

**Дж. Макнамара**

**СЕКРЕТЫ  
КОМПЬЮТЕРНОГО  
ШПИОНАЖА**

**ТАКТИКА И КОНТРМЕРЫ**

Перевод с английского  
А.В.Бутко  
под редакцией  
С.М.Молявко



Москва  
БИНОМ. Лаборатория знаний  
2004

УДК 004

ББК 67.408

М15

**Макнамара Д.**

М15 Секреты компьютерного шпионажа: Тактика и контрмеры /  
Д. Макнамара; Пер. с англ.; Под ред. С. М. Молявко. — М.: БИ-  
НОМ. Лаборатория знаний, 2004. — 536 с., ил.  
ISBN 5-94774-168-7 (русск.)  
ISBN 0-7645-3710-5 (англ.)

Обсуждаются средства и методы, которые применяются любителями и про-  
фессионалами в сфере компьютерного шпионажа, а также контрмеры, предна-  
значенные для борьбы с ними. Приводятся общие концепции и технологии, при-  
годные для использования на любых компьютерных системах, поэтому  
пользователи Windows, Linux, OpenBSD и MacOs найдут книгу полезной для  
себя.

Для пользователей персональных компьютеров, системных администраторов  
и всех, кто намерен защитить свои компьютеры от возможных посягательств.

УДК 004  
ББК 67.408

---

Справочное издание

**Макнамара Джоэль**

**Секреты компьютерного шпионажа. Тактика и контрмеры**

Редактор С. Молявко

Корректор Н. Савельева

Художественный редактор О. Лапко

Компьютерная верстка Л. Черепанова, Л. Катуркина

Подписано в печать 27.08.04. Формат 70x100<sup>1</sup>/16. Гарнитура Школьная

Бумага офсетная. Печать офсетная. Усл. печ. л. 43,55

Тираж 3000 экз. Заказ 2679

Издательство «БИНОМ. Лаборатория знаний»

Телефон (095) 955-0398, e-mail: lbz@aha.ru

---



ISBN 5-94774-168-7 (русск.)

ISBN 0-7645-3710-5 (англ.)

Copyright © 2003 by Wiley Publishing, Inc.

All Rights Reserved. Authorized translation  
from the English language edition published by  
John Wiley & Sons, Inc.

© Перевод на русский язык

БИНОМ. Лаборатория знаний, 2004

# Краткое оглавление

<b>Об авторе</b>	<b>13</b>
<b>Благодарности</b>	<b>13</b>
<b>Редакционный коллектив</b>	<b>14</b>
<b>Введение</b>	<b>15</b>
<b>Глава 1. Шпионы</b>	<b>21</b>
<b>Глава 2. Шпионаж и закон</b>	<b>57</b>
<b>Глава 3. Тайные проникновения</b>	<b>89</b>
<b>Глава 4. Проникновение в систему</b>	<b>119</b>
<b>Глава 5. В поиске доказательств</b>	<b>155</b>
<b>Глава 6. Взлом защищенных данных</b>	<b>213</b>
<b>Глава 7. Копирование информации</b>	<b>253</b>
<b>Глава 8. Мониторинг клавиатуры</b>	<b>273</b>
<b>Глава 9. «Троянские кони»</b>	<b>309</b>
<b>Глава 10. Сетевое наблюдение</b>	<b>339</b>
<b>Глава 11. Беспроводные сети 802.11b</b>	<b>387</b>
<b>Глава 12. Офисное оборудование</b>	<b>431</b>
<b>Глава 13. Высший компьютерный шпионаж</b>	<b>463</b>
<b>Приложение. Наша веб-страница</b>	<b>505</b>
<b>Предметный указатель</b>	<b>509</b>

# Оглавление

<b>Об авторе</b>	13
<b>Благодарности</b>	13
<b>Редакционный коллектив</b>	14
<b>Введение</b>	15
<b>О чем эта книга</b>	15
<b>Для кого написана эта книга</b>	17
<b>Структура книги</b>	17
<b>Подводные камни</b>	19
<b>Глава 1. Шпионы</b>	21
<b>Как узнать шпиона</b>	21
<b>За кем наблюдают шпионы, и кто они такие</b>	23
Экономический шпионаж	25
Начальство и наблюдение за сотрудниками	28
Полицейские расследования	30
Частные сыщики и консультанты – неофициальные расследования	33
«Невидимки» – поддерживаемые правительством агенты разведки	36
Преступники – те, кто ищет собственную выгоду	40
Доносчики, действующие ради всеобщего блага	41
Друзья и семья – с ними только в разведку ходить...	44
<b>Определите свой уровень паранойи</b>	47
<b>Анализ рисков 101</b>	49
Пять шагов анализа рисков	51
<b>Заключение</b>	55
<b>Глава 2. Шпионаж и закон</b>	57
<b>Законы о шпионаже</b>	57
Закон об уличной безопасности 1968 года (часть III – телефонное прослушивание)	58
Закон об иностранной разведке 1978 года	61
Закон о защите электронных систем связи 1986 года	64
Закон о компьютерном мошенничестве и злоупотреблениях 1986 года	67
Закон об экономическом шпионаже 1996 года	70
Законы штатов	71

