

**УДК 004.056**  
**ББК 32.973.202**  
**P24**

- P24 Кристиан Барнс, Тони Боутс, Дональд Лойд, Эрик Уле, Джеффри Посланс, Дэвид М. Зенджан, Нил О'Фаррел**  
 Защита от хакеров беспроводных сетей: Пер. с англ. А. В. Семенова. – М.: Компания АйТи; ДМК-Пресс. – 480 с.: ил. (Серия «Информационная безопасность»).

**ISBN 5-98453-012-0**

Цель этой книги – предоставить максимально исчерпывающую информацию о беспроводных коммуникациях людям, работающим во всех сферах бизнеса и информационных технологий, подготавливают ли они реальный бизнес-план для беспроводного проекта, являются ли они IS/IT-специалистами, планирующими новое беспроводное внедрение, включают ли они беспроводные возможности в домашнюю сеть, реагируют ли на атаку на их сеть или просто любят заниматься проблематикой безопасности.

**УДК 004.056**  
**ББК 32.973.202**

Original English language edition published by Singress Publishing, Inc. Copyright © by Singress Publishing, Inc. 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 1-928994-59-8 (англ.) Copyright © by Singress Publishing, Inc.  
 ISBN 5-98453-012-0 (АйТи) © Перевод на русский язык. Компания АйТи  
 © Оформление, издание. ДМК-Пресс

# Содержание

<b>Предисловие</b>	<b>17</b>
<b>Глава 1. Беспроводной вызов</b>	<b>19</b>
Введение	20
Обзор беспроводных технологий	21
Определение беспроводных решений на базе сотовых сетей	21
Определение беспроводных LAN	21
Конвергенция беспроводных технологий	22
Тенденции и статистика	22
Рост использования беспроводных приложений	22
Ближайшее беспроводное будущее	24
Понимание перспектив беспроводной технологии	26
Беспроводные сети	28
Преимущества беспроводных технологий	33
Удобство	34
Доступность	39
Скорость	39
Эстетика	41
Производительность	41
Беспроводная реальность сегодня	41
Конфликты стандартов	42
Коммерческие конфликты	44
Проблемы принятия рынком	44
Ограничения «радио»	44
Ограничения беспроводной безопасности	49
Проверка беспроводных стандартов	56
Сотовые беспроводные сети	56
Беспроводные LAN	63
Инфраструктура общедоступных ключей в беспроводных сетях	79
Заключение	85

## Ответы на ваши беспроводные вопросы

**Вопрос:** Будет ли i-Mode распространяться в Европе или Северной Америке?

**Ответ:** Хотя владелец i-Mode, компания NTT DoCoMo имеет заметные доли в пакетах акций нескольких северо-американских и европейский сотовых операторов, нет планов быстрого вывода i-Mode в современном виде на эти рынки. Это обусловлено прежде всего ограниченной скоростью доступа 9,6 Кб/с.

	Краткое изложение решений	86
	Часто задаваемые вопросы	89
<b>Средства и ловушки</b>	<b>Глава 2. Основы безопасности</b>	<b>91</b>
<b>Текстовая аутентификация</b>	Введение	92
Пример генератора словаря паролей для атак грубой силы, который может создавать этот словарь на основе набора букв, можно отыскать в Интернете на сайте <a href="http://www.dmzs.com/tools/files">www.dmzs.com/tools/files</a> . Есть и другие генераторы для атак грубой силы на POP: Telnet, FTP, Web и т. п., их можно найти на <a href="http://packetstormsecurity.com/crackers">http://packetstormsecurity.com/crackers</a> .	Основы систем безопасности и принципы защиты	92
	Обеспечение конфиденциальности	93
	Обеспечение целостности	94
	Обеспечение наличия	96
	Обеспечение неприкосновенности конфиденциальной информации	97
	Обеспечение аутентификации	97
	Обеспечение авторизации	102
	Обеспечение невозможности отказа	103
	Следы создания отчетов и аудита	106
	Использование шифрования	108
	Шифрование голоса	109
	Системы шифрования данных	110
	Обзор роли политики	110
	Идентификация ресурсов	112
	Критерии классификации	114
	Внедрение политики	114
	Определение стандартов безопасности и конфиденциальности	116
	Обзор стандартов безопасности	118
	Обзор стандартов конфиденциальности и их регулирование	122
	Обзор общих угроз и рисков	128
	Случай потери данных	129
	Случай отказа от предоставления услуг или разрушения услуг	129
	Прослушивание	131
	Предупреждение последствий организационных потерь	133
	Заключение	135

Краткое изложение решений	136
Часто задаваемые вопросы	139

## Фиксированные беспроводные технологии

В беспроводных фиксированных сетях и передатчик, и приемник постоянно находятся в определенном месте в отличие от мобильных сетей. Эти сети используют питание от переменного тока. Они могут быть организованы по схеме «точка-точка» или же «точка-многоточка» и могут использоваться как лицензируемый, так и нелицензируемый спектр.

