154
Выбор правильного антивирусного программного обеспечения для организации	154
Настройка и развертывание антивирусного программного обеспечения на конечных устройствах	155
Управление антивирусным ПО и его обновление.....	156
Ограничения антивирусного программного обеспечения	156
Внедрение брандмауэров на конечных устройствах	157
Настройка параметров брандмауэра для конечных устройств.....	158
Управление программным обеспечением брандмауэра и его обновление.....	159
Ограничения брандмауэров	159
Лучшие практики совместного использования антивирусного ПО и брандмауэров для защиты конечных точек.....	160
Устранение неполадок и решение проблем с антивирусным ПО и брандмауэрами на конечных устройствах	161
Управление безопасностью конечных точек и ее мониторинг.....	162
Аудит и отчетность по безопасности конечных точек.....	162
Мониторинг безопасности конечных точек в режиме реального времени.....	163
Реагирование на инциденты и нарушения безопасности на конечных устройствах	164
Управление политиками и настройками безопасности на конечных устройствах	164
Обновление ПО и устройств для обеспечения безопасности конечных точек	165
Обучение и подготовка пользователей по вопросам безопасности	166
Постоянная оценка и совершенствование мер обеспечения безопасности конечных точек	167
Передовые методы обеспечения безопасности конечных точек на предприятии.....	168
Разработка и обеспечение соблюдения политик и процедур безопасности.....	168
Внедрение многоуровневых мер безопасности	168
Регулярный мониторинг и оценка безопасности конечных точек	169
Поддержание ПО и устройств в актуальном состоянии.....	169
Подготовка и обучение пользователей.....	170
Регулярная оценка рисков	170
Наличие плана аварийного восстановления и обеспечения непрерывности бизнеса.....	171
Постоянная переоценка и совершенствование мер безопасности.....	172
Создание протоколов реагирования на инциденты и нарушения.....	172
Регулярный аудит и составление отчетов о состоянии безопасности	173

Будущее технологий защиты конечных точек.....	173
Искусственный интеллект и машинное обучение.....	173
Облачная защита конечных точек.....	174
Безопасность интернета вещей.....	175
Обнаружение угроз на основе поведенческих факторов.....	175
Биометрическая аутентификация.....	176
Сегментация сети.....	176
Квантово-устойчивая защита.....	176
Безопасность виртуализации и контейнеризации.....	177
Модели безопасности с нулевым доверием.....	178
Автоматизация и оркестровка решений по обеспечению безопасности конечных точек.....	179
Нормативные требования безопасности конечных точек и соответствие им.....	179
Соблюдение требований HIPAA.....	179
Соответствие стандарту PCI DSS.....	180
Соблюдение SOX.....	180
Соответствие требованиям GLBA.....	181
Соблюдение требований FISMA.....	181
Соблюдение требований GDPR.....	182
Соответствие стандарту ISO 27001.....	183
Соответствие требованиям NIST.....	183
Реагирование на инциденты и восстановление после нарушений безопасности конечных точек.....	184
Создание группы реагирования на инциденты.....	184
Разработка плана реагирования на инциденты.....	184
Выявление и локализация нарушения.....	185
Устранение причины инцидента.....	185
Восстановление после инцидента.....	185
Выполнение обзора и анализа после инцидента.....	186
Обновление процедур реагирования на инциденты и восстановления.....	187
Уведомление затронутых сторон и регулирующих органов.....	187
Глава 4. Управление идентификацией и доступом.....	188
Введение в тему.....	188
Обзор управления идентификацией и доступом.....	188
Важность управления идентификацией и доступом в обеспечении безопасности конечных точек.....	188
Ключевые понятия и терминология.....	189
Рамки и стандарты управления идентификацией и доступом.....	190
Преимущества и проблемы управления идентификацией и доступом.....	191

Реальные примеры управления идентификацией и доступом	192
Ключевые компоненты системы управления идентификацией и доступом	193
Лучшие практики управления идентификацией и доступом	193
Пароли и политика в отношении них	194
Введение в тему	194
Важность надежных паролей	195
Типы паролей	195
Показатели стойкости паролей	196
Распространенные ловушки с паролями	197
Создание и обеспечение соблюдения политик паролей	198
Лучшие методы обеспечения безопасности паролей	198
Управление паролями в гибридной среде	199
Внедрение многофакторной аутентификации	200
Инструменты и технологии управления паролями	201
Обучение и тренинги в области политики отношения к паролям	202
Мониторинг и аудит использования паролей	202
Реагирование на инциденты и восстановление после утечек, связанных с паролями	203
Соответствие требованиям и нормативные аспекты политики паролей	204
Будущее безопасности паролей	204
Двухфакторная аутентификация	205
Введение в тему	205
Типы двухфакторной аутентификации	206
Преимущества двухфакторной аутентификации	207
Внедрение двухфакторной аутентификации	207
Лучшие практики двухфакторной аутентификации	208
Управление двухфакторной аутентификацией в гибридной среде	209
Инструменты и технологии двухфакторной аутентификации	210
Обучение и тренинги по двухфакторной аутентификации	210
Мониторинг и аудит использования двухфакторной аутентификации	211
Реагирование на инциденты и восстановление после нарушений, связанных с 2FA	212
Соответствие двухфакторной аутентификации нормативным требованиям и ее нормативные аспекты	213
Будущее двухфакторной аутентификации	213
Управление доступом на основе ролей	214
Введение в тему	214
Роли и разрешения	215
Реализация контроля доступа на основе ролей	215
Управление контролем доступа на основе ролей в гибридной среде	216