<b>Патриотический Акт 2001 года</b>	<b>72</b>
Законы о прослушивании линий связи и доступе к хранимой информации	73
Закон об иностранной разведке	74
Закон о компьютерном мошенничестве и злоупотреблениях	76
Другие положения	78
Законы штатов	78
<b>Реалии соблюдения законодательства</b>	<b>79</b>
<b>Гражданский и уголовный суд</b>	<b>81</b>
<b>Начальство и подчиненные – узаконенный шпионаж</b>	<b>83</b>
<b>Внутрисемейные судебные разбирательства</b>	<b>85</b>
<b>Заключение</b>	<b>87</b>
<hr/> <b>Глава 3. Тайные проникновения</b>	<b>89</b>
<b>Взгляд изнутри</b>	<b>89</b>
Физические и сетевые проникновения	91
Запланированные и случайные проникновения	92
<b>Шпионская тактика</b>	<b>93</b>
Шпионские игры	93
Проникновения, санкционированные правительством: взгляд изнутри	94
<b>Использование уязвимых мест</b>	<b>101</b>
Анализ и планирование операции	101
Проникновение в офис	103
Документирование обстановки	108
<b>Контрмеры</b>	<b>111</b>
Физическая безопасность	111
Политика безопасности	114
<b>Заключение</b>	<b>117</b>
<hr/> <b>Глава 4. Проникновение в систему</b>	<b>119</b>
<b>Шпионская тактика</b>	<b>119</b>
Использование слабых мест	120
Средства проникновения в систему	140
<b>Контрмеры</b>	<b>149</b>
Настройки безопасности	149
Надежные пароли	154
Шифрование	154
<b>Заключение</b>	<b>154</b>

<b>Глава 5. В поиске доказательств</b>	<b>155</b>
<b>Законное наблюдение</b>	<b>155</b>
Как работают компьютерные полицейские	156
Конфискация	160
Дублирование информации	163
Экспертиза	164
<b>Шпионская тактика</b>	<b>166</b>
Использование слабых мест	166
Средства сбора доказательств	186
<b>Контрмеры</b>	<b>193</b>
Шифрование	194
Стеганография	202
Программы безвозвратного удаления файлов	206
Программное обеспечение для уничтожения доказательств	209
<b>Заключение</b>	<b>211</b>
<b>Глава 6. Взлом защищенных данных</b>	<b>213</b>
<b>Шпионская тактика</b>	<b>213</b>
Использование слабых мест	215
Утилиты взломщика	230
<b>Контрмеры</b>	<b>240</b>
Стойкое шифрование	240
Политики паролей	241
Списки паролей	244
Альтернативы паролю	245
<b>Заключение</b>	<b>251</b>
<b>Глава 7. Копирование информации</b>	<b>253</b>
<b>Шпионская тактика</b>	<b>253</b>
Используйте доступные ресурсы	254
Применяйте программы архивации	254
Исследуйте другие источники информации	255
Досконально изучите процесс копирования информации	255
<b>Необходимые носители информации</b>	<b>257</b>
Дискеты	257
CD-R/CD-RW	258
DVD	261
ZIP-диски	262
Устройства внешней памяти	262

Жесткие диски	264
Жесткие диски USB	268
Системы резервного копирования на магнитной ленте	269
<b>Альтернативные методы копирования данных</b>	<b>269</b>
Передача данных по сети	270
Цифровые камеры	271
<b>Заключение</b>	<b>271</b>
<b>Глава 8. Мониторинг клавиатуры</b>	<b>273</b>
<b>Что такое keylogger</b>	<b>273</b>
<b>Шпионская тактика</b>	<b>274</b>
Использование слабых мест	275
Средства мониторинга клавиатуры	286
<b>Контрмеры</b>	<b>291</b>
Просмотр установленных программ	293
Анализ автоматически загружаемых программ	293
Анализ активных процессов	295
Отслеживание процессов, ведущих запись в файл	296
Удаление исполняемых библиотек VB	298
Поиск уникальной строки	299
Использование персональных брандмаузеров	299
Использование программ проверки целостности файлов и реестра	299
Использование ПО для обнаружения keylogger	300
Использование программ перехвата сетевых пакетов	303
Обнаружение аппаратных keylogger-модулей	303
Использование паролей для работы с аппаратными keylogger-модулями	304
Использование Linux	306
Просмотр журнала системных ошибок	306
Удаление программ мониторинга клавиатуры	306
<b>Заключение</b>	<b>308</b>
<b>Глава 9. «Троянские кони»</b>	<b>309</b>
<b>Шпионская тактика</b>	<b>310</b>
Использование уязвимых мест	310
Троянские кони	325
<b>Контрмеры</b>	<b>331</b>
Сетевая защита	332
Использование мониторов реестра и программ проверки целостности файлов	333
Использование антивирусного программного обеспечения	334