## Глава 3. Архитектура и проектирование беспроводных сетей 141

Введение	142
Фиксированные беспроводные технологии	143
Услуга многоканального распределения сигнала между многими точками (MMDS)	144
LMDS – локальные услуги распределения сигнала по многим точкам	145
WLL (Wireless Local Loop – беспроводная локальная петля)	147
Микроволновая связь «точка-точка»	147
Беспроводные локальные сети – WLAN	149
Зачем нужен беспроводной стандарт LAN?	149
Развитие WLAN через архитектуру 802.11	158
Основной набор услуг	158
Расширенный набор услуг	160
Механизм CSMA-CA	162
Модульная конфигурация	164
Использование вариантов управления мощностью	164
Роуминг между многими ячейками	165
Безопасность WLAN	166
Развитие персональных сетей WPAN посредством архитектуры 802.15	167
Bluetooth	168
HomeRF	170
Высокопроизводительная радио LAN	171
Мобильные беспроводные технологии	171
Технологии первого поколения	173
Технологии второго поколения	174
Технология 2,5G	174
Технологии третьего поколения	174
Протокол беспроводных приложений WAP	175

Глобальная система мобильных коммуникаций	176
Пакетная радиослужба GPRS	178
Услуга коротких сообщений	179
Беспроводные оптические технологии	179
Исследование процесса проектирования	180
Проведение предварительных исследований	180
Анализ существующего окружения	181
Предварительное проектирование	182
Окончательное проектирование	182
Реализация внедрения	183
Создание документации	184
Создание методологии проектирования	184
Создавая сетевой план	185
Разработка сетевой архитектуры	191
Формализация стадии детального проектирования	195
Понимание атрибутов беспроводной сети в аспекте проектирования	200
Поддержка приложений	201
Природный ландшафт	204
Топология сети	206
Заключение	208
Краткое изложение решений	210
Часто задаваемые вопросы	214
<b>Глава 4. Распространенные атаки и уязвимости</b>	<b>215</b>
Введение	216
Слабости WEP	216
Критика общего проектирования	217
Слабость алгоритма шифрования	219
Слабости управления ключами	222
Слабости в поведении пользователей	225
Проведение разведки	227
Нахождение сети	227

<b>Заметки из подполья</b>	Нахождение слабостей в мишени	228
	Использование этих слабостей	229
<b>Шлюз компании Lucent Technologies сообщает SSID открытым текстом даже в сетях с шифрованием</b>	Вынюхивание, перехват и прослушивание	230
	Определение вынюхивания	231
	Устройства для вынюхивания	231
	Сценарий для вынюхивания	231
	Защита от вынюхивания и подслушивания	233
Как было объявлено в Интернете на сайте <a href="http://www.securiteam.com/securitynews/5ZP0I154UG.html">www.securiteam.com/securitynews/5ZP0I154UG.html</a> , шлюз компании Lucent открывает атакующему простой путь для соединения с закрытой сетью. Чтобы соединиться с беспроводной сетью, пользователь должен знать SSID сети. Даже если сеть защищена при помощи WEP, часть передаваемых посланий шлюз передает в незашифрованном виде, включая SSID. Все, что должен сделать атакующий, – это «вынюхивать» сеть для определения ее SSID, после этого он сможет соединиться с сетью.	Подмена устройства и неавторизованный доступ	235
	Определение «подмены»	235
	Набор средств для «подмены»	236
	Сценарий «подмены»	236
	Защита от подмены и неавторизованных атак	237
	Модификация сети и ее ограбление	238
	Определение ограбления	238
	Набор средств для ограбления	239
	Сценарий «ограбления»	240
	Защита от модификации сети и ее ограбления	240
	Отказ от предоставления услуги и атаки переполнения	241
	Определение атак переполнения и отказа от предоставления услуг	241
	Набор средств для DoS	242
	Сценарий DoS и переполнения	242
	Защита от атак DoS и переполнения	243
	Введение в злонамеренное ПО	243
	Кражи пользовательских устройств	245
	Заклучение	247
	Краткое изложение решений	247
	Часто задаваемые вопросы	251
<b>Глава 5. Контрмеры для обеспечения беспроводной безопасности</b>		<b>253</b>
	Введение	254

## Стратегии для анализа угроз

- определить активы компании;
- определить возможные доступы к ним в точки зрения авторизации;
- определить вероятность того, что неавторизованный пользователь сможет получить доступ к этим активам;
- определить потенциальные потери;
- определить стоимость восстановления после потерь и ремонтных работ или оценить потери;
- определить необходимые контрмеры безопасности;
- определить стоимость внедрения контрмер;
- сравнить стоимость обеспечения безопасности ресурсов с величиной потерь.

