



## ОГЛАВЛЕНИЕ

Список принятых сокращений .....	6
Введение .....	8
1. Теоретические основы информационной безопасности .....	10
1.1. Базовые понятия .....	10
1.2. Общая схема процесса обеспечения безопасности .....	14
1.3. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа .....	15
1.4. Модели безопасности .....	20
1.4.1. Модель Харрисона — Руззо — Ульмана .....	22
1.4.2. Модель Белла – ЛаПадулы .....	26
1.4.3. Ролевая модель безопасности .....	30
1.5. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408 .....	32
2. Основы криптографии .....	35
2.1. Основные понятия. Классификация шифров .....	35
2.2. Симметричные шифры .....	43
2.2.1. Схема Фейстеля .....	43
2.2.2. Шифр DES .....	45
2.2.3. Шифр ГОСТ 28147-89 .....	55
2.2.4. Шифр Blowfish .....	57
2.3. Управление криптографическими ключами для симметричных шифров .....	59
2.4. Асимметричные шифры .....	67
2.4.1. Основные понятия .....	67
2.4.2. Распределение ключей по схеме Диффи — Хеллмана .....	71
2.4.3. Криптографическая система RSA .....	73
2.4.4. Криптографическая система Эль-Гамала .....	76
2.4.5. Совместное использование симметричных и асимметричных шифров .....	79
2.5. Хеш-функции .....	79
2.5.1. Хэш-функции без ключа .....	80
2.5.2. Алгоритм SHA-1 .....	82
2.5.3. Хеш-функции с ключом .....	84
2.6. Инфраструктура открытых ключей. Цифровые сертификаты .....	85

---

3. Защита информации в IP-сетях .....	93
3.1. Протокол защиты электронной почты S/MIME .....	94
3.2. Протоколы SSL и TLS.....	96
3.3. Протоколы IPSec и распределение ключей.....	100
3.3.1. Протокол AH.....	103
3.3.2. Протокол ESP.....	105
3.3.3. Протокол SKIP.....	107
3.3.4. Протоколы ISAKMP и IKE.....	110
3.3.5. Протоколы IPSec и трансляция сетевых адресов .....	115
3.4. Межсетевые экраны .....	117
4. Анализ и управление рисками в сфере информационной безопасности .....	121
4.1. Введение в проблему.....	121
4.2. Управление рисками. Модель безопасности с полным перекрытием .....	125
4.3. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001 .....	129
4.3.1. ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью».....	130
4.3.2. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».....	141
4.4. Методики построения систем защиты информации .....	145
4.4.1. Модель Lifecycle Security.....	145
4.4.2. Модель многоуровневой защиты.....	149
4.4.3. Методика управления рисками, предлагаемая «Майкрософт» .....	152
4.5. Методики и программные продукты для оценки рисков.....	158
4.5.1. Методика CRAMM.....	158
4.5.2. Методика FRAP .....	164
4.5.3. Методика OCTAVE.....	168
4.5.4. Методика RiskWatch .....	172
4.5.5. Проведение оценки рисков в соответствии с методикой «Майкрософт».....	177
4.5.6. Анализ существующих подходов .....	190

---

4.6. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник — нарушитель» .....	192
5. Практикум по информационной безопасности.....	195
5.1. Управление доступом к файлам на NTFS .....	195
5.2. Управление доступом в СУБД SQL Server .....	202
5.3. Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.....	211
5.4. Использование сканеров безопасности для получения информации о хостах в сети .....	217
5.5. Встроенный межсетевой экран (firewall) Windows Server 2008 .....	219
5.6. Использование цифровых сертификатов .....	224
5.7. Создание центра сертификации (удостоверяющего центра) в Windows Server 2008 .....	229
5.8. Шифрование данных при хранении — файловая система EFS..	237
5.9. Использование Microsoft Security Assessment Tool .....	243
5.10. Лабораторный практикум Kaspersky Security Center .....	247
5.10.1. Установка Kaspersky Security Center.....	250
5.10.2. Развертывание антивирусной защиты: установка агентов администрирования, проверка совместимости .....	263
5.10.3. Развертывание антивирусной защиты и управление лицензионными ключами .....	278
5.10.4. Конфигурирование сервера администрирования .....	284
5.10.5. Работа с вирусными инцидентами .....	299
5.11. Настройка протокола IPSec в Windows Server 2008.....	309
Библиографический список.....	318