

ЗАЩИТА ДАННЫХ

От авторизации до аудита



Джейсон Андресс



FOUNDATIONS OF INFORMATION SECURITY

**A Straightforward
Introduction**

by Jason Andress



**no starch
press**

San Francisco

Джейсон Андресс

ЗАЩИТА ДАННЫХ

От авторизации до аудита



Санкт-Петербург • Москва • Минск

2021

ББК 32.988.02-018-07
УДК 004.056.53

Андресс Джейсон

А65 Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.: ил. — (Серия «Для профессионалов»).

ISBN 978-5-4461-1733-8

Чем авторизация отличается от аутентификации? Как сохранить конфиденциальность и провести тестирование на проникновение? Автор отвечает на все базовые вопросы и на примерах реальных инцидентов рассматривает операционную безопасность, защиту ОС и мобильных устройств, а также проблемы проектирования сетей. Книга подойдет для новичков в области информационной безопасности, сетевых администраторов и всех интересующихся. Она станет отправной точкой для карьеры в области защиты данных.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.988.02-018-07
УДК 004.056.53

Права на издание получены по соглашению с No Starch Press. Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав.

Информация, содержащаяся в данной книге, получена из источников, рассматриваемых издательством как надежные. Тем не менее, имея в виду возможные человеческие или технические ошибки, издательство не может гарантировать абсолютную точность и полноту приводимых сведений и не несет ответственности за возможные ошибки, связанные с использованием книги. Издательство не несет ответственности за доступность материалов, ссылки на которые вы можете найти в этой книге. На момент подготовки книги к изданию все ссылки на интернет-ресурсы были действующими.

ISBN 978-1718500044 англ.

© 2019 by Jason Andress.

Foundations of Information Security: A Straightforward Introduction.

ISBN 978-1-7185-0004-4, published by No Starch Press.

ISBN 978-5-4461-1733-8

© Перевод на русский язык ООО Издательство «Питер», 2021

© Издание на русском языке, оформление ООО Издательство «Питер», 2021

© Серия «Для профессионалов», 2021

Оглавление

Об авторе	16
О научном редакторе	16
Благодарности	17
Введение	18
Для кого эта книга?	18
Структура.....	19
От издательства	20
Глава 1. Что такое информационная безопасность?	21
Определение информационной безопасности	22
Когда можно считать себя в безопасности?	22
Модели для обсуждения вопросов безопасности	24
Триада конфиденциальности, целостности и доступности	24
Паркеровская гексада	27
Атаки.....	29
Типы атак	29
Угрозы, уязвимости и риски.....	31
Управление рисками	32
Реакция на чрезвычайные происшествия	37
Глубокая защита	40
Итоги	43
Упражнения.....	44
Глава 2. Идентификация и аутентификация	46
Идентификация.....	47
Кем мы себя называем	47

Проверка личности.....	47
Обход идентификации	48
Аутентификация.....	49
Факторы.....	49
Многофакторная аутентификация.....	51
Взаимная аутентификация	52
Общие методы идентификации и аутентификации.....	53
Пароли.....	53
Биометрические данные.....	54
Аппаратные токены	57
Итоги.....	58
Упражнения.....	59
Глава 3. Авторизация и контроль доступа	60
Что такое контроль доступа?	60
Внедрение контроля доступа.....	62
Списки контроля доступа	63
Возможности	69
Модели контроля доступа	69
Дискреционный контроль доступа.....	69
Обязательный контроль доступа.....	70
Контроль доступа на основе правил.....	70
Контроль доступа на основе ролей.....	71
Контроль доступа на основе атрибутов.....	71
Многоуровневый контроль доступа	72
Контроль физического доступа	75
Итоги.....	77
Упражнения.....	78
Глава 4. Аудит и отчетность	79
Отчетность.....	81
Преимущества ведения отчетности с точки зрения безопасности.....	81
Неоспоримость.....	82
Сдерживание.....	82

Обнаружение и предотвращение вторжений	83
Допустимость записей.....	83
Аудит.....	84
Что нужно проверять во время аудита?.....	84
Ведение журналов	85
Мониторинг	86
Аудит с выполнением оценки.....	87
Итоги.....	88
Упражнения.....	89
Глава 5. Криптография.....	90
История криптографии	90
Шифр Цезаря.....	91
Криптографические машины.....	91
Принципы Керкхофса.....	95
Современные криптографические инструменты.....	96
Шифры с ключевыми словами и одноразовые блокноты.....	97
Шифры с ключевыми словами.....	97
Одноразовые блокноты.....	98
Симметричная и асимметричная криптография	99
Хеш-функции	103
Цифровые подписи	104
Сертификаты.....	105
Защита данных в состоянии покоя, в движении и в процессе использования.....	106
Защита данных в состоянии покоя.....	107
Защита данных в движении	108
Защита данных при использовании.....	109
Итоги.....	110
Упражнения.....	111
Глава 6. Соответствие, законы и нормативные положения	112
Что такое соответствие?.....	112
Типы соответствия.....	113
Последствия несоответствия.....	114