Инструменты и технологии управления доступом на основе ролей	217
Обучение и тренинги по управлению доступом на основе ролей.....	218
Мониторинг и аудит использования RBAC	218
Реагирование на инциденты и восстановление после нарушений, связанных с контролем доступа на основе ролей	219
Соответствие нормативным требованиям и нормативные соображения для контроля доступа на основе ролей.....	219
Будущее ролевого контроля доступа	220
Единый вход и федеративная идентификация.....	221
Введение в тему	221
Подробнее о едином входе и федеративной идентификации.....	221
Реализация единого входа и федеративной идентификации.....	222
Управление единым входом и федеративной идентификацией в гибридной среде	223
Инструменты и технологии единого входа и федеративной идентификации	224
Обучение и тренинги по единому входу и федеративной идентификации	225
Мониторинг и аудит использования единого входа и федеративной идентификаций	226
Реагирование на инциденты и восстановление после нарушений, связанных с SSO и FI.....	226
Нормативные требования для SSO и FI и соответствие им	227
Будущее единого входа и федеративной идентификации.....	228
Управление идентификацией и доступом в облаке	228
Введение в тему	228
Подробнее об облачном управлении идентификацией и доступом.....	229
Реализация управления идентификацией и доступом в облаке	229
Управление идентификацией и доступом в гибридной облачной среде	230
Инструменты и технологии управления идентификацией и доступом в облаке	231
Обучение и тренинги по облачному управлению идентификацией и доступом	232
Мониторинг и аудит использования облачного управления идентификацией и доступом.....	232
Реагирование на инциденты и восстановление после нарушений, связанных с управлением идентификацией и доступом в облаке.....	233
Нормативные требования для облачного управления идентификацией и доступом и соответствие им.....	234
Будущее облачного управления идентификацией и доступом	235
Управление идентификационными данными и администрирование	235
Введение в тему	235
Подробнее об управлении идентификационными данными и администрировании.....	236

Реализация управления идентификационными данными и администрирования.....	237
Управление идентификационными данными и администрирование в гибридной среде	237
Инструменты и технологии управления идентификацией и администрирования.....	238
Обучение по вопросам управления идентификацией и администрирования.....	239
Мониторинг и аудит использования средств управления идентификационными данными и администрирования.....	239
Реагирование на инциденты и восстановление при нарушениях, связанных с управлением идентификационными данными и администрированием	240
Соответствие нормативным требованиям к управлению идентификационными данными и администрированию.....	241
Будущее управления идентификацией и администрирования	241
Соответствие нормативным требованиям и нормативные аспекты управления идентификацией и доступом	242
Введение в тему	242
Основные положения и стандарты	243
Планирование и реализация соответствия	244
Мониторинг и аудит соответствия	244
Отчетность и устранение несоответствий	245
Соответствие нормативным требованиям и системы управления идентификацией и доступом.....	246
Соблюдение нормативных требований и управление идентификацией и доступом в облаке.....	247
Соответствие нормативным требованиям и управление идентификацией и администрирование	247
Соответствие нормативным требованиям и управление идентификацией и доступом в гибридной среде	248
Соответствие нормативным требованиям. Инструменты и технологии управления идентификацией и доступом	249
Управление учетными записями пользователей и доступом	251
Введение в тему	251
Создание учетных записей пользователей и управление ими	251
Назначение доступа пользователей и управление им.....	251
Управление предоставлением и удалением учетных записей пользователей	252
Управление аутентификацией и авторизацией пользователей	253
Управление паролями пользователей и многофакторная аутентификация	254
Управление сессиями пользователей и контроль доступа	254
Управление учетными записями пользователей и доступом.	
Аудит и отчетность	255

