

Для тех, кто хочет стать профессионалом

Кузнецов А. В.

Информационная БЕЗОПАСНОСТЬ

Анализ и оценка угроз
Кибер/криптозащита организаций
Разработка безопасного ПО



Содержание

ВВЕДЕНИЕ	17
-----------------------	-----------

Раздел 1. Введение в тематику обеспечения информационной безопасности

ГЛАВА 1. Информация как отправная точка	23
--	-----------

1.1. РАЗВИТИЕ И РАСПРОСТРАНЕНИЕ ИНФОРМАЦИИ И ИНФОРМАЦИОН- НЫХ ТЕХНОЛОГИЙ.....	24
--	-----------

1.2. ИНФОРМАЦИЯ КАК АКТИВ	26
--	-----------

1.3. СОСТОЯНИЯ И КАТЕГОРИИ ИНФОРМАЦИИ.....	28
---	-----------

ГЛАВА 2. Фундамент обеспечения информационной безопасности	33
---	-----------

2.1. КЛЮЧЕВЫЕ ПОНЯТИЯ.....	34
-----------------------------------	-----------

2.2. ПОПУЛЯРНЫЕ КОНЦЕПЦИИ	36
--	-----------

Конфиденциальность, целостность и доступность (CIA Triad)	36
---	----

Аутентификация, авторизация и учёт (AAA)	39
--	----

Циклы PDCA и OODA	40
-------------------------	----

Модели зрелости (Maturity models)	42
---	----

Концепция «Эшелонированной обороны» (Defense in Depth)	43
--	----

Концепция «Нулевого доверия» (Zero Trust)	44
---	----

2.3. ОСНОВНЫЕ ПРИНЦИПЫ И МЕТОДЫ	47
--	-----------

2.4. ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ	50
---	-----------

Обеспечение безопасности персональных данных.....	53
---	----

Обеспечение безопасности критической информационной инфраструктуры РФ	56
--	----

Обеспечение защиты информации при осуществлении банковской деятельности и деятельности в сфере финансовых рынков.....	59
--	----

Охрана конфиденциальности информации, составляющей коммерческую тайну.....	61
Ключевое международное законодательство	63

**ГЛАВА 3. Ответственность и этические принципы в
областях обеспечения и нарушения информаци-
онной безопасности..... 67**

3.1. ВИДЫ ОТВЕТСТВЕННОСТИ.....	68
3.2. ЭТИЧЕСКИЕ ПРИНЦИПЫ.....	69

**ГЛАВА 4. Профессиональные специализации в области
обеспечения информационной безопасности .. 71**

4.1. НАПРАВЛЕНИЯ ПОДГОТОВКИ И ПРОФЕССИОНАЛЬНЫЕ СТАНДАРТЫ..	72
4.2. СПЕЦИАЛИЗАЦИИ И ПРОФЕССИОНАЛЬНЫЕ СЕРТИФИКАЦИИ	77
ВЫВОДЫ	79
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	80
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	81

**Раздел 2. Определение актуальных угроз и выбор
мер защиты информации**

ГЛАВА 5. Угрозы информационной безопасности..... 85

5.1. ПОНЯТИЕ УГРОЗЫ.....	86
5.2. ИСТОЧНИКИ УГРОЗ.....	88
5.3. СПОСОБЫ РЕАЛИЗАЦИИ УГРОЗ	88
Способы реализации угроз на основе методики ФСТЭК России	90
Способы реализации угроз на основе модели угроз ФСТЭК России ..	91
Модель STRIDE	92

5.4. ВРЕДНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.....	94
5.5. СЕТЕВЫЕ АТАКИ	98
5.6. УЯЗВИМОСТИ.....	102
ГЛАВА 6. Типизация кибератак.....	109
6.1. МОДЕЛЬ CYBER KILL CHAIN®.....	110
6.2. МАТРИЦА MITRE ATT&CK®	112
ГЛАВА 7. Определение актуальных угроз	119
7.1. ВАРИАНТЫ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ	120
7.2. МОДЕЛИРОВАНИЕ УГРОЗ ПО МЕТОДИКЕ ФСТЭК РОССИИ.....	125
7.3. ДЕРЕВЬЯ АТАК.....	136
7.4. ТИПОВЫЕ ПРОБЛЕМЫ ПРИ ОПРЕДЕЛЕНИИ АКТУАЛЬНЫХ УГРОЗ	137
ГЛАВА 8. Меры защиты информации.....	139
8.1. КЛАССИФИКАЦИЯ МЕР ЗАЩИТЫ ИНФОРМАЦИИ.....	140
8.2. ВАРИАНТЫ ВЫБОРА И ОБОСНОВАНИЯ МЕР ЗАЩИТЫ ИНФОРМАЦИИ... 	142
8.3. ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПО МЕТОДИКЕ ФСТЭК РОССИИ. 	145
8.4. ВАРИАНТЫ ПРИОРИТИЗАЦИИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ	149
ГЛАВА 9. Лучшие практики в области обеспечения информационной безопасности	151
9.1. СТАНДАРТЫ СЕМЕЙСТВА ISO/IEC 27000.....	152
9.2. СТАНДАРТ NIST CYBERSECURITY FRAMEWORK.....	153
9.3. НАБОР TOP CRITICAL SECURITY CONTROLS	155
9.4. ПРОЕКТЫ СООБЩЕСТВА OWASP.....	156