Достижение соответствия мерами контроля.....	115
Типы мер контроля.....	115
Ключевые и компенсирующие меры контроля.....	116
Соблюдение нормативных требований.....	116
Законы и информационная безопасность.....	118
Соответствие государственным нормативным требованиям.....	118
Соответствие отраслевым нормативным требованиям.....	120
Законы за пределами США.....	122
Выбор структуры для соответствия.....	123
Международная организация по стандартизации.....	124
Национальный институт стандартов и технологий.....	124
Пользовательские структуры.....	125
Соответствие требованиям в условиях технологических изменений.....	125
Соответствие в облаке.....	126
Соответствие в блокчейне.....	129
Соответствие в криптовалютах.....	129
Итоги.....	130
Упражнения.....	131
Глава 7. Операционная безопасность.....	132
Процесс обеспечения операционной безопасности.....	132
Определение важной информации.....	133
Анализ угроз.....	133
Анализ уязвимостей.....	134
Оценка рисков.....	135
Применение контрмер.....	135
Законы операционной безопасности.....	136
Первый закон: знайте об угрозах.....	136
Второй закон: знайте, что защищать.....	137
Третий закон: защищайте информацию.....	137
Операционная безопасность в частной жизни.....	138
Истоки операционной безопасности.....	140
Сунь-цзы.....	140

Джордж Вашингтон.....	140
Война во Вьетнаме.....	141
Бизнес.....	142
Межведомственный вспомогательный персонал OPSEC	142
Итоги.....	143
Упражнения.....	144
Глава 8. Человеческий фактор в безопасности.....	145
Сбор информации для атак социальной инженерии	146
Данные от людей.....	146
Данные из открытых источников.....	147
Другие виды данных	153
Типы атак социальной инженерии.....	154
Претекстинг.....	154
Фишинг.....	154
Проход «паровозиком»	156
Обучение безопасности	156
Пароли.....	157
Обучение социальной инженерии.....	157
Использование сетей	158
Вредоносное ПО.....	159
Личное оборудование	159
Политика чистого стола.....	159
Знакомство с политикой и нормативными знаниями	160
Итоги.....	160
Упражнения.....	161
Глава 9. Физическая безопасность.....	162
Выявление физических угроз.....	163
Меры контроля физической безопасности.....	163
Сдерживающие меры.....	164
Детективные меры (меры обнаружения).....	164
Превентивные меры.....	165
Использование мер контроля физического доступа.....	166

Защита людей.....	166
Физические проблемы людей.....	166
Обеспечение безопасности.....	167
Эвакуация.....	168
Административные меры контроля.....	169
Защита данных.....	169
Физические проблемы для данных.....	170
Доступность данных.....	171
Остаточные данные.....	171
Защита оборудования.....	172
Физические проблемы для оборудования.....	172
Выбор места.....	174
Обеспечение доступа.....	174
Условия окружающей среды.....	175
Итоги.....	175
Упражнения.....	176
Глава 10. Сетевая безопасность.....	177
Защита сетей.....	178
Проектирование безопасных сетей.....	178
Использование брандмауэров.....	179
Внедрение систем обнаружения сетевых вторжений.....	182
Защита сетевого трафика.....	183
Использование виртуальных частных сетей.....	184
Защита данных в беспроводных сетях.....	184
Использование безопасных протоколов.....	186
Инструменты сетевой безопасности.....	186
Инструменты защиты беспроводной сети.....	187
Сканеры.....	187
Снифферы пакетов.....	188
Приманки.....	189
Инструменты брандмауэра.....	190

Итоги	191
Упражнения	191
Глава 11. Безопасность операционной системы	192
Усиление защиты операционной системы	193
Удаление ненужного ПО	193
Удаление ненужных служб	194
Замена учетных записей по умолчанию	196
Использование принципа наименьших привилегий	197
Регулярные обновления	198
Ведение журнала и аудит	198
Защита от вредоносного ПО	199
Программные брандмауэры и обнаружение вторжений на хост	201
Инструменты безопасности операционной системы	202
Сканеры	202
Инструменты оценки уязвимости	204
Фреймворки эксплойтов	206
Итоги	207
Упражнения	208
Глава 12. Безопасность мобильных устройств, встроенных устройств и интернета вещей	209
Безопасность мобильных устройств	210
Защита мобильных устройств	210
Проблемы с мобильной безопасностью	212
Безопасность встроенных устройств	215
Где используются встроенные устройства	215
Проблемы безопасности встроенных устройств	218
Безопасность интернета вещей	220
Что такое IoT-устройство?	220
Проблемы безопасности интернета вещей	222
Итоги	224
Упражнения	225

Глава 13. Безопасность приложений	226
Уязвимости разработки программного обеспечения.....	227
Переполнение буфера.....	228
Состояние гонки.....	228
Атаки проверки ввода.....	229
Атаки аутентификации.....	230
Атаки авторизации.....	230
Криптографические атаки.....	231
Веб-безопасность.....	231
Атаки на стороне клиента.....	232
Атаки на стороне сервера.....	233
Безопасность баз данных.....	235
Проблемы протокола.....	236
Доступ без аутентификации.....	237
Выполнение произвольного кода.....	237
Повышение уровня привилегий.....	238
Инструменты безопасности приложений.....	239
Снифферы.....	239
Инструменты анализа веб-приложений.....	240
Фаззеры.....	243
Итоги.....	243
Упражнения.....	244
Глава 14. Оценка безопасности	245
Оценка уязвимости.....	245
Отображение и обнаружение.....	246
Сканирование.....	247
Технологические вызовы в оценке уязвимостей.....	249
Тестирование на проникновение.....	250
Процесс пентеста.....	251
Классификация пентестов.....	253
Цели пентестов.....	254

Программы Bug Bounty	257
Технологические вызовы пентестирования	258
Как понять, что вы в безопасности?.....	258
Реалистичное тестирование	259
Как определить собственные атаки?	260
Заделывание дыр в безопасности – дорогое удовольствие.....	263
Итоги	263
Упражнения.....	264
Список источников.....	265