

Кафедрою безпеки інформаційних систем і технологій підготовлено та надруковано навчальний посібник «Безопасность информационных систем и технологий» (російською мовою) автори Есин В.И., Кузнецов А.А., Сорока Л.С.



В учебном пособии рассматриваются современные направления обеспечения безопасности информационных систем и технологий. Излагаются технические, криптографические, программные методы и средства защиты информации. Формулируются проблемы уязвимости современных информационных систем и технологий, рассматриваются вопросы защиты информации в распределенных информационных системах, организационно-правовое обеспечение защиты информации.

Учебное пособие предназначено для студентов и аспирантов высших учебных заведений по направлениям и специальностям подготовки "Безопасность информационных и коммуникационных систем", "Информационные управляющие системы и технологии", "Компьютеризированные системы управления и автоматика", слушателей курсов повышения квалификации, а также для широкого круга читателей, интересующихся современными проблемами безопасности информационных систем и технологий.

Содержание

<i>Введение</i>	8
I. Основы безопасности информации	9
<i>Глава 1. Роль информации в современном мире и необходимость ее защиты</i>	9
1.1. Информация, ее значение и необходимость защиты в современных условиях.....	9
1.2. Подделка документов.....	24
<i>Глава 2. Угрозы безопасности информационным системам</i>	29
2.1. Случайные угрозы.....	30
2.2. Преднамеренные угрозы.....	31
2.3. Классификации угроз.....	36
<i>Глава 3. Каналы утечки информации</i>	42
3.1. Характеристика основных каналов утечки информации.....	42
3.2. Каналы утечки информации при эксплуатации ЭВМ.....	62
<i>Глава 4. Угрозы безопасности программному обеспечению</i>	69
4.1. Угрозы безопасности программному обеспечению информационных систем.....	69
4.2. Общая характеристика и классификация вредоносных программ....	74
II. Методы и средства защиты информации в информационных системах	116
<i>Глава 5. Защита информации от случайных угроз</i>	116
5.1. Классификация методов защиты информации от случайных угроз... 116	
5.2. Характеристика методов и средств защиты информации.....	116
<i>Глава 6. Технические методы и средства защиты информации</i>	130
6.1. Классификация технических средств защиты.....	130
6.2. Характеристика методов и средств защиты.....	131
<i>Глава 7. Защита информации от несанкционированного доступа</i>	154
7.1. Принципы защиты информации от несанкционированного доступа. 154	
7.2. Методы идентификации и аутентификации пользователей.....	159
<i>Глава 8. Криптографические методы защиты информации</i>	177
8.1. Основные понятия и история криптографии.....	177
8.2. Шифр замены.....	185
8.3. Шифр перестановки.....	193
8.4. Шифр Вернама и проблема практического использования абсолютно стойкого шифра.....	198
8.5. Классификация шифров.....	204
8.6. Краткая характеристика шифров с ключом.....	204
8.7. Симметричная криптография.....	212
8.7.1. Основы построения потоковых шифров.....	212
8.7.2. Линейные регистры сдвига.....	219

8.7.3. Нелинейные потоковые шифры.....	224
8.7.4. Основы блочного шифрования.....	226
8.7.5. Режимы блочного шифрования.....	231
8.7.5.1. Режим электронной кодовой книги.....	231
8.7.5.2. Режим сцепления блоков шифртекста.....	235
8.7.5.3. Режим обратной связи по шифру.....	240
8.7.5.4. Режим обратной связи по выходу.....	244
8.7.6. Сети Фейстеля.....	247
8.7.7. Стандарт шифрования DES.....	255
8.7.8. Стандарт шифрования ГОСТ.....	261
8.7.9. Шифр TEA.....	263
8.7.10. Шифр IDEA.....	264
8.7.11. Открытый конкурс США на криптостандарт блочного шифрования и его результаты.....	267
8.7.11.1. Шифр MARS.....	270
8.7.11.2. Шифр RC6.....	279
8.7.11.3. Шифр Serpent.....	282
8.7.11.4. Шифр TwoFish.....	284
8.7.11.5. Шифр RIJNDAEL.....	286
8.7.12. Европейский криптопроект NESSIE.....	295
8.7.13. Национальный конкурс по разработке стандарта симметричного блочного криптоалгоритма Украины.....	296
8.7.13.1. Симметричный блочный криптографический алгоритм «Калина».....	296
8.7.13.2. Симметричный блочный криптографический алгоритм «Мухомор».....	326
8.7.13.3. Симметричный блочный криптографический алгоритм «Лабиринт».....	345
8.7.13.4. Симметричный блочный криптографический алгоритм RSB-32.....	363
8.7.13.5. Симметричный блочный криптографический алгоритм ADE.....	375
8.8. Асимметричная криптография.....	410
8.8.1. Основные принципы асимметричной криптографии.....	410
8.8.2. Схема асимметричного шифрования RSA.....	414
8.8.3. Схема асимметричного шифрования Рабина.....	419
8.8.4. Схема асимметричного шифрования Эль Гамала.....	420
8.8.5. Электронная цифровая подпись.....	422
8.9. Основные типы криптоаналитического вскрытия.....	426
8.9.1. Методы криптоанализа.....	432
8.10. Стойкость криптографических систем.....	450

8.11. Управление криптографическими ключами.....	454
8.11.1. Генерация ключей.....	454
8.11.2. Хранение ключей.....	457
8.11.3. Распределение ключей.....	462
8.11.4. Депонирование ключей.....	474
<i>Глава 9. Программные методы и средства защита.....</i>	<i>479</i>
9.1. Программное обеспечение и информационная безопасность.....	479
9.1.1. Основные механизмы информационной безопасности в программном обеспечении.....	479
9.1.2. Контроль жизненного цикла программного обеспечения.....	485
9.1.3. Защита программного обеспечения.....	489
9.2. Защита от вредоносного программного обеспечения.....	501
9.2.1. Методы и средства защиты от вредоносного программного обеспечения.....	501
9.2.2. Организация системы антивирусной защиты.....	526
<i>Глава 10. Защита информации в распределенных информационных системах.....</i>	<i>536</i>
10.1. Межсетевые экраны	538
10.2. Технология VPN.....	547
10.3. Сканеры уязвимости.....	553
<i>Глава 11. Организационно-правовое обеспечение защиты информации..</i>	<i>563</i>
11.1. Основные международные стандарты по информационной безопасности.....	563
11.1.1. Требования к безопасности информационных систем в США..	564
11.1.2. Требования к безопасности информационных систем в России	568
11.1.3. Известные международные стандарты по информационной безопасности.....	574
11.1.4. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа, введенные в действие в Украине.....	592
11.2. Организационные мероприятия по защите информации.....	599
<i>Приложение 1.....</i>	<i>610</i>
<i>Глоссарий.....</i>	<i>639</i>
<i>Список используемой литературы.....</i>	<i>649</i>

Зацікавлені в придбанні можуть звертатися: CSD@univer.kharkov.ua

Зараз готується до видання посібник (за грифом МОН України) українською мовою «Безпека інформаційних систем та технологій» тих же авторів.