

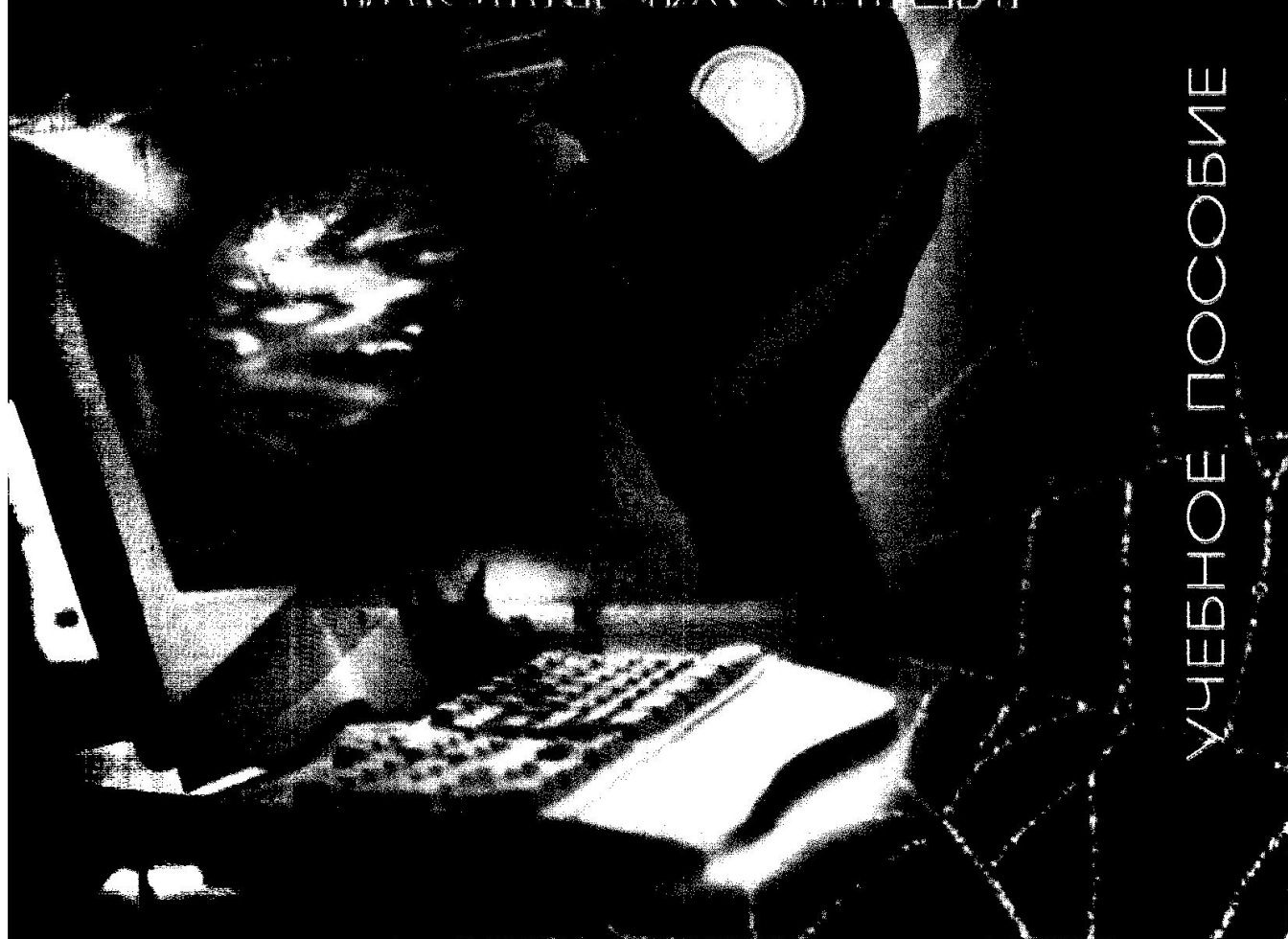


ЕВРОПЕЙСКИЙ УНИВЕРСИТЕТ

Н.Г.Мелволев / Л.В.Москалик

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

УЧЕБНОЕ ПОСОБИЕ



Н.Г. Медведев, Д.В. Москалик

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Учебное пособие

Киев

Издательство Европейского университета
2002

СОДЕРЖАНИЕ

1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Виртуальные частные сети и информационные сети общего пользования	5
1.2. Основные понятия компьютерной безопасности	6
1.3. Особенности безопасности компьютерных сетей	7

2. НАПАДЕНИЕ

2.1. Классификация компьютерных атак	8
2.2. Статистика самых распространенных атак	9
2.3. Анализ сетевого трафика сети Internet	10
2.4. Ложный ARP-сервер в сети Internet	11
2.5. Ложный DNS-сервер в сети Internet	12
2.6. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet лож- ного маршрутизатора	14
2.7. Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)	15
2.8. Направленный шторм ложных TCP-запросов на создание соединения	16
2.9. Атаки, использующие ошибки реализации сетевых служб	18
2.10. Атака через WWW	18
2.11. Причины успеха удаленных атак	19

3. ЗАЩИТА

3.1. Проблемы защиты информации	23
3.2. Базовые методы защиты от удалённых атак в сети Internet	26
3.3. Современные криптографические методы	27
3.3.1. Введение в криптографию	27
3.3.2. Краткое описание основных алгоритмов шифрования данных	33
3.3.3. Алгоритм RSA	43
3.3.4. Оценка надежности криптосистем	45
3.4. Почему криптосистемы ненадежны?	47

4. ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ

<i>4.1. Совместимость.</i>	69
<i>4.2. Безопасность.</i>	72
<i>4.3. Доступность.</i>	74
<i>4.4. Управляемость.</i>	74

5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В INTRANET

<i>5.1. Разработка сетевых аспектов политики безопасности</i>	76
<i>5.2. Безопасность программной среды</i>	79
<i>5.3. Аутентификация в открытых сетях</i>	81
<i>5.4. Концепция передачи данных в открытых сетях</i>	82

6. ЗАКЛЮЧЕНИЕ

<i>Internet: эволюция философии защиты.</i>	85
---	----

7. СПИСОК СПЕЦИАЛЬНЫХ ТЕРМИНОВ

8. СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Навчальне видання

МЕДВЕДЄВ Микола Георгійович
МОСКАЛИК Дмитро Володимирович

АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Навчальний посібник

Редактор *О. О. Івлєв*
Комп'ютерна верстка та дизайн *Н. М. Іванченко*
Оформлення обкладинки *О. С. Сідавського*

Підписано до друку 09.09.2002. Формат 84×108 1/32.
Папір офсетний. Гарнітура Таймс.
Ум. друк. арк. 5,04. Обл.-вид. арк. 4,45.
Тираж 500 прим. Зак. № *16-215*.

Видання надруковано з оригінала-макета, підготовленого
Видавництвом Європейського університету.
03179, Україна, Київ-179, вул. М. Ушакова, 8а.

Реєстраційне свідоцтво ДК № 603 від 19.09.2001.