Политика повторных визитов	255
Обращение к проблемам при помощи политики	257
Анализ угрозы	259
Угроза = риск + уязвимость	260
Проектирование и развертывание безопасной сети	266
Внедряя WEP	271
Определение WEP	271
Обеспечение конфиденциальности при помощи WEP	272
Процесс аутентификации в WEP	273
Преимущества и выгоды WEP	273
Недостатки WEP	274
Смысл безопасности при использовании WEP	274
Внедрение WEP в продуктах Aironet	274
Внедрение WEP в Orinoco AP-1000	275
Обеспечение безопасности WLAN при помощи WEP: примерный сценарий	276
Фильтрация MAC-адресов	278
Определение фильтрации MAC	279
Выгоды и преимущества от использования MAC-адресов	280
Недостатки MAC	280
Обеспечение безопасности при помощи фильтрации MAC-адресов	281
Внедрение MAC-фильтров в AP-1000	281
Внедрение MAC-фильтров в Aironet 340	281
Фильтрация MAC-адресов: сценарий конкретного случая	285
Фильтрация протоколов	285
Определение фильтров протокола	285
Преимущества и выгоды от применения фильтрации протокола	286
Недостатки фильтрации протокола	287

Аспекты безопасности при использовании фильтров протокола	287
Использование закрытых сетей и систем	287
Определение закрытой системы	287
Выгоды и преимущества закрытой системы	289
Недостатки закрытой системы	289
Аспекты безопасности в использовании закрытой системы	289
Закрытие сети на оборудовании Cisco Aironet серии AP	290
Закрытие сети на оборудовании ORiNOCO AP-1000	291
Пример внедрения закрытой системы	291
Включение WEP на устройстве ORiNOCO	291
Распределение IP-адресов	292
Выделение IP-адресов во WLAN	292
Развертывание IP-адресов во WLAN: выгоды и преимущества	293
Развертывание IP-адресов во WLAN: недостатки	294
Проблемы безопасности при развертывании IP-адресов во WLAN	294
Пример развертывания IP-адресов во WLAN	295
Использование VPN	295
Преимущества и выгоды от VPN	297
Недостатки VPN	298
Аспекты безопасности при использовании VPN	299
Выстраивание защиты с использованием VPN	299
Использование VPN, пример внедрения	300
Безопасность пользователей	301
Выгоды и преимущества от безопасности конечных пользователей	304
Недостатки от безопасности конечного пользователя	305
Безопасность пользователя: пример внедрения	305



Заключение	306
Краткое изложение решений	307
Часто задаваемые вопросы	310

**Активное вождение**

Активное вождение – это термин, обозначающий действия людей, которые перемещаются, имея в своем распоряжении беспроводное оборудование для отслеживания других беспроводных сетей. Термин образован по аналогии с термином «активный обзвон», относящимся к хорошо известной практике постоянного перебора определенного набора номеров через модем, чтобы обнаружить соединенные с ними компьютеры.

**Глава 6. Проникновение  
сквозь меры безопасности****311**

Введение	312
Планирование и подготовка	312
Нахождение мишени	313
Обнаружение открытой системы	314
Выявление закрытой системы	315
Использование WEP	315
Безопасность 64-битных и 128-битных ключей	316
Приобретение WEP-ключа	317
Активное вождение	318
К каким угрозам для безопасности сети приводит «открытость сети»?	319
Кража пользовательских устройств	322
В чем явные выгоды от кражи устройств?	323
Фильтрация MAC-адресов	324
Что такое MAC-адрес?	324
Где встречается фильтрация MAC-адресов в процессе аутентификации/ассоциации?	325
Определение фильтрации MAC-адресов включено	326
MAC-спуфинг	326
Обход современных механизмов безопасности	327
Сетевые экраны	328
Что теперь?	330
Использование инсайдеров	331
Что надо узнавать?	331
Мишени социальной инженерии	332
Установка ложной точки доступа	332

Где лучше всего расположить ложную ТД?	333
Конфигурирование ложной ТД	333
Риск, создаваемый ложной ТД	334
Можно ли зарегистрировать ложную ТД?	334
Использование VPN	335
Заключение	336
Краткое изложение решений	337
Часто задаваемые вопросы	340

## Соображения об оборонительном мониторинге

- определите границы вашей беспроводной сети, чтобы точно знать, когда они будут нарушаться;
- ограничивайте силу сигнала, чтобы сохранить его в пределах сети;
- составьте список всех авторизованных беспроводных точек доступа (ТД) в расположении своей компании; подробное знание их поможет вам быстро локализовать ложную ТД.

