

0- 806614

ВЫСШЕЕ ОБРАЗОВАНИЕ

Е.К. Баранова, А.В. Бабаиш

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УЧЕБНОЕ ПОСОБИЕ

Электронно-
Библиотечная
Система
znanium.com



ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ	3
ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	6
1.1. Проблема обеспечения информационной безопасности	6
1.1.1. Определение понятия «информационная безопасность»	6
1.1.2. Составляющие информационной безопасности	9
1.2. Уровни формирования режима информационной безопасности	12
1.2.1. Задачи информационной безопасности общества	12
1.2.2. Уровни формирования режима информационной безопасности	13
1.3. Нормативно-правовые основы информационной безопасности в РФ	15
1.3.1. Правовые основы информационной безопасности общества	15
1.3.2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации	16
1.3.3. Ответственность за нарушения в сфере информационной безопасности	19
1.4. Стандарты информационной безопасности	22
1.4.1. Требования безопасности к информационным системам	22
1.4.2. Принцип иерархии: класс—семейство—компонент—элемент	23
1.4.3. Функциональные требования	24
1.4.4. Требования доверия	25
1.5. Стандарты информационной безопасности распределенных систем	26
1.5.1. Сервисы безопасности в вычислительных сетях	26
1.5.2. Механизмы безопасности	27
1.5.3. Администрирование средств безопасности	27
1.6. Федеральная служба по техническому и Экспортному контролю (ФСТЭК)	30
1.7. Административный уровень обеспечения информационной безопасности	31
1.7.1. Цели, задачи и содержание административного уровня	31
1.7.2. Разработка политики информационной безопасности	32
1.8. Классификация угроз информационной безопасности	34
1.8.1. Классы угроз информационной безопасности	34

1.8.2. Каналы несанкционированного доступа к информации	37
1.8.3. Технические каналы утечки информации	38
1.9. Анализ угроз информационной безопасности	44
1.9.1. Наиболее распространенные угрозы нарушения доступности информации	44
1.9.2. Основные угрозы нарушения целостности информации	46
1.9.3. Основные угрозы нарушения конфиденциальности информации	47
Литература к главе 1	48
ГЛАВА 2. ВРЕДОНОСНЫЕ ПРОГРАММЫ И ЗАЩИТА ОТ НИХ	49
2.1. Вредоносные программы как угроза информационной безопасности	49
2.1.1. Вредоносное программное обеспечение (ПО) и информационная безопасность	49
2.1.2. Хронология развития вредоносных программ	50
2.1.3. Классификация вредоносного программного обеспечения	55
2.2. Антивирусные программы	59
2.2.1. Особенности работы антивирусных программ	59
2.2.2. Методы защиты от вредоносных программ	59
2.2.3. Факторы, определяющие качество антивирусных программ	60
2.3. Угрозы для мобильных устройств	61
2.3.1. Классификация угроз для мобильных устройств	61
2.3.2. Защита мобильных устройств	64
Литература к главе 2	66
ГЛАВА 3. АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ, УГРОЗ И УЯЗВИМОСТЕЙ СИСТЕМЫ	67
3.1. Методики оценки рисков в сфере информационной безопасности	67
3.1.1. Общие понятия и терминология	67
3.1.2. Описание процесса оценки рисков информационной безопасности	70
3.1.3. Обзор существующих стандартов и методик оценки рисков информационной безопасности	75
3.1.4. Подходы к оценке рисков информационной безопасности	82
3.2. Программное обеспечение для оценки рисков информационной безопасности	88
3.3. Базовый подход к обоснованию проекта подсистемы обеспечения информационной безопасности	102

3.3.1. Оценка потерь от реализации потенциальных угроз и затрат на защиту информации	102
3.3.2. Идентификация риска	103
3.3.3. Модель безопасности с полным перекрытием	104
3.4. Пакет методологии CORAS как программное обеспечение для анализа рисков информационной безопасности предприятия	106
ПРИЛОЖЕНИЕ 3.1	114
Применение модели с полным перекрытием для анализа рисков информационной безопасности малого предприятия	114
ПРИЛОЖЕНИЕ 3.2	118
Использование программного обеспечения Coras для анализа рисков филиала MBA	118
Литература к главе 3	126
ГЛАВА 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ	127
4.1. Особенности обеспечения информационной безопасности в компьютерных сетях	127
4.1.1. Общие сведения о безопасности в компьютерных сетях	127
4.2. Сетевые модели передачи данных	130
4.2.1. Понятие протокола передачи данных	130
4.2.2. Принципы организации обмена данными в вычислительных сетях	132
4.2.3. Транспортный протокол TCP и модель TCP/IP	132
4.3. Модель взаимодействия открытых систем OSI/ISO	134
4.3.1. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO	134
4.3.2. Распределение функций безопасности по уровням модели OSI/ISO	135
4.4. Адресация в глобальных сетях	137
4.4.1. Основы построения IP-протокола	137
4.4.2. Классы адресов вычислительных сетей	139
4.4.3. Система доменных имен	139
4.5. Классификация удаленных угроз в вычислительных сетях	149
4.6. Типовые удаленные атаки и их характеристика	153
4.7. Механизмы обеспечения информационной безопасности в информационных системах	158
4.7.1. Идентификация и аутентификация	158
4.7.2. Методы разграничения доступа	162
4.7.3. Регистрация и аудит	164

4.7.4. Межсетевое экранирование	166
4.7.5. Технология виртуальных частных сетей	169
Литература к главе 4	171

ГЛАВА 5. МЕТОДЫ ПРИНЯТИЯ РЕШЕНИЙ В РАЗРАБОТКЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	173
5.1. Основные понятия и определения	173
5.1.1. Принятие решений как особый вид человеческой деятельности	173
5.1.2. Люди, принимающие решения, и их роль в процессе принятия решений	174
5.1.3. Альтернативы	176
5.1.4. Критерии	176
5.1.5. Оценка важности критериев	178
5.1.6. Многодисциплинарный характер науки о принятии решений	180
5.2. Анализ задач и методов принятия решений	181
5.2.1. Схема процесса принятия решений	181
5.2.2. Классификация задач принятия решений	184
5.2.3. Классификация методов принятия решений	187
5.2.4. Системы поддержки принятия решений	189
5.3. Принятие решений на основе метода анализа иерархий	190
5.3.1. Иерархическое представление проблемы	190
5.3.2. Структуризация задачи в виде иерархии	191
5.3.3. Парное сравнение альтернатив (метод парных сравнений)	192
5.3.4. Вычисление коэффициентов важности для элементов каждого уровня	201
5.3.5. Подсчет количественной оценки качества альтернатив (иерархический синтез)	211
5.3.6. Метод сравнения объектов относительно стандартов	217
5.3.7. Многокритериальный выбор в иерархиях с различным числом и составом альтернатив под критериями	221
5.4. Методы принятия решений, основанные на исследовании операций	226
5.4.1. Отличительные черты подхода исследования операций	226
5.4.2. Динамическое программирование	227
Задания к главе 5	234
ПРИЛОЖЕНИЕ 5Л	238
Использование методов принятия решений в разработке комплексной системы защиты информации	238
Литература к главе 5	250