Использование специального ПО для обнаружения троянских коней	335
Избавление от троянских коней	336
Использование программ сторонних разработчиков	337
<b>Заключение</b>	<b>337</b>
<hr/>	
<b>Глава 10. Сетевое наблюдение</b>	<b>339</b>
<hr/>	
<b>Знакомство с сетевым шпионажем</b>	<b>339</b>
Типы сетевых атак	340
Отправные точки сетевой атаки	341
Кража информации в ходе сетевой атаки	343
Риски, связанные с широкополосными соединениями	344
<b>Шпионская тактика</b>	<b>347</b>
Использование уязвимых мест	347
Средства сбора сетевой информации и шпионажа	361
<b>Контрмеры</b>	<b>367</b>
Установка пакетов обновлений для операционной системы и отдельных приложений	367
Использование систем обнаружения вторжений	368
Использование брандмауэров	370
Виртуальные частные сети	373
Мониторинг сетевых подключений	375
Применение программ перехвата сетевых пакетов	376
Применение сканеров портов и уязвимых мест	377
Шифрование сообщений электронной почты	377
Шифрование мгновенных сообщений	378
Использование безопасных протоколов	379
Не доверяйте неизвестным вам компьютерам и сетям	379
Повышение безопасности системы при разделяемом доступе к файлам	380
Использование безопасных веб-служб электронной почты	381
Использование программ анонимной пересылки корреспонденции	382
Использование прокси-серверов	383
<b>Заключение</b>	<b>385</b>
<hr/>	
<b>Глава 11. Беспроводные сети 802.11b</b>	<b>387</b>
<hr/>	
<b>Знакомство с беспроводными технологиями</b>	<b>387</b>
История беспроводных технологий	388
<b>Шпионская тактика</b>	<b>389</b>
Использование уязвимых мест	390
Средства шпионажа для беспроводных сетей	397
<b>Контрмеры</b>	<b>422</b>

Мониторинг вашей собственной сети	422
Правильное размещение антенны	423
Обнаружение средств поиска беспроводных ЛВС	424
Средства одурачивания шпионов	425
Включение WEP-шифрования	426
Регулярная смена WEP-ключей	426
Аутентификация MAC-адресов	426
Изменение SSID	427
Отключение функции передачи SSID	427
Изменение пароля по умолчанию базовой станции	427
Применяйте статические IP-адреса	428
Размещайте базовые станции за пределами брандмауэра	428
Применение виртуальных частных сетей	428
Не рассчитывайте на расстояние как меру безопасности	428
Отключайте базовую станцию	429
<b>Заключение</b>	<b>429</b>
<b>Глава 12. Офисное оборудование</b>	<b>431</b>
<b>Офисное оборудование</b>	<b>431</b>
Факсы	431
Машины для уничтожения бумаги	434
<b>Средства связи</b>	<b>438</b>
Телефоны	438
Сотовые телефоны	443
Автоответчики и голосовая почта	449
Пейджеры	451
<b>Персональные электронные устройства</b>	<b>454</b>
КПК	455
Цифровые камеры	457
Устройства GPS	458
Игровые приставки	458
MP3-плееры	458
Цифровые видеомагнитофоны	460
<b>Заключение</b>	<b>460</b>
<b>Глава 13. Высший компьютерный шпионаж</b>	<b>463</b>
<b>ТЕМPEST – перехват электромагнитного излучения</b>	<b>463</b>
Мониторинг побочного излучения: реальность или фантастика?	465
Контрмеры по защите от мониторинга излучения	470
<b>Оптические стандарты ТЕМPEST – светодиоды и отраженный свет</b>	<b>472</b>

