

# Оглавление

Предисловие.....	3
Введение.....	5
<b>1. Современные проблемы информационной безопасности ..</b>	<b>12</b>
1.1. Информационная безопасность и проблемы защиты информации .....	12
1.2. Ретроспективный анализ развития подходов к защите информации .....	18
1.3. Современная постановка задачи защиты информации.....	27
1.4. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации.....	33
Контрольные вопросы.....	38
<b>2. Угрозы и уязвимость информации .....</b>	<b>39</b>
2.1. Понятие угрозы безопасности информации, системная классификация угроз .....	39
2.2. Показатели уязвимости информации .....	45
2.3. Модели оценки ущерба от реализации угроз безопасности информации .....	49
Контрольные вопросы.....	54
<b>3. Защита информации от несанкционированного доступа ..</b>	<b>56</b>
3.1. Общесистемные аспекты .....	56
3.1.1. Введение в проблему .....	56
3.1.2. Модель нарушителя доступа при защите АС от НСД.....	60
3.1.3. Отношения доступа и их представления в АС.....	61
3.1.4. Системная организация защиты информации от НСД.....	63
3.2. Методы аутентификации.....	67
3.2.1. Общая характеристика функции аутентификации.....	67
3.2.2. Аутентификация на знании.....	69
3.2.3. Аутентификация на основе обладания предметом.....	77
3.2.4. Аутентификация на воплощенных характеристиках.....	81
3.3. Методы реализации контроля и разграничения доступа.....	85
3.3.1. Общая характеристика функции контроля и разграничения доступа.....	85
3.3.2. Способы контроля и управления доступом .....	89
3.3.3. Механизмы контроля и разграничения доступа.....	91
Контрольные вопросы.....	98
<b>4. Криптографические методы защиты информации .....</b>	<b>100</b>
4.1. Общесистемные аспекты криптологии .....	100
4.2. Основные понятия криптологии.....	103
4.3. Криптографические алгоритмы.....	106

4.3.1. Шифры перестановки .....	106
4.3.2. Шифры замены .....	107
4.3.3. Симметричные блочные шифры .....	111
4.4. Криптографические протоколы .....	113
4.4.1. Общие сведения .....	113
4.4.2. Организация секретной связи .....	115
4.4.3. Обеспечение целостности сообщений .....	119
4.4.4. Цифровая подпись .....	121
4.4.5. Неотслеживаемость информации .....	125
4.5. Ключевая подсистема криптосистемы .....	126
4.5.1. Строение и порядок ключевого множества .....	126
4.5.2. Генерация ключей .....	128
4.5.3. Обеспечение секретности ключей .....	132
4.5.4. Протоколы обмена ключами .....	135
4.5.5. Стойкость к компрометациям и архитектура ключевых систем в различных сетях связи .....	141
4.5.6. Особенности ключевых систем для защищенного хранения данных .....	144
Контрольные вопросы .....	145
<b>5. Противодействие утечке по техническим каналам .....</b>	<b>147</b>
5.1. Технические каналы как источники утечки информации .....	147
5.2. ТКУИ объектов информатизации .....	151
5.3. Каналы утечки речевой информации .....	156
5.4. ТКУИ при передаче по каналам связи .....	159
5.5. Технические каналы утечки видовой информации .....	160
5.6. ТКУИ средств вычислительной техники .....	161
5.7. Акустические и виброакустические каналы утечки речевой информации .....	165
5.8. Способы противодействия утечке по техническим каналам ..	171
Контрольные вопросы .....	175
<b>6. Вредоносное программное обеспечение (компьютерные вирусы) .....</b>	<b>176</b>
6.1. Компьютерные вирусы как вид информационно-программного оружия .....	176
6.2. Общее описание компьютерных вирусов .....	179
6.3. Видовая классификация компьютерных вирусов .....	185
6.4. Методы и средства антивирусной защиты .....	187
6.4.1. Невосприимчивость к заражению вирусами .....	187
6.4.2. Защита от вирусов в статике процессов .....	188
6.4.3. Защита от вирусов в динамике процессов .....	190
6.4.4. Организационно-правовые меры .....	192
6.5. Антивирусная политика на объекте информатизации .....	193
Контрольные вопросы .....	196
<b>7. Организационно-правовое обеспечение информационной безопасности .....</b>	<b>198</b>

7.1. Предмет и содержание проблемы .....	198
7.2. Законодательная база информационной безопасности .....	200
7.3. Государственная система защиты информации .....	203
7.3.1. Структура государственной системы .....	203
7.3.2. Полномочия субъектов государственной системы .....	204
7.4. Лицензирование деятельности в области защиты информации .....	207
7.4.1. Общие основы лицензирования .....	207
7.4.2. Защита государственной тайны .....	209
7.4.3. Техническая защита конфиденциальной информации .....	211
7.5. Техническое регулирование в области защиты информации .	219
7.5.1. Общие правовые основы технического регулирования .....	219
7.5.2. Организационная схема сертификации средств защиты информации .....	222
7.6. Организационные структуры объектового уровня .....	223
7.7. Службы безопасности объектового уровня .....	227
7.8. Корпоративная нормативная база по защите информации .....	230
7.9. Политика безопасности .....	233
7.10. Организация объектовых режимов безопасности .....	237
7.11. Порядок проведения служебных расследований .....	246
7.12. Информационная безопасность в аспекте управления персоналом .....	248
Контрольные вопросы .....	255
<b>8. Комплексные системы защиты информации .....</b>	<b>256</b>
8.1. Системный подход при комплексной защите информации .....	256
8.1.1. Объект защиты .....	256
8.1.2. Системность и комплексность защиты информации .....	257
8.1.3. Учет совокупной эффективности системы защиты информации .....	260
8.2. Макроструктурные компоненты КСЗИ .....	262
8.3. Функциональные подсистемы .....	265
8.4. Обеспечивающие подсистемы .....	268
8.5. Технологическая составляющая КСЗИ .....	274
8.6. Управление информационной безопасностью .....	275
8.7. Подсистема информационного обеспечения КСЗИ .....	277
Контрольные вопросы .....	278
Литература .....	279