ВЫВОДЫ	157
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	158
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	159

Раздел 3. Основные технологии и инструменты обеспечения информационной безопасности

ГЛАВА 10. Общие сведения о технологиях и инструментах.....	163
---	------------

10.1. РАЗВИТИЕ ТЕХНОЛОГИЙ И ИНСТРУМЕНТОВ.....	164
10.2. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	167
10.3. СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.....	167

ГЛАВА 11. Встроенные и наложенные средства защиты информации	175
---	------------

11.1. ИДЕНТИФИКАЦИЯ.....	176
11.2. АУТЕНТИФИКАЦИЯ	178
Пароли.....	180
Современные протоколы аутентификации	182
Популярные парольные атаки.....	186
11.3. АВТОРИЗАЦИЯ.....	187
Мандатное разграничение прав доступа.....	188
Дискреционное разграничение прав доступа	190
Ролевое разграничение прав доступа	195
Атрибутное (контекстное) разграничение прав доступа	195
11.4. РЕГИСТРАЦИЯ (УЧЁТ) СОБЫТИЙ БЕЗОПАСНОСТИ.....	196
11.5. КОНТРОЛЬ УТЕЧЕК	200
11.6. ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	201
11.7. СРЕДСТВА АНТИВИРУСНОЙ ЗАЩИТЫ.....	203

Сигнатурный анализ.....	205
Эвристический анализ	205
Поведенческий анализ.....	206
11.8. НАЛОЖЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИО- НИРОВАННОГО ДОСТУПА	206

ГЛАВА 12. Хостовые и сетевые средства защиты информации 209

12.1. МЕЖСЕТЕВЫЕ ЭКРАНЫ	211
12.2. СИСТЕМЫ ОБНАРУЖЕНИЯ/ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ.....	217
12.3. СРЕДСТВА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ..	219
ВЫВОДЫ	220
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	221
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	222

Раздел 4. Криптографическая защита информации

ГЛАВА 13. Основные криптосистемы и их компоненты.. 225

13.1. КРАТКАЯ ИСТОРИЯ КРИПТОГРАФИИ.....	226
13.2. КЛАССИФИКАЦИЯ КРИПТОСИСТЕМ	228
13.3. СИММЕТРИЧНОЕ ШИФРОВАНИЕ.....	230
13.4. АСИММЕТРИЧНОЕ ШИФРОВАНИЕ	232
13.5. ХЭШ-ФУНКЦИЯ.....	235
13.6. ЭЛЕКТРОННАЯ ПОДПИСЬ.....	237
13.7. ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ	240

ГЛАВА 14. Практика криптографической защиты информации 247

14.1. СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	248
14.2. ПРАКТИКА ПРИМЕНЕНИЯ ШИФРОВАЛЬНЫХ СРЕДСТВ.....	249
14.3. СОВРЕМЕННЫЕ ПРОТОКОЛЫ ШИФРОВАНИЯ.....	253
ГЛАВА 15. Безопасность криптосистем	257
15.1. ЗАЩИТА ЗАКРЫТЫХ КЛЮЧЕЙ	258
15.2. АТАКИ НА КРИПТОСИСТЕМЫ.....	259
ГЛАВА 16. Особенности применения шифровальных средств в России	263
16.1. СЕРТИФИКАЦИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	264
16.2. ИСПОЛЬЗОВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.....	266
ВЫВОДЫ	268
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	269
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	269

Раздел 5. Безопасная разработка приложений

Глава 17. Процессы безопасной разработки приложений	273
17.1. МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ	274
17.2. ПРИНЦИПЫ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРИЛОЖЕНИЙ	277
17.3. ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ	278
ГЛАВА 18. Лучшие практики безопасной разработки ...	281

