

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

Книга содержит обширную информацию о работе беспроводных сетей во всем мире, знакомит с методами усиления безопасности данных, связанными с карманными персональными компьютерами, сотовыми терминалами и другими беспроводными устройствами. Вниманию читателя представлено подробное рассмотрение причин уязвимости беспроводных сетей и анализ таких специфических угроз, как подслушивание или атака типа «отказ в обслуживании». Описаны принципы действия сетей беспроводной передачи данных ближнего, дальнего и среднего радиусов действия и соответствующие стандарты, а также основные протоколы безопасности, включая SSL, WTLS, 802.1x и IPSec. Примеры реального внедрения беспроводных технологий, описание организации безопасного доступа к бизнес-приложениям и будущих возможностей сетей третьего поколения помогут снизить риск угроз нападения и сохранить безопасность беспроводных коммуникаций.



www.dmk-press.ru

Internet-магазин
www.aliants-kniga.ru

Книга-почтой:
Россия, 123242, Москва, а/я 20
e-mail: orders@aliants-kniga.ru

Оптовая продажа:
“Альянс-книга”
(495)258-9194, 258-9195
e-mail: books@aliants-kniga.ru

ISBN 5-94074-248-3



БЕЗОПАСНОСТЬ
БЕСПРОВОДНЫХ СЕТЕЙ



БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

Мерритт Максим
Дэвид Полино

Перевод с английского Семенова А. В.



А

Мерритт Максим, Дэвид Поллино

БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

Информационные технологии для инженеров



Москва

А

**УДК 004.056.5
ББК 32.973.202
М17**

Максим М.

- М17** Безопасность беспроводных сетей / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. – М. : Компания АйТи; ДМК Пресс. – 288 с.: ил. – (Информационные технологии для инженеров).

ISBN 5-98453-007-4 (АйТи) – ISBN 5-94074-248-3 (ДМК Пресс)

Книга содержит обширную информацию о работе беспроводных сетей во всем мире, знакомит с методами усиления безопасности данных, связанными с карманными персональными компьютерами, сотовыми терминалами и другими беспроводными устройствами. Вниманию читателя представлено подробное рассмотрение причин уязвимости беспроводных сетей и анализ таких специфических угроз, как подслушивание или атака типа «отказ в обслуживании». Описаны принципы действия сетей беспроводной передачи данных ближнего, дальнего и среднего радиусов действия и соответствующие стандарты, а также основные протоколы безопасности, включая SSL, WTLS, 802.1x и IPSec. Примеры реального внедрения беспроводных технологий, описание организации безопасного доступа к бизнес-приложениям и будущих возможностей сетей третьего поколения помогут снизить риск угроз нападения и сохранить безопасность беспроводных коммуникаций.

Original English language published by The McGraw-Hill Companies. Copyright © by The McGraw-Hill Companies. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 0-07-222286-7 (англ.)

Copyright © by The McGraw-Hill Companies

ISBN 5-98453-007-4 (АйТи)

© Перевод на русский язык.
Компания АйТи

ISBN 5-94074-248-3 (ДМК Пресс)

© Издание на русском языке,
оформление. ДМК Пресс

Содержание

Предисловие	12
ЧАСТЬ I	
Введение в беспроводной мир	15
Глава 1	
Добро пожаловать в мир беспроводных технологий!	16
История развития беспроводных технологий	18
1970-е годы: первые беспроводные сети	19
1980-е годы: рынок услуг беспроводной связи начинает развиваться	20
1990-е годы: позиция беспроводных сетей на рынке укрепляется	23
Середина 1990-х годов: появление новых беспроводных сетей	25
Конец 1990-х годов: появление беспроводной Internet-связи	26
История вопроса безопасности беспроводных сетей	30
Подслушивание и создание помех	31
Беспроводные Internet-технологии:	
безопасность становится главной темой	32
Беспроводная цепь добавленной стоимости	33
Состояние беспроводной отрасли в 2001 году	39
Беспроводные технологии в Северной Америке: 2001 год	39
Беспроводные технологии в Европе: 2001 год	46
Беспроводные технологии в Японии: 2001 год	49
Беспроводные технологии в Азии: 2001 год	52
Заключение	53
Глава 2	
Угрозы безопасности беспроводных сетей	54
Неконтролируемая территория	54
Подслушивание	54
Глушение	56
Отказ в обслуживании	56
Вторжение и модификация данных	57
Атака «man in the middle»	58
Абонент-мошенник	58
Ложные точки доступа в сеть	59

Оборудование атакующего	61
Тайные беспроводные каналы	64
Проблемы роуминга	66
Угрозы криптозащиты	67
Заключение	67

Глава 3

Общие сведения о протоколах беспроводной безопасности и криптографии.....69

Побеждая страх, неопределенность и сомнения	69
Модель OSI	70
Упрощенная модель OSI	71
Internet-модель	72
Протоколы безопасности для локальных беспроводных сетей (WLAN).....	72
Криптография	73
Протокол SSL/TLS	74
Протокол SSH	75
Протокол или программа?	76
Доступ с терминала и передача файлов.....	76
Перенаправление порта	76
Несколько слов о предосторожности	77
Атаки «man in the middle» для SSL/TLS и SSH	78
Протокол WLTS	78
Механизм защиты WEP	79
Протокол 802.1x	80
Протокол IPSec	81
Заключение	82