Управление безопасностью и соответствием требованиям безопасности учетных записей пользователей и доступа	256
Управление учетными записями пользователей и доступом в гибридной среде	256
Управление учетными записями пользователей и доступом. Инструменты и технологии	257
Управление учетными записями пользователей и доступом. Обучение.....	258
Управление учетными записями пользователей и доступом. Реагирование на инциденты и восстановление после них.....	259
Управление учетными записями пользователей и доступом. Соответствие требованиям и нормативные аспекты.....	260
Будущее управления учетными записями и доступом пользователей.....	261
Управление привилегированным доступом	262
Введение в тему	262
Идентификация привилегированных пользователей и управление ими	262
Реализация контроля привилегированного доступа.....	264
Мониторинг и аудит привилегированного доступа.....	264
Управление привилегированным доступом в гибридной среде	265
Инструменты и технологии для управления привилегированным доступом.....	266
Соответствие нормативным требованиям и нормативные соображения в отношении привилегированного доступа	267
Реагирование на инциденты и восстановление в случае привилегированного доступа	267
Будущее управления привилегированным доступом	268
Автоматизация управления идентификацией и доступом	269
Введение в тему	269
Автоматизация предоставления пользователям учетных записей и доступа	270
Автоматизация аутентификации и авторизации	271
Автоматизация контроля доступа и управления сессиями.....	271
Автоматизация аудита и отчетности.....	272
Автоматизация соблюдения нормативно-правовых требований.....	272
Автоматизация реагирования на инциденты и восстановления	273
Инструменты и технологии для автоматизации управления идентификацией и доступом.....	274
Внедрение автоматизированных решений по идентификации и доступу в гибридной среде и управление ими.....	275
Будущее автоматизации управления идентификацией и доступом	275
Мониторинг и аудит доступа пользователей	276
Введение в тему	276
Идентификация и отслеживание действий пользователя	276
Реализация и настройка журналов аудита.....	277

Анализ и интерпретация данных аудита	277
Реагирование на подозрительные действия и инциденты безопасности.....	278
Соответствие нормативным требованиям и нормативные соображения для мониторинга и аудита доступа пользователей	278
Инструменты и технологии для мониторинга и аудита доступа пользователей ...	279
Управление мониторингом и аудитом доступа пользователей в гибридной среде	279
Будущее мониторинга и аудита доступа пользователей.....	280
Реагирование на инциденты и восстановление после нарушений в области управления идентификацией и доступом	281
Планирование инцидентов, связанных с управлением идентификацией и доступом	281
Выявление и расследование нарушений	282
Сдерживание и ликвидация угрозы	282
Восстановление и возобновление нормальной работы	283
Обзор ситуации после инцидента и извлеченные уроки	283
Нормативные требования к реагированию на инциденты и соответствие им.....	284
Управление реагированием на инциденты в гибридной среде	284
Будущие тенденции в реагировании на инциденты и восстановлении после нарушений в области управления идентификацией и доступом.....	285
Будущее технологии управления идентификацией и доступом.....	286
Достижения в области искусственного интеллекта и машинного обучения.....	286
Расширение применения биометрической аутентификации	287
Достижения в области управления идентификацией и доступом	287
Появление управления идентификацией и доступом как услуги	288
Интеграция управления идентификацией и доступом с интернетом вещей.....	288
Роль блокчейна в управлении идентификацией и доступом	289
Влияние квантовых вычислений на управление идентификацией и доступом	289
Разработка стандартов и лучших практик для управления идентификацией и доступом	290
Сдвиг в сторону моделей безопасности с нулевым доверием.....	291
Роль управления идентификацией и доступом в кибербезопасности	291
Глава 5. Криптография и шифрование данных.....	293
Введение в тему	293
Обзор криптографии и шифрования данных	294
Типы шифрования	294
Цифровые подписи и аутентификация	295
Управление ключами и генерация ключей	295
Стандарты шифрования и лучшие практики.....	296

Методы симметричного шифрования	297
Основные техники симметричного шифрования.....	297
Передовые методы симметричного шифрования.....	298
Сравнение алгоритмов симметричного шифрования.....	299
Управление ключами симметричного шифрования.....	299
Симметричное шифрование в действии. Приложения и примеры применения в реальном мире.....	300
Стандарты и лучшие практики симметричного шифрования.....	301
Проблемы и ограничения симметричного шифрования	302
Симметричное шифрование и квантовые вычисления.....	302
Симметричное шифрование и будущее криптографии.....	303
Асимметричное шифрование и инфраструктура открытых ключей.....	304
Введение в тему	304
Генерация ключей в асимметричном шифровании и управление ими	305
Цифровые подписи и аутентификация с асимметричным шифрованием	306
Инфраструктура открытых ключей и управление сертификатами	306
Приложения в реальном мире и примеры использования асимметричного шифрования	307
Стандарты и лучшие практики асимметричного шифрования.....	308
Проблемы и ограничения асимметричного шифрования	309
Асимметричное шифрование и квантовые вычисления.....	310
Будущее асимметричного шифрования и инфраструктуры открытых ключей.....	310
Цифровые подписи и аутентификация.....	311
Введение в тему	311
Алгоритмы и методы цифровой подписи	311
Управление ключами и центрами сертификации в цифровых подписях	312
Приложения и примеры использования цифровых подписей в реальном мире.....	312
Стандарты цифровой подписи и лучшие практики.....	313
Проблемы и ограничения цифровых подписей	314
Цифровые подписи и квантовые вычисления.....	315
Будущее цифровых подписей и аутентификации.....	315
Шифрование в сетевых коммуникациях.....	316
Введение в тему	316
Симметричное и асимметричное шифрование в сетевых коммуникациях.....	316
Безопасность транспортного уровня и уровень защищенных сокетов	317
Виртуальные частные сети и туннелирование	318
Шифрование электронной почты и безопасный обмен сообщениями	318
Шифрование в беспроводных и мобильных сетевых коммуникациях.....	319
Шифрование в облачных и распределенных сетевых коммуникациях.....	320