<b>HIJACK и NONSTOP</b>	<b>473</b>
<b>ECHELON – глобальная система наблюдения</b>	<b>473</b>
Принципы работы проекта ECHELON	475
ECHELON: дискуссии и контрмеры	477
<b>Carnivore/DCS-1000</b>	<b>481</b>
Обзор системы Carnivore	482
Carnivore: дискуссии и контрмеры	483
<b>Magic Lantern</b>	<b>485</b>
<b>Модификация приложений и компонентов операционной системы</b>	<b>488</b>
<b>Разведывательные вирусы и «черви»</b>	<b>492</b>
Вирусы и черви	493
Контрмеры	498
<b>Камеры наблюдения</b>	<b>499</b>
Веб-камеры	500
Промышленные камеры наблюдения	502
<b>Заключение</b>	<b>503</b>
<b><u>Приложение. Наша веб-страница</u></b>	<b>505</b>
<b>Системные требования</b>	<b>505</b>
<b>Ссылки на нашем веб-сайте</b>	<b>506</b>
<b>Разрешение вопросов</b>	<b>506</b>
<b>Предметный указатель</b>	<b>509</b>

# Об авторе

Джоэль Макнамара обладает более чем 20-летним опытом работы в компьютерной индустрии. С 1995 года он выступает в роли консультанта по компьютерной безопасности и вопросам защиты информации. Он поддерживает «Полную неофициальную информационную страницу по стандартам TEMPEST» (веб-сайт, посвященный теме секретных правительственныех наблюдательных технологий), является автором популярной бесплатной утилиты, распространяемой по принципу открытого кода, под названием *Private Idaho* (удобная интерфейсная программа для утилит PGP и программ анонимной пересылки корреспонденции). Он был упомянут в списке благодарностей разработчика первого макровируса, атакующего продукты компании Microsoft, который продемонстрировал незащищенность тогдашних систем. В свое свободное время Джоэль соревнуется в марафонском беге и других видах спорта, направленных на выработку выносливости, а также является добровольным помощником вспомогательной команды медиков по ликвидации последствий стихийных бедствий.

## Благодарности

Всем сотрудникам издательского дома Wiley, в особенности моему редактору Кати Фелтман и редактору проекта Марку Иноксу, спасибо за время и терпение, потраченное вами на поддержку начинающего автора в деле написания его первой книги. Также благодарю Нэнси Сиксмис, моего редактора по копированию, и Расса Шамвея, технического редактора, за его зоркий глаз и взгляд «в глубину вещей».

Я в большом долгу у моего друга Джефа Мэддена, который долгое время подталкивал меня к идее написания книги. Спасибо за твою поддержку и добровольное участие в роли неофициального литературного агента и советчика в издательской индустрии.

Спасибо моей жене Дарси за поддержку в течение многих лет, в особенности в последние полгода, когда я работал над этим проектом.

И, наконец, я бы вряд ли написал когда-нибудь эту книгу без моего отца Доуга, который привил мне интерес к теме шпионажа еще в раннем детстве, в возрасте шести лет, сводив на первый фильм о Джеймсе Бонде.

# Введение

«Информация – это кислород современной эпохи. Она проходит сквозь заборы, обвитые колючей проволокой, и ей ни почем границы, обозначенные высоковольтными проводами».

Рональд Рейган

## О чем эта книга

Рональд Рейган, которого называли «великим мастером общения», забыл упомянуть только о том, что иногда, чтобы найти информацию, приходится хорошо поискать.

Возможно, вам нечего скрывать, однако пронырливые сотрудники, любопытные члены вашей семьи, враждебно настроенные взломщики, шпионы, направленные крупными корпорациями, офицеры полиции, системные администраторы, частные сыщики, а также ревнивые друзья (подруги) так и норовят выяснить, чем вы занимаетесь за компьютером. И если вам есть что скрывать, то что случится, когда они это обнаружат?

Вам не нужно проходить подготовку агента ЦРУ либо располагать бюджетом Национального управления безопасности для проведения простого экономического шпионажа. Короткий поиск в Интернете выведет вас на сотни доступных программ с полными инструкциями по их применению, с помощью которых среднестатистический гражданин может превратиться в настоящего Джеймса Бонда в плане электронного шпионажа, и эти программные средства активно используются для законного и незаконного наблюдения за компьютерными пользователями.

Сложно сказать, сколько шпионских операций происходит ежедневно (если даже кто-то назовет вам конкретную цифру, примите ее с разумной долей скептицизма, поскольку, скорее, она является всего лишь догадкой). Средства массовой информации отлично справляются с освещением громких шпионских операций, но известно о них нам становится только тогда, когда шпион оказывается пойманым. Оценить же общее количество менее значительных операций гораздо труднее, поскольку в большинстве ситуаций коммерческие компании и правительственные агентства стараются скрыть факты шпионажа, чтобы недопустить негативной реакции со стороны общественности. (Держатели акций не слишком обрадуются, если узнают, что кому-то удалось взломать систему защиты компаний и получить доступ к информации об исследованиях и разработках в области будущих продуктов.)