## Глава 7. Контроль и обнаружение вторжения

341

Введение	342
Проектирование для обнаружения вторжения	342
Начиная с закрытой сети	343
Устранение проблем, связанных с окружающей средой	344
Исключение интерференции	345
Защитный мониторинг	346
Доступность и обеспечение соединения	346
Контроль за работой сети	350
Стратегии определения вторжения	352
Интегральный мониторинг безопасности	353
Популярные продукты для мониторинга	357
Оценки уязвимости	361
Необходимые действия в случае атаки	363
Политики и процедуры	365
Реакция на вторжение	365
Составление отчета	366
Зачистка	367
Предотвращение вторжения	367
Анализ местности для поиска ложных ТД	368
Размещение ложной ТД	368
Заключение	374

Краткое изложение решений	375
Часто задаваемые вопросы	377

**Аудит**

Аудит беспроводных сетей состоит из нескольких шагов, в которых для проведения определенных действий нужны различные ресурсы или устройства. Эти действия можно подразделить на шесть категорий:

- планирование аудита;
- сбор аудиторской информации;
- анализ собранной информации и создание отчета;
- представление аудиторского отчета;
- обзор ситуации после аудита;
- дальнейшие действия.

**Глава 8. Аудит****379**

Введение	380
Проектирование и планирование успешного аудита	380
Типы аудита	381
Когда проводить аудит	385
Действия в процессе аудита	388
Средства аудита	390
Определяющие факторы успеха аудита	391
Определение стандартов	393
Стандарты	393
Стратегии	394
Полезные советы	394
Политики	394
Процедуры	395
Аудит, стандарты безопасности и полезные советы	395
Корпоративные политики безопасности	397
Хартии аудиторов и неправильное поведение системы	399
Определение границ аудита	401
Организация процесса создания документации	401
Проведение аудита	402
Аудиторы и технологи	402
Получение поддержки от отделов ИТ и ИС	402
Сбор данных	404
Анализ данных аудита	406
Матричный анализ	406
Собрание рекомендаций	406
Создание отчета по результатам аудита	408
Важность качества аудиторского отчета	408

Написание аудиторского отчета	409
Заключительные мысли об аудите	412
Образец аудиторского отчета	412
Заключение	417
Краткое изложение решений	418
Часто задаваемые вопросы	420

## Создание сверхбезопасной WLAN

- Убедитесь, что ваша ТД позволяет вам изменить ESSID, пароли и поддерживает 128-битный WEP.
- Используйте ТД, которая поддерживает функциональность «закрытой сети».
- Будьте уверены, что ваши ТД позволяют проводить модернизацию.
- Изолируйте ТД и регулируйте доступ из их сети в вашу внутреннюю сеть.
- Проводите аудиты вашей сети с использованием NetStumbler или других средств беспроводного сканирования, чтобы убедиться в том, что неавторизованные хакеры не могут получить к ней доступа.
- Обновляйте политику безопасности, чтобы отразить в ней все опасности небезопасной беспроводной сети.

## Глава 9. Примеры внедрений 421

Введение	422
Развертывание беспроводной сети без обеспечения ее безопасности	423
Организация супербезопасной беспроводной LAN	425
Место расположения и доступ	425
Конфигурация ТД	426
Безопасное проектирование	428
Обеспечение безопасности при помощи политики	432
Активное вождение	433
Разведка вашего местоположения	440
Сложные случаи развертывания беспроводных сетей	441
Создание проверочного листа для беспроводной безопасности	443
Минимальная безопасность	443
Средняя безопасность	444
Оптимальная безопасность	445
Заключение	447
Краткое изложение решений	448
Часто задаваемые вопросы	449

## Приложение. Защита вашей беспроводной сети от хакеров 451

Глава 1. Беспроводной вызов	452
Глава 2. Основы безопасности	454

Глава 3. Архитектура и проектирование беспроводных сетей	457
Глава 4. Распространенные атаки и уязвимости	461
Глава 5. Контрмеры для обеспечения беспроводной безопасности	465
Глава 6. Проникновение сквозь меры безопасности	468
Глава 7. Контроль и обнаружение вторжения	470
Глава 8. Аудит	472
Глава 9. Примеры внедрений	474