Стандарты шифрования и лучшие практики для сетевых коммуникаций	321
Проблемы и ограничения шифрования в сетевых коммуникациях	322
Шифрование и квантовые вычисления в сетевых коммуникациях	323
Будущее шифрования в сетевых коммуникациях.....	323
Нормативные требования к шифрованию данных и соответствие им	324
Введение в тему	324
Стандарты и правила шифрования данных.....	325
Соответствие нормативным требованиям и шифрование данных в здравоохранении	325
Соответствие нормативным требованиям и шифрование данных в сфере финансовых услуг	326
Соответствие требованиям и шифрование данных в государственном секторе ...	327
Соответствие нормативным требованиям и шифрование данных в розничной торговле.....	328
Соответствие нормативным требованиям и шифрование данных в технологической отрасли.....	329
Соответствие нормативным требованиям и шифрование данных в энергетике и коммунальном хозяйстве.....	330
Соответствие требованиям и шифрование данных в транспортной отрасли.....	331
Проблемы и ограничения, связанные с соблюдением нормативно-правовых требований к шифрованию данных.....	332
Будущие нормативные требования к шифрованию данных	332
Инструменты и технологии для шифрования данных	333
Введение в тему	333
Инструменты и решения для шифрования программного обеспечения	333
Аппаратные шифровальные устройства и приборы	334
Услуги облачного шифрования и защиты данных	335
Системы управления ключами и шифрованием.....	336
SDK и API для шифрования.....	336
Новые инструменты и технологии для шифрования данных	337
Проблемы и ограничения инструментов и технологий для шифрования данных	337
Будущее инструментов и технологий для шифрования данных	338
Управление шифрованием в гибридной среде	339
Введение в тему	339
Шифрование в гибридных облачных средах	339
Шифрование в гибридных локальных и облачных средах	340
Шифрование в гибридных мультиоблачных средах	341
Управление ключами для гибридного шифрования.....	341
Системы управления шифрованием для гибридных сред.....	342



Проблемы и ограничения управления шифрованием в гибридной среде	343
Будущее управления шифрованием в гибридной среде	344
Будущее криптографии и шифрования данных	344
Достижения в сфере алгоритмов шифрования	344
Квантовые вычисления и криптография	345
Искусственный интеллект и шифрование	345
Блокчейн и криптография	346
Роль правительства в криптографии	347
Влияние шифрования на кибербезопасность	348
Будущее соблюдения нормативных требований и регулирования	348
Будущее средств и технологий шифрования	349
Будущее шифрования в гибридных средах	350
Заключение и перспективы на будущее	351
Глава 6. Реагирование на инциденты и аварийное восстановление	352
Введение в тему	352
Обзор реагирования на инциденты и аварийного восстановления	352
Важность реагирования на инциденты и планирования аварийного восстановления	352
Ключевые компоненты планирования реагирования на инциденты и аварийного восстановления	353
Типы инцидентов и катастроф, на случай которых необходимо планировать действия	354
Процесс реагирования на инциденты и аварийного восстановления	354
Роль групп реагирования на инциденты и аварийного восстановления	356
Установление целей реагирования на инциденты и аварийного восстановления	356
Терминология реагирования на инциденты и аварийного восстановления	357
Разработка плана реагирования на инциденты	358
Определение масштаба и целей плана реагирования на инциденты	358
Выявление и оценка потенциальных инцидентов и угроз	358
Разработка процедур и протоколов реагирования на инциденты	358
Доведение до сведения заинтересованных сторон плана реагирования на инциденты и их обучение	359
Тестирование и поддержание плана реагирования на инциденты	359
Регулярный пересмотр и обновление плана реагирования на инциденты	360
Планирование непрерывности бизнеса и аварийное восстановление	361
Введение в тему	361
Определение критических бизнес-процессов	361
Разработка анализа воздействия на бизнес	362