18.1. СТАНДАРТЫ СЕРИИ ISO/IEC 27034	282
18.2. НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ГОСТ Р 5XXXX	285
18.3. NIST SSDF	287
18.4. OWASP CLASP И SSDF	288

ГЛАВА 19. Рекомендации по безопасному написанию кода293

19.1. ОБЩИЕ ПРАКТИКИ ПРОГРАММИРОВАНИЯ	294
19.2. ВАЛИДАЦИЯ ВХОДНЫХ ДАННЫХ.....	295
19.3. КОДИРОВАНИЕ ВЫХОДНЫХ ДАННЫХ.....	298
19.4. АУТЕНТИФИКАЦИЯ И УПРАВЛЕНИЕ ПАРОЛЯМИ, А ТАКЖЕ КРИПТОГРА- ФИЧЕСКАЯ ЗАЩИТА	300
19.5. ОБРАБОТКА ОШИБОК И РЕГИСТРАЦИЯ СОБЫТИЙ	304

ГЛАВА 20. Автоматизация и контроль соблюдения требований безопасности307

20.1. ОСНОВНЫЕ СПОСОБЫ ВЕРИФИКАЦИИ ТРЕБОВАНИЙ БЕЗОПАС- НОСТИ	308
20.2. ЦИКЛ DEVSECOPS.....	310
ВЫВОДЫ	312
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	313
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	313

Раздел 6. Анализ и оценка защищённости

ГЛАВА 21. Роль и место оценки защищённости в обе- спечении информационной безопасности317

21.1. ЦЕЛИ И КРИТЕРИИ ОЦЕНКИ ЗАЩИЩЁННОСТИ.....	318
21.2. ВАРИАНТЫ АНАЛИЗА И ОЦЕНКИ ЗАЩИЩЁННОСТИ	320
21.3. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	323
21.4. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ.....	325
ГЛАВА 22. Аудит информационной безопасности	331
22.1. ВИДЫ АУДИТА.....	332
22.2. ПРИНЦИПЫ ПРОВЕДЕНИЯ АУДИТА	332
22.3. ПОРЯДОК ПРОВЕДЕНИЯ АУДИТА	333
22.4. ОЦЕНКИ И ОТЧЁТНОСТЬ ПО РЕЗУЛЬТАТАМ АУДИТА.....	338
ГЛАВА 23. Практико-ориентированный анализ и оценка защищённости	341
23.1. РАЗВЕДКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ	342
23.2. ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ	345
23.3. ВЫЯВЛЕНИЕ ИЗВЕСТНЫХ УЯЗВИМОСТЕЙ	350
23.4. КИБЕРУЧЕНИЯ	352
ГЛАВА 24. Методы анализа защищённости отдельных приложений	355
24.1. АНАЛИЗ (ИНСПЕКЦИЯ) КОДА.....	356
24.2. СТАТИЧЕСКИЙ АНАЛИЗ	356
24.3. ДИНАМИЧЕСКИЙ АНАЛИЗ	357
24.4. КОМПОНЕНТНЫЙ АНАЛИЗ И АНАЛИЗ ВНЕШНИХ ЗАВИСИМОСТЕЙ..	358
24.5. ФАЗЗИНГ-ТЕСТИРОВАНИЕ	359

ВЫВОДЫ	360
ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ	361
ЗАДАНИЯ ДЛЯ САМОПРОВЕРКИ	362
ЗАКЛЮЧЕНИЕ.....	364
ПРИЛОЖЕНИЕ А. Справочные сведения о распределении зон ответственности при использовании «облачных решений»	365
ПРИЛОЖЕНИЕ Б. Справочные сведения о локальных нормативных актах организации по обеспечению информационной безопасности.....	369
ПРИЛОЖЕНИЕ В. Справочные сведения об административной и уголовной ответственностях за нарушения в области обеспечения информационной безопасности	373
ПРИЛОЖЕНИЕ Г. Схема инкапсуляции и декапсуляции данных при передаче по сети	381
ПРИЛОЖЕНИЕ Д. Справочные сведения о регистрируемых категориях событий безопасности	383
ПРИЛОЖЕНИЕ Е. Справочные сведения о протоколах для (без)опасной передачи данных	395
ПРИЛОЖЕНИЕ Ж. Справочные сведения о мерах по разработке безопасного программного обеспечения	397

ГЛОССАРИЙ.....	411
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	425