Хотя мы не знаем, сколько случаев компьютерного шпионажа имеет место каждый день, об общем уровне распространения компьютерного шпионажа мы можем судить, исходя из следующих соображений:

- Использование компьютеров для хранения конфиденциальных и секретных данных значительно увеличилось (в личной, деловой и правительственной сферах). А скопировать информацию, представленную в цифровом виде, намного проще и быстрее, чем данные с традиционных (например, бумажных) носителей.
- Существует огромное количество уязвимых мест в защите операционных систем и приложений и не меньшее число программных приложений, специально разработанных для использования этих уязвимостей.
- За последние несколько лет значительно возросло число компьютеров, подключенных к Интернету, что увеличивает потенциальный риск удаленных сетевых атак.
- Большинство случаев шпионажа, о которых стало известно широкой общественности, показали, что наибольшая угроза, как правило, исходит «изнутри». Хотя информация об атаках «извне» становится известной гораздо чаще и вызывает все большее беспокойство у общественности, вероятность успешных атак подобного рода гораздо ниже, чем угроза получения несанкционированного доступа к информации в домашних или корпоративных условиях.

Когда вы начинаете думать о подобных вещах, то понимаете реальность угрозы со стороны современной интерпретации второй древнейшей профессии. Риск увеличивается и в связи с наличием огромного количества общедоступной информации по теме шпионажа и взлома, а также полностью готовых к использованию утилит в сети Интернет, с помощью которых практически любой может попробоваться в роли компьютерного шпиона-любителя. (Действительно, риск со стороны amateurs выше, поскольку их больше, а при помощи современных хакерских утилит любитель может нанести недостаточно защищенному компьютеру не меньший ущерб, чем профессиональный шпион.)

В этой книге обсуждаются средства и методы, которые применяются любителями и профессионалами в сфере шпионажа, а также контрмеры, предназначенные для борьбы с ними. Обычные взломщики также используют некоторые из описываемых здесь методик (в особенности это касается сетей), однако ряд шпионских операций все-таки связаны с получением физического доступа к компьютеру. (Многие книги, посвященные компьютерной безопасности, часто умалчивают о подобных методах, говоря, что если шпион получит физический доступ к вашему компьютеру, то вам «крышка». По-моему, такое обобщение несколько чрезмерно. Важно иметь представление о том, что и как можно «выкачать» из компьютера, если кто-либо получит к нему физический доступ. Зная это, вы можете попытаться лучше защитить ваш компьютер в подобной ситуации.)

Большую часть времени мы будем говорить об операционной системе Microsoft Windows (поскольку на данный момент она занимает лидирующее положение на рынке операционных систем). Тем не менее в книге приводятся общие концепции и технологии, пригодные для использования на любых компьютерных системах, поэтому даже если вы используете ОС Linux, OpenBSD или Mac OS, то найдете эту книгу полезной и для себя.

## Для кого написана эта книга

Целевой аудиторией данной книги мы считаем всех, кого интересует возможность либо опасность шпионажа с чьей-либо стороны. К данной аудитории могут относиться все: от пользователей персональных компьютеров до системных администраторов, ответственных за обеспечение корпоративной безопасности.

Если в ваши обязанности входит сбор улик с компьютеров (имеется в виду законное наблюдение), когда вы являетесь представителем правоохранительных органов, системным администратором либо судебным экспертом, эта книга станет для вас небесполезным пополнением библиотеки.

Вам не понадобится допуск для работы с секретной информацией либо опыт работы в области криптографии, чтобы освоить данную книгу. Читатели как с техническим образованием, так и без оного найдут здесь полезную для себя информацию, которая должна помочь им разобраться с рисками шпионажа и с тем, как защитить свои компьютеры от различного рода посягательств.

## Структура книги

Большинство глав книги поделены на две части: «Шпионская тактика» и «Контрмеры». В разделе «Шпионская тактика» описываются уязвимые места в системах защиты, а также способы, средства и методы получения доступа к защищенной информации. Например, из раздела «Шпионская тактика» главы 4 «Проникновение в систему» вы узнаете о том, как шпионы обходят защиту компьютера при помощи пароля в BIOS либо в окне аутентификации входа в систему.

В ряде ситуаций вас попросят представить себя на месте шпиона, заинтересованного в тайном сборе некоторой информации. Это не означает, что данная книга является инструкцией по проведению электронного шпионажа, мы просто хотим заставить вас понять, как мыслит шпион, желающий получить несанкционированный доступ к данным. Уловив ход мыслей шпиона, собирающегося похитить у вас конфиденциальную информацию, вы сможете лучше подготовиться к ее защите путем ужесточения мер безопасности.