Разработка стратегий восстановления	363
Создание плана обеспечения непрерывности бизнеса	364
Тестирование и обучение по плану обеспечения непрерывности бизнеса	365
Поддержание и обновление плана непрерывности бизнеса	365
Реализация плана аварийного восстановления	366
Тестирование плана аварийного восстановления и обучение.....	366
Поддержание и обновление плана аварийного восстановления.....	366
Команды и роли в реагировании на инциденты	367
Создание группы реагирования на инциденты	367
Определение ролей и обязанностей команды реагирования на инциденты.....	368
Сбор группы реагирования на инциденты	369
Обучение и тренировки группы реагирования на инциденты.....	369
Координация действий с внешними группами реагирования на инциденты	370
Поддержание готовности группы реагирования на инциденты.....	371
Типы инцидентов и угроз безопасности	371
Кибернетические атаки.....	371
Вредоносные программы и Ransomware.....	372
Фишинг и социальная инженерия.....	372
Инсайдерские угрозы	373
Инциденты, связанные с физической безопасностью	373
Стихийные бедствия и отключения электроэнергии.....	374
Атаки на цепочки поставок.....	374
IoT и угрозы операционных технологий	375
Инциденты, связанные с безопасностью облачных вычислений.....	376
Нарушения нормативно-правового соответствия и нормативных требований.....	377
Выявление инцидентов безопасности и реагирование на них.....	377
Выявление инцидентов безопасности	377
Сбор и сохранение доказательств	378
Сдерживание и ликвидация инцидента.....	379
Восстановление после инцидента	380
Общение. Документирование инцидента.....	381
Анализ после инцидента и извлечение уроков.....	382
Постоянное совершенствование возможностей реагирования на инциденты.....	383
Анализ и отчетность после инцидента	383
Анализ после инцидента.....	383
Отчетность.....	384
Извлеченные уроки	384
Непрерывное совершенствование.....	385

Стратегии и решения для аварийного восстановления.....	386
Введение в тему	386
Решения для резервного копирования и восстановления.....	386
Решения для репликации и высокой доступности	387
Облачные решения для аварийного восстановления.....	388
Тестирование и моделирование решений для аварийного восстановления	389
Внедрение и обслуживание решений по аварийному восстановлению	390
Планирование непрерывности бизнеса и аварийного восстановления.....	391
Аварийное восстановление как услуга.....	392
Гибридные решения для аварийного восстановления	392
Соответствие нормативным требованиям и нормативные соображения при аварийном восстановлении.....	393
Тестирование и постоянное совершенствование мер реагирования на инциденты и аварийного восстановления	394
Создание и тестирование планов реагирования на инциденты.....	394
Регулярные учения и тренировки по реагированию на инциденты	395
Оценка эффективности реагирования на инциденты и аварийного восстановления	396
Постоянное совершенствование процессов реагирования на инциденты и аварийного восстановления.....	396
Измерения и отчетность о результатах реагирования на инциденты и аварийного восстановления	397
Включение извлеченных уроков в планирование реагирования на инциденты и аварийного восстановления	398
Аудит и соблюдение процессов реагирования на инциденты и аварийного восстановления	398
Поддержание планов реагирования на инциденты и аварийного восстановления в актуальном состоянии	399
Проблемы и ограничения при реагировании на инциденты и аварийном восстановлении.....	400
Недостаток ресурсов.....	400
Ограниченная видимость.....	400
Недостаточная автоматизация	400
Недостаточная координация.....	401
Недостаточная стандартизация	401
Недостаточная масштабируемость	401
Недостаточная гибкость	402
Недостаточная переносимость	402
Недостаточная операционная совместимость	402
Недостаточная интеграция.....	403
Недостаточные тестирование и валидация.....	403

Недостаточные обслуживание и поддержка	404
Ограниченный бюджет и финансирование	404
Ограниченное время и давление.....	404
Недостаток знаний и навыков.....	405
Нечеткость управления и подотчетности.....	405
Недостаточно тесные коммуникация и сотрудничество.....	406
Ограниченные обратная связь и совершенствование	406
Неполное соблюдение правовых норм и регулирование.....	406
Недостаточные устойчивость и адаптивность.....	407
Будущее реагирования на инциденты и аварийного восстановления	407
Искусственный интеллект и машинное обучение в реагировании на инциденты.....	407
Предиктивная аналитика для аварийного восстановления.....	408
Реагирование на инциденты и аварийное восстановление на основе облачных технологий.....	408
Автоматизация и оркестровка реагирования на инциденты и аварийного восстановления	409
Интеграция IoT и интеллектуальных устройств для реагирования на инциденты и восстановления после катастроф.....	409
Виртуальная и дополненная реальность для обучения и моделирования реагирования на инциденты.....	410
Блокчейн для реагирования на инциденты и восстановления после катастроф.....	410
Квантовые вычисления для реагирования на инциденты и аварийного восстановления	410
Расширенное шифрование и кибербезопасность для реагирования на инциденты и аварийного восстановления	411
Мониторинг в режиме реального времени для реагирования на инциденты и аварийного восстановления.....	411
Совместное и скоординированное реагирование на инциденты и восстановление после стихийных бедствий.....	412
Этические и социальные последствия применения технологий реагирования на инциденты и восстановления после катастроф	413
Глава 7. Соблюдение нормативных требований и юридические вопросы.....	414
Обзор правовых и нормативных требований к компьютерной безопасности	414
Введение в тему	414
Общие сведения о HIPAA	414
Общие сведения о PCI DSS.....	415
Общие сведения о GDPR.....	415
Передовой опыт в области обеспечения соответствия	416
Исполнение законов и штрафные санкции	417

