

ВЫСШЕЕ ОБРАЗОВАНИЕ

# ЗАЩИТА ИНФОРМАЦИОННЫХ СИСТЕМ

## Кибербезопасность



А. Н. Баланов



E.LANBOOK.COM

## ОГЛАВЛЕНИЕ

<b>Введение</b> .....	<b>9</b>
<b>Глава 1. Основы кибербезопасности:</b>	
<b>история, определения, основные понятия</b> .....	<b>10</b>
1.1. Исторический контекст развития кибербезопасности.....	10
1.1.1. Первые шаги в кибербезопасности.....	10
1.1.2. Эпоха хакерства и компьютерных вирусов .....	10
1.1.3. Развитие стандартов и принципов безопасности .....	11
1.1.4. Эпоха кибератак и кибершпионажа.....	11
1.1.5. Рост кибербезопасности как профессиональной области....	11
1.2. Основные определения в области кибербезопасности .....	13
1.3. Ключевые понятия и термины .....	16
1.3.1. Аутентификация.....	17
1.3.2. Авторизация.....	17
1.3.3. Шифрование.....	17
1.3.4. Фишинг.....	18
1.3.5. Угрозы «внутреннего врага» .....	18
1.3.6. Брандмауэр.....	18
1.3.7. Zero-day уязвимость .....	19
1.3.8. Социальная инженерия .....	19
1.4. Роль государства в кибербезопасности.....	21
1.4.1. Законодательное регулирование .....	21
1.4.2. Государственные агентства и службы кибербезопасности .....	22
1.4.3. Национальные стратегии и политика кибербезопасности...	22
1.4.4. Международное сотрудничество .....	23
1.4.5. Финансирование и поддержка исследований .....	23
1.4.6. Образование и повышение квалификации .....	23
1.5. Современные вызовы и тренды .....	24
1.5.1. Увеличение объема и сложности данных .....	25
1.5.2. Распространение Интернета вещей (IoT) .....	25
1.5.3. Рост киберпреступности .....	25
1.5.4. Угрозы от государственных акторов .....	26
1.5.5. Искусственный интеллект (ИИ) и машинное обучение (МО) в кибербезопасности .....	26
1.5.6. Защита приватности и соответствие законодательству о данных .....	26

1.5.7. Расширение периметра безопасности.....	27
<b>Глава 2. Классификация угроз кибербезопасности.....</b>	<b>29</b>
2.1. Основные виды угроз для информационных систем.....	29
2.1.1. Вирусы и вредоносное ПО .....	29
2.1.2. Социальная инженерия .....	30
2.1.3. Вторжения и атаки на периметр.....	30
2.1.4. Угрозы изнутри.....	30
2.1.5. Отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS) атаки .....	30
2.1.6. Утечка данных .....	31
2.1.7. Недостатки в разработке программного обеспечения .....	32
2.1.8. Угрозы для физической безопасности.....	32
2.1.9. Распространение ложной информации .....	33
2.2. Механизмы и методы атаки .....	34
2.2.1. Фишинг (Phishing) .....	34
2.2.2. Троянские кони (Trojans).....	35
2.2.3. Вредоносное программное обеспечение (Malware) .....	35
2.2.4. Сетевые атаки (Network Attacks).....	36
2.2.5. Инженерия обратной связи (Reverse Engineering).....	36
2.2.6. Социальная инженерия (Social Engineering) .....	36
2.2.7. Уязвимости в приложениях и операционных системах.....	37
2.2.8. Угрозы физической безопасности.....	37
2.3. Факторы возникновения угроз.....	38
2.3.1. Технологические факторы.....	38
2.3.2. Человеческий фактор .....	39
2.3.3. Организационные факторы .....	39
2.3.4. Экономические факторы.....	39
2.3.5. Политические и геополитические факторы .....	40
2.4. Анализ и оценка рисков.....	40
2.4.1. Шаги оценки рисков.....	40
2.4.2. Методы анализа и оценки рисков .....	42
2.4.3. Пример анализа и оценки рисков.....	43
2.5. Профилактика и реагирование на угрозы .....	44
2.5.1. Профилактика угроз .....	45
2.5.2. Реагирование на угрозы.....	46
2.5.3. Пример профилактики и реагирования .....	47
<b>Глава 3. Теория информационной безопасности .....</b>	<b>50</b>
3.1. Модели безопасности данных.....	50
3.2. Принципы и методы обеспечения информационной безопасности .....	55