Глава 4

Безопасность беспроводных устройств.....83

Проблемы безопасности беспроводных устройств	83
Физическая безопасность	83
Утечка информации.....	84
Решения, обеспечивающие безопасность устройства.....	85
Безопасность приложений.....	86

Детальный анализ устройств	86
Ноутбуки	86
Карманные компьютеры	89
Беспроводная инфраструктура	90
Мобильные телефоны	91
Заключение	92
ЧАСТЬ II	
Технологии беспроводных сетей	93
Глава 5	
Основные сведения о сотовых сетях	94
Технология FDMA	95
Технология TDMA	96
Технология CDMA	98
Основная информация о распределенном спектре	99
Аналогия.....	99
TDMA против CDMA	101
Технология PDC	102
Технология iDEN: еще одна альтернатива для американских пользователей	104
Угрозы безопасности	105
Типы мошенничества в сотовых сетях.....	106
Борьба с мошенничеством	107
Общие принципы безопасности	108
Внутри GSM	110
GSM-безопасность.....	112
Анализ GSM-алгоритмов.....	115
Внутри CDMA	118
Почему нельзя использовать общедоступные ключи для сотовой аутентификации?.....	119
Сотовая сеть и безопасность.....	123
Прогнозы на будущее	127
Глава 6	
Введение в беспроводные сети передачи данных	129
Сотовые цифровые пакеты данных (CDPD)	131
Архитектура CDPD	132
Безопасность CDPD	132

Mobitex.....	135
Архитектура Mobitex.....	135
Услуги GPRS – General Packet Radio Service.....	141
GPRS-архитектура	144
Вопросы безопасности GPRS	145
GPRS-безопасность.....	147
Введение в WAP-протокол.....	150
WAP-устройство.....	151
WAP-шлюз	153
Модель WAP-безопасности	154
Заключение.....	157

Глава 7

Стандарты беспроводных сетей	159
Нынешние и будущие технологии	159
Инфракрасное излучение.....	159
Радиоволны	160
Распределенный спектр	161
Метод OFDM	161
Существующие и готовящиеся стандарты	162
Стандарт IEEE 802	162
Стандарт 802.11	162
Основы стандарта 802.11	163
Интерфейс 802.11b.....	164
Интерфейс 802.11a.....	164
Интерфейс 802.11g.....	166
Интерфейс 802.11j	167
Интерфейсы 802.11h и 5GPP.....	167
Интерфейс 802.11e	167
Интерфейс 802.11i	167
Интерфейс 802.11f	168
Интерфейс IEEE 802.15	169
Интерфейс IEEE 802.16	170
Интерфейс IEEE 802.1x	171
Интерфейс ETSI	171
Технология Bluetooth	173
Стандарт HomeRF.....	173
Ультраширокополосное радио	174
Заключение.....	174

ЧАСТЬ III

Стратегии построения беспроводных сетей	175
Глава 8	
Внедрение беспроводных LAN: соображения безопасности	176
Общие приложения беспроводной сети	176
Физическая безопасность	177
Сетевая безопасность.....	179
Рекомендации по обеспечению безопасности приложений.....	184
Проекты на территории предприятий	184
Корпоративный проект 1	184
Корпоративный проект 2	186
Гостевая корпоративная сеть	187
Корпоративная конфигурация «точка–точка».....	189
Проект беспроводного ISP	190
Решения для торговли и производства.....	190
Решение для торговых агентов	190
Решение для склада.....	192
Решение для малого предприятия или домашнего офиса (SOHO).....	194
Заключение	196
Глава 9	
Предоставление безопасного беспроводного доступа к данным	197
Планирование беспроводной передачи данных:	
первые важные шаги.....	201
Потенциальные сценарии беспроводных приложений.....	203
Варианты беспроводной политики	208
Беспроводная логистика	209
Политики беспроводной безопасности	210
Заключение	213
Глава 10	
Примеры беспроводных проектов	215
Реальные примеры внедрений	219
Пример 1.....	219
Пример 2.....	221
Пример 3.....	223
Пример 4.....	224
Пример 5.....	226
Пример 6.....	227
Первая характеристика – простота.....	230

Вторая характеристика – гибкость.....	230
Третья характеристика – масштабируемость.....	230
Четвертая характеристика – интегральность	231
Пятая характеристика – мотивация пользователей.....	231
Заключение.....	231
Глава 11	
Будущее беспроводных сетей.....	233
Сети 3G.....	234
Статус 3G-сетей в мире (2002 год)	235
Что такое <i>EDGE</i> ?.....	237
Что ожидает сетевых операторов?.....	238
Подождите – на подходе сети 4G!	239
Что нас ждет впереди – беспроводные сети?.....	242
Новые беспроводные продукты	244
Новые рынки беспроводных сетей	245
Столкновение двух миров.....	246
Взгляд в будущее – ключевые моменты	246
Переход к беспроводной связи.....	248
Заключение.....	250
Глава 12	
Оценка беспроводных LAN.....	251
С чего начать	251
Беспроводная политика	252
Процесс.....	253
Сбор информации	253
Что искать?	254
Анализ данных.....	255
Организация данных.....	255
Нанесение на карту области покрытия	255
Дальнейшие действия.....	255
Проверка информации и принятие мер безопасности.....	256
Текущая оценка	257
Развивающиеся рынки.....	257
Заключение.....	258
Глоссарий	260
Предметный указатель	273