Отраслевые нормативные акты.....	417
Международные аспекты соответствия	418
Необходимо следить за изменениями в нормативных актах	418
Юридические обязательства и риски	419
Аудит и тестирование на соответствие нормативным требованиям.....	419
Соответствие требованиям HIPAA. Руководящие принципы и лучшие практики	419
Введение в тему	419
Правила и стандарты HIPAA	420
Соблюдение требований HIPAA организациями и их деловыми партнерами	421
Анализ и управление рисками HIPAA.....	421
Стандарты безопасности HIPAA и технические меры защиты	422
Стандарты конфиденциальности HIPAA и административные гарантии	422
Обучение и тренинги по соблюдению требований HIPAA	423
Аудит и обеспечение соблюдения требований HIPAA	424
Соблюдение требований HIPAA и реагирование на инциденты	425
Соблюдение требований HIPAA в облаке и ходе удаленной работы	425
Соответствие требованиям HIPAA для мобильных и IoT-устройств	426
Соблюдение требований HIPAA в ходе работы со сторонними поставщиками услуг.....	427
Соблюдение требований HIPAA и планирование непрерывности бизнеса.....	428
Соблюдение требований HIPAA и международные аспекты.....	428
Соответствие стандарту PCI DSS. Стандарты и процедуры обеспечения соответствия	429
Введение в тему	429
Стандарты и требования PCI DSS.....	430
Соответствие стандарту PCI DSS для продавцов и поставщиков услуг.....	430
Вопросники самооценки PCI DSS и отчеты о соответствии.....	431
Стандарты безопасности PCI DSS и технические меры защиты.....	432
Соответствие стандарту PCI DSS и реагирование на инциденты.....	432
Соответствие стандарту PCI DSS в облаке и удаленная работа	433
Соответствие требованиям PCI DSS для мобильных и IoT-устройств.....	434
Соответствие требованиям PCI DSS при работе со сторонними поставщиками услуг.....	434
Соответствие стандарту PCI DSS и планирование непрерывности бизнеса.....	435
Международные аспекты соответствия PCI DSS	435
Аудит и обеспечение соблюдения требований PCI DSS.....	436
Общий регламент по защите данных: требования и соблюдение	437
Введение в тему	437
Правила и стандарты, предусмотренные GDPR.....	437

Соответствие требованиям GDPR	438
Оценки воздействия на защиту данных GDPR	439
GDPR. Права субъектов данных	439
Стандарты и технические меры безопасности GDPR	440
Стандарты конфиденциальности GDPR и административные меры	441
Обучение и тренинги по соблюдению требований GDPR	441
Аудит и обеспечение соблюдения требований GDPR	442
Соблюдение требований GDPR и реагирование на инциденты	442
Соблюдение требований GDPR в облаке и в ходе удаленной работы	443
Соответствие требованиям GDPR для мобильных и IoT-устройств	444
Соблюдение требований GDPR в ходе работы со сторонними поставщиками услуг	444
Соответствие требованиям GDPR и планирование непрерывности бизнеса	445
Международные аспекты соблюдения GDPR	446
Другие ключевые нормативные акты и стандарты в области компьютерной безопасности	446
Соответствие требованиям SOX. Стандарты и процедуры	446
NIST Cybersecurity Framework (CSF). Обзор и внедрение	447
Соответствие требованиям FISMA. Руководящие принципы и лучшие практики	449
CIS Critical Security Controls. Стандарты и внедрение	450
ISO/IEC 27001. Системы управления информационной безопасностью	450
CSA Cloud Security Alliance. Стандарты и соответствие	451
Соответствие требованиям GLBA. Защита финансовых данных	452
Соблюдение требований FERPA. Защита документов об образовании	452
Соответствие требованиям SOC 2. Стандарты для сервисных организаций	453
Соблюдение закона Сарбейнса – Оксли. Стандарты и процедуры	454
Исполнение и штрафы за несоблюдение требований	455
Гражданские и уголовные наказания	455
Административные штрафы и санкции	455
Отзыв лицензий и разрешений	456
Судебные запреты и запретительные приказы	456
Растрата и возмещение прибыли	457
Лишение государственных контрактов и грантов	457
Негативная реклама и репутационный ущерб	458
Тюремное заключение и лишение свободы	458
Корпоративная и персональная ответственность	459
Сроки давности и исковая давность	459
Юридическая ответственность и риски в сфере компьютерной безопасности	460
Юридическая ответственность за утечку данных	460