3.3. Теория управления рисками.....	59
3.4. Защита информации от утечек.....	63
<b>Глава 4. Физическая безопасность .....</b>	<b>68</b>
4.1. Защита физических средств .....	68
4.2. Методы противодействия физическим угрозам .....	71
4.3. Принципы безопасного размещения инфраструктуры.....	76
<b>Глава 5. Технические средства защиты информации .....</b>	<b>78</b>
5.1. Классификация средств защиты .....	78
5.2. Защита периметра и межсетевые экраны.....	82
5.3. Системы обнаружения и предотвращения вторжений .....	86
<b>Глава 6. Защита программного обеспечения и приложений.....</b>	<b>90</b>
6.1. Особенности безопасности веб-приложений .....	90
6.2. Методы обнаружения и устранения уязвимостей ПО .....	93
6.3. Правила безопасного кодирования.....	95
<b>Глава 7. Защита данных и конфиденциальной информации.....</b>	<b>98</b>
7.1. Классификация данных и уровни их защиты .....	98
7.2. Шифрование данных.....	101
7.3. Управление ключами и сертификация .....	104
<b>Глава 8. Безопасность сетевых взаимодействий.....</b>	<b>109</b>
8.1. Протоколы и стандарты безопасности .....	109
8.2. VPN и безопасные каналы передачи данных.....	110
<b>Глава 9. Организация системы управления информационной безопасностью .....</b>	<b>115</b>
9.1. Методологии и стандарты управления ИБ .....	115
9.2. Роль и ответственность персонала в системе ИБ .....	118
<b>Глава 10. Проактивная защита и реагирование на инциденты.....</b>	<b>121</b>
10.1. Мониторинг и выявление инцидентов безопасности .....	121
10.2. Организация команды быстрого реагирования.....	124
10.3. Процедуры восстановления после инцидентов.....	127
<b>Глава 11. Обучение и повышение квалификации в области кибербезопасности.....</b>	<b>131</b>
11.1. Формирование культуры безопасности среди персонала .....	131
11.2. Программы обучения и сертификации специалистов .....	133
11.3. Методики и материалы для проведения тренингов .....	136
11.4. Оценка эффективности обучающих программ.....	137

<b>Глава 12. Регулирование и соответствие в кибербезопасности .....</b>	<b>140</b>
12.1. Законодательные основы кибербезопасности .....	140
12.2. Международные стандарты и нормы .....	142
12.3. Подготовка и прохождение аудитов безопасности.....	143
12.4. Этические аспекты в кибербезопасности.....	145
12.5. Применение регулятивных требований на практике .....	148
<b>Глава 13. Киберугрозы будущего и прогнозирование .....</b>	<b>153</b>
13.1. Тенденции развития киберугроз .....	153
13.2. Анализ угроз с использованием искусственного интеллекта.....	154
13.3. Прогнозирование кибератак с использованием Big Data .....	156
13.4. Методы противодействия будущим угрозам.....	158
13.5. Оценка потенциальных рисков от новых технологий .....	160
<b>Глава 14. Продвинутое технологии в кибербезопасности.....</b>	<b>166</b>
14.1. Защита облачных технологий .....	166
14.2. Безопасность в сетях 5G .....	169
14.3. Блокчейн и кибербезопасность .....	171
14.4. Квантовая криптография .....	173
14.5. Биометрические системы безопасности.....	176
14.6. Автоматизированные системы обнаружения угроз.....	179
<b>Глава 15. Человеческий фактор в кибербезопасности .....</b>	<b>183</b>
15.1. Психология атакующего и защищаемого .....	183
15.2. Социальная инженерия и методы противодействия.....	185
15.3. Обучение и мотивация персонала к безопасному поведению .....	188
15.4. Проблема «внутреннего врага».....	190
15.5. Повышение осведомленности и вовлеченности персонала в процесс обеспечения безопасности .....	192
15.6. Оценка и улучшение человеческого фактора в системе ИБ.....	195
<b>Глава 16. Кибервойны и государственная безопасность.....</b>	<b>198</b>
16.1. Основные акторы и сценарии киберконфликтов .....	198
16.2. Государственные стратегии кибербезопасности.....	200
16.3. Основы киберразведки .....	201
16.4. Применение кибероружия и его последствия .....	202
16.5. Защита критически важной инфраструктуры.....	204
16.6. Международное сотрудничество в области кибербезопасности.....	206