Вслед за разделом «Шпионская тактика» идет раздел «Контрмеры», в котором рассказывается о том, как предотвратить проникновение шпиона, и описываются необходимые для этого практические средства и методы. Вы узнаете об использовании надежных паролей, настроек безопасности Windows и других методах защиты информации от шпионского нападения.

В книге присутствует множество врезок (вроде той, что размещена ниже этой страницы), в которых приводятся реальные истории о шпионах, используемой ими тактике, уязвимых местах и контрмерах, реализация которых поможет вам защитить вашу систему. Врезки вставлены в текст для вашего информирования в образовательных целях и просто для развлечения. Кроме того, в книге приводится огромное количество ссылок на веб-ресурсы, где вы сможете найти более подробную информацию по тем или иным вопросам.

## Контрмеры: OODA-цикл

Джон Байд работал военным пилотом ВВС США еще во времена корейской войны. Байда заинтересовал вопрос, почему американцы превалировали над азиатами практически во всех воздушных поединках. Ведь по сравнению с истребителями F-86, на которых летали американские пилоты, МиГ-15 российского производства являлся на тот момент гораздо более быстрым и маневренным самолетом. Хотя очевидно, что навыки и опыт американских пилотов были выше, однако статистика успешных поединков (10:1) обуславливала другим немаловажным фактором.

Несмотря на то, что по техническим параметрам МиГ-15 мог легко увернуться и обойти F-86, американский самолет имел кабину с большим обзором, за счет чего пилот имел возможность лучше видеть поле боя. Вдобавок расположение рычагов на F-86 облегчало управление самолетом. С учетом этих двух факторов, Байд выдвинул теорию, что хороший пилот на F-86 имел возможность более оперативно анализировать ситуацию и принимать решения, чем пилот того же класса на МиГ-15.

Эти наблюдения помогли разработать Байду концепцию OODA (Observe, Orient, Decide, Act – наблюдение, ориентирование, принятие решения и действие), названную «циклом Байда». В соответствии с этой концепцией, любой человек, находящийся на пороге принятия решения, сам того не осознавая, проходит все стадии этого цикла. Он анализирует ситуацию, ориентируется в ней, принимает решение, основываясь на предыдущем опыте, и, наконец, действует.

Байд допустил, что вы выиграете в конфликтной ситуации, если сможете ускорить ваш собственный цикл принятия решений и замедлить принятие решений вашим противником. Любопытно, что, в случае прерывания этого цикла на любом этапе, он начинается заново. То есть, если вы помешаете противнику в момент, когда он принял решение, но еще не начал действовать, ему придется опять начать с анализа текущей ситуации.

(Байд принял участие в разработке истребителя F-16, а его идеи в тактике и стратегии стали частью военной маневренной доктрины, принятой ВВС и ВМС США, а также нашли применение в теории бизнеса. Его считают одним из самых выдающихся военных стратегов XX века. Более подробно узнать о Байде вы можете, посетив веб-сайт [www.belisarius.com](http://www.belisarius.com).)

Данная книга предназначена для того, чтобы помочь вам ускорить ваш собственный цикл принятия решений в вопросах, касающихся компьютерного шпионажа. Как минимум, мы поможем вам лучше ориентироваться в возможных угрозах, и если вы вдруг окажетесь жертвой компьютерного шпионажа, подумайте, как помешать шпиону принимать решения и таким образом получить преимущества.

В книге вы можете встретить абзацы, отмеченные различными значками, предназначенными для выделения важной информации. Приведем список обозначений и их толкование:



Замечание! Под этим значком помещена дополнительная либо важная информация, а также технические сведения по данной теме.



Внимание! Здесь приводятся предупреждения и подсказки, помогающие избежать некоторых подводных камней.



Ссылки! В этих абзацах приводятся ссылки на веб-ресурсы, содержащие дополнительную информацию по конкретной теме.

## Подводные камни

Перед тем, как приступить к чтению книги, обратите внимание на следующие моменты:

- **Ссылки.** Гиперссылки на веб-ресурсы являлись актуальными на момент сдачи книги в печать. Если вы не новичок в среде Интернет, то вам должно быть известно, что ссылки имеют свойство устаревать. Если гиперссылка не работает, то в предшествующем ей тексте вы наверняка сможете найти достаточно информации, чтобы сформулировать запрос в вашем любимом поисковом сервере. Кроме того, существует официальный веб-сайт нашей книги, на котором вы можете найти обновленные ссылки либо избавить себя от труда набирать ссылки вручную. Наша веб-страничка размещена по адресу [www.wiley.com/comrbooks/mcnamara](http://www.wiley.com/comrbooks/mcnamara).
- **Цены.** В книге обсуждаются многие программные и аппаратные средства, и я постарался указать стоимость для большинства из них (как вы, наверное, заметите, вообще-то я сторонник экономии и поэтому отдаю предпочтение бесплатным либо недорогим, но эффективным средствам). В подавляющем большинстве книг вы редко увидите цены, что лично меня раздражает, поскольку нет ничего более неприятного, как прочесть о великолепном продукте и потом выяснить, что цена не позволит приобрести его бюджетным организациям либо частному лицу. Конечно, я понимаю, что цены меняются слишком быстро, а ведь только между моментом завершения написания книги и ее выходом из печати проходит несколько месяцев. Однако эти цены должны помочь вам, по крайней мере, составить общее представление о том, сколько это может стоить. Большинство приводимых розничных цен являлись актуальными на начало 2003 года.
- **Интернет-источники.** Ряд упоминаемых в книге программных утилит размещены на сайтах, которые люди честные терпят как неприятных соседей. Поэтому, загружая утилиты с хакерских веб-страниц и даже с более уважаемых сайтов, посвященных вопросам компьютерной безопасности, всегда придерживайтесь простейших мер безопасности. Убедитесь в том, что вы используете самое современное антивирусное ПО и программы для обнаружения троянских коней, и протестируйте загруженную утилиту на компьютере, который не содержит критичной информации (желательно с запущенным персональным брандмауэром), чтобы удостовериться в отсутствии враждебного программного кода.
- **Юридические нюансы.** На страницах книги, и особенно в главе 2, которая так и называется «Шпионаж и закон», рассматривается ряд тем, связанных с юриспруденцией. Тем не менее, поскольку я не являюсь адвокатом и не выступаю в роли юрисконсульта на телевидении, все вопросы касательно законодательства и предусматриваемых наказаний вам следует задавать квалифицированному специалисту в данной области.

# Глава 1

## Шпионы

«Наверное, я мог бы стать выдающимся шпионом, просто я не хотел им становиться – мне нужно было заработать немного денег и бросить это занятие».

Роберт Хансен, агент ФБР, осужденный за шпионаж в пользу Советского Союза

## Как узнать шпиона

Компьютерные шпионы, как правило, не носят длинных плащей. Они не надевают черную облегающую одежду и не висят на телеграфных столбах, прослушивая ваши переговоры. Вряд ли кого-то из таких шпионов зовут Борис, и едва ли вы услышите их сильный славянский акцент. Большинство из них даже не являются взломщиками либо хакерами и могут перепутать название набора утилит хакера и отвара из корнеплодов\*. Но если компьютерные шпионы мало соответствуют классическому образу шпиона, нарисованному в сознании общества средствами массовой информации, как же их тогда узнать?

Как людей любой профессии, компьютерных шпионов можно поделить на две категории: любителей и профессионалов своего дела.

Любителями называют рядовых шпионов. Несмотря на то, что у них могут существовать достаточно веские основания для занятий шпионажем, это редко превращается в их основной заработок. Такие шпионы просто имеют немного больше опыта в работе с компьютером, чем обычные пользователи. В то же время это не означает, что они являются компьютерными «гуру», – они просто нашли время на изучение новых технологий, которые могут использоваться для наблюдения за компьютерами, то есть в целях компьютерного шпионажа. Для изучения или приобретения современной шпионской экипировки достаточно иметь немного денег и доступ к Интернету. Подобные шпионы не похожи на киношных Тома Круза или Сандру Балок – в роли наблюдающего за вами человека может выступать ваш начальник, коллега по работе, супруг(а), дети или соседи.

---

\* Игра слов в английском: rootkit – так называется набор утилит, устанавливаемых взломщиком на компьютере-жертве; a root beer – шипучий напиток из корнеплодов, приправляемый мускатным маслом и т. п. – *Прим. перев.*

Профессиональные шпионы обладают более широкими техническими познаниями в отличие от любителей. Профессионалы зарабатывают шпионажем себе на жизнь. Шпионаж может быть законным и незаконным. Законные случаи шпионажа касаются наблюдения за людьми и компьютерными системами с целью расследования случаев распространения детской порнографии, к примеру. В то же время выведение коммерческих секретов путем проникновения во внутренние сети корпораций отнюдь нельзя отнести к законной деятельности. Хотя и профессионалы, и аматоры часто прибегают к одним и тем же средствам, профессиональные шпионы характеризуются более глубоким владением материала и имеют доступ к более совершенной прослушивающей технике. Как и в случае с любителями, профессиональных шпионов нельзя узнать по внешнему виду. Вспомним хотя бы Элдрика Эймса и Роберта Хансена: белые, среднего телосложения обычные сотрудники ЦРУ и ФБР, которые годами работали на русских, ничем не выделяясь среди массы других агентов. Опять-таки, профессиональные компьютерные шпионы не похожи на те романтизированные образы, которые создает современный кинематограф, хотя, возможно, некоторые из них действительно имеют прекрасную помощницу по имени Наташа.