Обязательства, связанные с киберпреступностью и компьютерным мошенничеством.....	460
Ответственность за нарушение прав интеллектуальной собственности	461
Обязательства в области конфиденциальности и защиты данных.....	461
Обязательства, связанные с непропорциональным использованием сетей и систем.....	462
Ответственность за обработку данных третьими сторонами и облачные услуги.....	462
Ответственность за инсайдерские угрозы и непропорциональные действия сотрудников	463
Ответственность за халатность и несоблюдение нормативных требований	464
Ответственность за утрату или повреждение данных и систем	464
Обязательства, связанные с ответственностью за качество продукции и дефектное программное обеспечение.....	464
Ответственность за международные и межюрисдикционные проблемы в области компьютерной безопасности.....	465
Обязательства по киберстрахованию и возмещению ущерба.....	465
Ответственность за кибервымогательство и атаки Ransomware.....	466
Ответственность за кибертерроризм и кибератаки, спонсируемые государством.....	467
Передовой опыт в области соблюдения нормативных требований и управления рисками.....	467
Разработка комплексного плана обеспечения соответствия.....	467
Внедрение строгих мер контроля доступа и аутентификации	468
Обеспечение конфиденциальности и защиты данных	469
Регулярный аудит безопасности и оценка уязвимостей.....	469
Создание планов реагирования на инциденты и аварийного восстановления.....	469
Обеспечение регулярного обновления и исправления ПО	470
Обучение сотрудников по вопросам осведомленности о безопасности и тренинги.....	470
Поддержание культуры осведомленности о безопасности	471
Внедрение стратегий шифрования и резервного копирования данных.....	471
Получение и поддержание страхового покрытия киберстрахования	472
Киберстрахование и снижение рисков.....	472
Покрытие и лимиты киберстрахования.....	472
Оценка киберрисков вашей организации.....	472
Оценка и выбор полиса киберстрахования.....	473
Включение киберстрахования в план управления рисками.....	474
Внедрение дополнительных мер по снижению рисков	474
Регулярный пересмотр и обновление политики киберстрахования	475
Обеспечение соблюдения требований и условий политики.....	475

Составление претензии и навигация по процессу рассмотрения претензий.....	476
Роль киберстрахования в плане реагирования на инциденты кибербезопасности.....	477
Аудит и соответствие требованиям процессов реагирования на инциденты и аварийного восстановления.....	477
Планирование и подготовка к аудиту реагирования на инциденты.....	477
Оценка текущих процессов реагирования на инциденты.....	478
Оценка команд и ресурсов реагирования на инциденты.....	478
Выявление слабых мест и пробелов в планировании реагирования на инциденты.....	479
Внедрение лучших практик реагирования на инциденты.....	479
Обеспечение соответствия отраслевым стандартам и нормам.....	480
Регулярное тестирование и поддержание процедур реагирования на инциденты.....	481
Оценка эффективности аудита реагирования на инциденты.....	481
Документирование и передача результатов аудита реагирования на инциденты.....	481
Постоянное совершенствование процессов реагирования на инциденты и аварийного восстановления.....	482
Глава 8. Передовые темы и новые технологии.....	484
Искусственный интеллект в кибербезопасности.....	484
Введение в тему.....	484
Применение искусственного интеллекта в операциях по обеспечению безопасности.....	484
Повышение эффективности обнаружения угроз и реагирования на них с помощью искусственного интеллекта.....	485
Оценка рисков и управление ими на основе ИИ.....	485
Будущее искусственного интеллекта в кибербезопасности.....	486
Вызовы и ограничения ИИ в сфере безопасности.....	486
Обеспечение этичности и прозрачности ИИ в сфере безопасности.....	487
Лучшие практики внедрения ИИ в кибербезопасность.....	488
Пересечение ИИ и МО в кибербезопасности.....	489
Автоматизация операций по кибербезопасности на основе искусственного интеллекта.....	490
Квантовые вычисления и кибербезопасность.....	491
Введение в тему.....	491
Последствия квантовых вычислений для кибербезопасности.....	491
Защита от угроз квантовых вычислений.....	492
Квантовое распределение ключей и криптография.....	492
Будущее квантовых вычислений и их влияние на безопасность.....	493