<b>Глава 17. Цифровая гигиена и личная кибербезопасность .....</b>	<b>208</b>
17.1. Основы цифровой гигиены: от паролей до резервного копирования.....	208
17.2. Защита личных данных и анонимность в Интернете.....	210
17.3. Безопасное использование социальных сетей.....	212
17.4. Защита устройств: смартфоны, компьютеры, IoT.....	213
17.5. Осознанное потребление цифровых контентов и услуг .....	215
17.6. Угрозы в Интернете: фишинг, мошенничество и прочие риски .....	217
17.7. Принципы защиты домашней сети.....	218
<b>Глава 18. Криптография в кибербезопасности .....</b>	<b>221</b>
18.1. Основы симметричной и асимметричной криптографии.....	221
18.2. Протоколы шифрования и их применение .....	222
18.3. Сертификаты и инфраструктура открытых ключей (PKI) ....	224
18.4. Криптографические атаки и защита от них .....	226
18.5. Применение криптографии в современных приложениях и системах.....	227
18.6. Технологии блокчейн и их роль в кибербезопасности .....	229
18.7. Квантовые угрозы криптографии и будущее шифрования ..	231
<b>Глава 19. Ответственность и управление инцидентами .....</b>	<b>233</b>
19.1. Подготовка к инцидентам: планирование и роли .....	233
19.2. Фазы управления инцидентом .....	236
19.3. Ответ на инциденты: детекция, реагирование и восстановление .....	237
19.4. Анализ и уроки из инцидентов безопасности.....	240
19.5. Легальные аспекты и ответственность после инцидентов ....	242
19.6. Общение с общественностью и медиа после киберинцидентов .....	244
19.7. Постоянное улучшение процессов управления инцидентами .....	245
<b>Глава 20. Будущее кибербезопасности: вызовы и возможности .....</b>	<b>247</b>
20.1. Технологические инновации и их влияние на кибербезопасность .....	247
20.2. Развитие облачных технологий и новые угрозы .....	248
20.3. Безопасность квантовых вычислений и сетей .....	251
20.4. Искусственный интеллект и кибербезопасность: друзья или враги?.....	253

20.5. Роль человеческого фактора в будущем кибербезопасности.....	257
20.6. Безопасность в эпоху Интернета вещей и умных городов.....	259
20.7. Прогнозы и стратегии развития кибербезопасности на следующие десятилетия.....	261
<b>Дополнительные материалы .....</b>	<b>263</b>
Практические задачи по кибербезопасности.....	263
Кейсы и анализ реальных инцидентов .....	267
Материалы для преподавателей: примеры заданий и критерии оценки .....	269
Самостоятельные работы: анализ сценариев угроз, разработка планов ответа на инциденты.....	271
Рекомендации для дальнейшего обучения и профессионального развития. ....	274