

В.И. Аверченков

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

4-е издание, стереотипное

Москва
Издательство «ФЛИНТА»
2021

УДК 004.732.056.5

ББК 16.84

A19

Р е ц е н з е н т ы:

кафедра «Защита информации» Воронежского государственного технического университета; доктор технических наук профессор *И.С. Константинов*

Аверченков В.И.

A19 Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 269 с. – ISBN 978-5-9765-1256-6. – Текст : электронный.

Рассмотрен комплекс вопросов, связанных с проведением аудита информационной безопасности на предприятии, даны основные понятия, показана роль анализа и управления информационными рисками. Проведено описание международных и российских стандартов информационной безопасности, изложены методологические основы применения стандартов ISO 15408 и ISO 17799 для оценки и управления безопасностью информационных технологий, дана характеристика программных средств, применяемых при аудите информационной безопасности. Особое внимание уделено практическим вопросам методики проведения аудита информационной безопасности на предприятии.

Учебное пособие предназначено для студентов, обучающихся по специальности «Организация и технология защиты информации», а также может быть полезно специалистам, занимающимся организационными вопросами защиты информации на предприятиях.

УДК 004.732.056.5

ББК 16.84

ISBN 978-5-9765-1256-6

© В.И. Аверченков, 2016

© Издательство «ФЛИНТА», 2016

Оглавление

Предисловие	3
Глава 1. Основы построения систем информационной безопасности	5
1.1. Цель и задачи информационной безопасности (ИБ).....	5
1.2. Угрозы ИБ и их источники.....	6
1.3. Модель построения системы информационной безопасности предприятия.....	12
1.4. Разработка концепция обеспечения ИБ.....	14
Контрольные вопросы.....	17
Глава 2. Аудит безопасности и методы его проведения	18
2.1. Понятие аудита безопасности.....	18
2.2. Методы анализа данных при аудите ИБ.....	23
2.3. Анализ информационных рисков предприятия.....	25
2.4. Методы оценивания информационных рисков.....	30
2.5. Управление информационными рисками.....	33
Контрольные вопросы.....	37
Глава 3. Стандарты информационной безопасности	38
3.1. Предпосылки создания стандартов ИБ.....	38
3.2. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).....	40
3.3. Гармонизированные критерии Европейских стран.....	49
3.4. Германский стандарт BS1.....	52
3.5. Британский стандарт BS 7799.....	54
3.6. Международный стандарт ISO 17799.....	56
3.7. Международный стандарт ISO 15408 «Общие критерии».....	58
3.8. Стандарт COBIT.....	62
3.9. Стандарты по безопасности информационных технологий в России.....	71
Контрольные вопросы.....	82
Глава 4. Оценка безопасности информационных технологий на основе «Общих критериев»	83

4.1. Предпосылки введения международного стандарта ISO 15408.....	83
4.2. Основные понятия общих критериев.....	85
4.3. Методология оценки безопасности информационных технологий по общим критериям.....	93
4.4. Оценка уровня доверия функциональной безопасности информационной технологии.....	96
4.5. Обзор классов и семейств ОК.....	102
Контрольные вопросы.....	107
Глава 5. Международный стандарт управления информационной безопасностью ISO 17799.....	108
5.1. Назначение стандарта ISO 17799 для управления информационной безопасностью.....	108
5.2. Практика прохождения аудита и получения сертификата ISO 17799.....	112
5.3. Раздел 1. Политика безопасности.....	113
5.4. Раздел 2. Организационные меры по обеспечению информационной безопасности.....	116
5.5. Раздел 3. Классификация ресурсов и их контроль.....	121
5.6. Раздел 4. Безопасность персонала.....	124
5.7. Раздел 5. Физическая безопасность.....	129
5.8. Раздел 6. Администрирование компьютерных систем и вычислительных сетей.....	137
5.9. Раздел 7. Управление доступом к системам.....	154
5.10. Раздел 8. Разработка и сопровождение информационных систем.....	171
5.11. Раздел 9. Планирование бесперебойной работы организации.....	180
5.12. Раздел 10. Соответствие системы основным требованиям.....	184
Контрольные вопросы.....	189
Глава 6. Программные средства для проведения аудита информационной безопасности.....	191
6.1. Анализ видов используемых программных продуктов....	191
6.2. Система CRAMM.....	192
6.3. Система КОНДОР.....	198

6.4. Сетевые сканеры.....	200
Контрольные вопросы.....	205
Глава 7. Методика проведения аудита информационной безопасности на предприятии.....	206
7.1. Три подхода к проведению аудита ИБ.....	206
7.2. Задачи и содержание работ при проведении аудита ИБ.....	208
7.3. Подготовка предприятий к проведению аудита ИБ.....	211
7.4. Планирование процедуры аудита ИБ.....	216
7.5. Организация и проведения работ по аудиту.....	221
7.6. Алгоритм проведения аудита безопасности предприятия.....	224
7.7. Перечень и систематизация данных, необходимых для проведения аудита ИБ.....	229
7.8. Выработка рекомендаций и подготовка отчетных документов.....	233
7.9. Экономическая оценка обеспечения ИБ.....	236
Контрольные вопросы.....	247
Заключение.....	249
Глоссарий.....	252
Список использованной и рекомендуемой литературы.....	264