Лучшие практики подготовки к использованию квантовых вычислений в области кибербезопасности.....	493
Пересечение квантовых вычислений и искусственного интеллекта в кибербезопасности	494
Преодоление трудностей при внедрении квантовых вычислений в операции по обеспечению безопасности.....	495
Опережая события: исследования и разработки в области квантовых вычислений и кибербезопасности.....	495
Безопасность блокчейна. Угрозы и решения	496
Введение в тему	496
Угрозы безопасности блокчейна.....	496
Защита конфиденциальности и приватности транзакций блокчейна	497
Обеспечение целостности и доступности данных блокчейна	497
Лучшие практики по внедрению безопасности блокчейна.....	498
Новые тенденции и инновации в области безопасности блокчейна.....	499
Решение проблем, связанных с масштабированием безопасности блокчейна	500
Интеграция безопасности блокчейна в операции по обеспечению безопасности предприятия	501
Опережая события: исследования и разработки в области безопасности блокчейна.....	502
Новые тенденции в области киберугроз и уязвимостей	503
Развивающийся ландшафт киберугроз.....	503
Новые тенденции в атаках с помощью вредоносного ПО и Ransomware	503
Расширение IoT и рост количества связанных с ним уязвимостей	504
Влияние облачных вычислений на кибербезопасность	504
Появление 5G и его последствия для безопасности.....	505
Угроза атак с использованием искусственного интеллекта.....	505
Влияние социальной инженерии и человеческих уязвимостей.....	506
Будущее киберугроз и уязвимостей.....	507
Лучшие практики для опережения новых угроз.....	508
Будущее кибербезопасности. Предсказания и прогнозы	508
Будущее разведки угроз и охоты на угрозы.....	508
Влияние краевых вычислений на кибербезопасность	509
Роль искусственного интеллекта в операциях по кибербезопасности	510
Будущее безопасности блокчейна.....	510
Изменчивый ландшафт киберугроз	511
Интеграция кибербезопасности и физической безопасности.....	511
Будущее образования и обучения в области кибербезопасности.....	512
Растущая важность кибербезопасности в интернете вещей.....	513
Расширение правил и стандартов кибербезопасности	513
Будущее инвестиций и инноваций в области кибербезопасности	514

Инновации в области киберзащиты и управления рисками	514
Усиление безопасности сетей и конечных точек.....	514
Эволюция управления идентификацией и доступом	515
Внедрение решений для обнаружения угроз и реагирования на них.....	516
Развитие технологии обмана	516
Интеграция больших данных и аналитики в киберзащиту	517
Появление блокчейна в сфере кибербезопасности.....	517
Внедрение облачной безопасности и защиты данных	518
Будущее искусственного интеллекта в киберзащите.....	519
Важность непрерывной оценки и снижения рисков	520
Роль сотрудничества и обмена информацией в киберзащите.....	520
Навигация по сложному ландшафту современных киберугроз	521
Современные постоянные угрозы.....	521
Обнаружение уязвимостей нулевого дня и реагирование на них	521
Навигация в мире кибератак, спонсируемых государством	522
Защита от современных вредоносных программ и программ-вымогателей.....	522
Защита от передовых методов социальной инженерии	523
Противодействие угрозе инсайдерских атак.....	523
Решение проблем безопасности мобильных устройств и IoT.....	524
Влияние облачных вычислений на современные киберугрозы.....	525
Опережая новые угрозы и тактические приемы	525
Передовые методы борьбы с современными киберугрозами	526
Влияние новых технологий на кибербезопасность.....	527
Последствия внедрения сетей 5G для кибербезопасности	527
Риски, связанные с искусственным интеллектом и машинным обучением	528
Проблемы обеспечения безопасности интернета вещей.....	528
Будущее технологии блокчейна и ее безопасность.....	529
Достижения в области краевых вычислений и их последствия для безопасности	529
Роль виртуальной и дополненной реальности в кибербезопасности	530
Важность кибербезопасности в новых технологиях, таких как самоуправляющиеся автомобили и беспилотники	531
Влияние квантовых вычислений на кибербезопасность	531
Будущее носимых технологий и их проблемы безопасности.....	532
Последствия внедрения передовой робототехники и автоматизации для кибербезопасности	532
Лучшие практики для опережающего развития в области кибербезопасности	533
Принятие проактивного подхода к кибербезопасности	533
Внедрение строгой аутентификации и контроля доступа.....	533
Поддержание программного обеспечения и систем в актуальном состоянии	534

Внедрение решений для обнаружения современных угроз и реагирования на них.....	534
Соблюдение правил и стандартов кибербезопасности.....	535
Проведение регулярных тренингов по кибербезопасности и программ повышения осведомленности.....	535
Поощрение сотрудничества и обмена информацией.....	536
Ведение комплексных планов резервного копирования и восстановления данных.....	536
Включение кибербезопасности в планирование непрерывности бизнеса.....	537
Регулярная оценка рисков кибербезопасности и управление ими.....	538
Заключение.....	539
Список использованной литературы.....	540
Список ссылок.....	542