Такое деление шпионов на категории необходимо по двум причинам:

- **Чтобы лучше представлять технические возможности и ограничения потенциального противника.** Полагаем, это очевидно, поскольку вы должны быть уверенными в надежности принятых вами мер безопасности.
- **Чтобы иметь возможность поставить себя на место шпиона.** В этой книге мы будем рассматривать тактику шпионажа, уделяя особое внимание компьютерному наблюдению. В последующих параграфах вам не раз придется примерять на себя шпионское одеяние, чтобы лучше понять, как защитить собственный компьютер, – ведь, чтобы по-настоящему обезопасить себя, необходимы не только соответствующие инструментальные средства и технологии, но и понимание склада ума потенциального шпиона. Мы часто говорим: «А что бы на нашем месте сделал \_\_\_\_\_ (подставьте имя вашего любимого персонажа)?» Когда вы заботитесь о защите информации, вам необходимо задуматься над вопросом: «А что бы сделал в этом случае человек, занимающийся экономическим шпионажем?»

Известный китайский стратег Сунь-Цзы говорил: «Знающий и себя и неприятеля может быть уверен в исходе сражения. Знающий себя, но не знающий неприятеля с каждой победой потерпит поражение. И, наконец, не знающий ни себя, ни противника никогда не победит».

В этой главе мы научим вас, как изучить себя и как узнать своих врагов применительно к сфере компьютерного шпионажа.

# За кем наблюдают шпионы, и кто они такие

Начнем с изучения врага. Компьютерный шпионаж представляет собой целенаправленную охоту за информацией или доказательствами чего-либо. *Толковый словарь американского английского (American Heritage Dictionary of the English Language, Fourth Edition)* поясняет значение термина «информация» как «осведомленность об определенных событиях или ситуациях, приобретенная в результате общения, получения новостей либо логических умозаключений». Свидетельства или доказательства, с другой стороны, представляют собой «сведения, призванные помочь в формировании логических суждений». Клерк, занимающийся промышленным шпионажем, может наблюдать за переносным компьютером руководителя проекта по выпуску новой операционной системы Longhorn компанией Microsoft. Жена, подозревающая мужа в любовной афере, может разыскивать доказательства своей правоты в электронной почте мужа. В зависимости от назначения, информация может выступать в качестве свидетельства в том или ином деле. К примеру, хранящийся в КПК адрес может принадлежать наркодилеру и служить доказательством причастности владельца КПК к распространению наркотиков.

Помните о том, что шпионажем считается целенаправленный сбор информации. Несмотря на то, что жена, подозревающая мужа в супружеской измене, занимается целенаправленным поиском информации и доказательств, случайное обнаружение ею в незакрытом окне почтовой программы сообщения двусмысленного содержания нельзя квалифицировать как шпионаж.

Собираемые наблюдателем данные и улики могут носить общий характер либо иметь определенную направленность, в зависимости от того, какие цели он преследует. Экономического шпиона, скорее всего, будут интересовать исключительно финансовые таблицы. С другой стороны, содержимое жесткого диска, найденного у террориста, должно быть изучено более детально не только для нахождения доказательств совершенных преступлений, но и для поиска любой информации, которая может быть связана с планированием будущих террористических актов.

Помимо сбора информации или доказательств, компьютерный шпионаж также подразумевает скрытость и несанкционированность проникновения. В подавляющем большинстве случаев вы ведь не станете предоставлять кому бы то ни было явные или неявные разрешения для наблюдения за вашим компьютером. В качестве исключений можно привести обычный мониторинг активности пользователей в организации либо тот случай, когда вы говорите дружественно настроенному полицейскому, что вам нечего скрывать, вам не нужен адвокат, и, разумеется, офицер может взглянуть на ваш компьютер. В некоторых случаях вам даже ничего не понадобится говорить офицеру полиции – если на вас

пало подозрение в участии в незаконной деятельности, по решению суда за вашим компьютером может быть установлено наблюдение. Следует различать понятия несанкционированный и незаконный доступ. Несанкционированный (вами) доступ необязательно является незаконным. Если проникновение в закрытую компьютерную сеть с целью кражи коммерческих тайн нарушает целый перечень законов, то размещение программы типа keylogger\* на компьютере вашего сына без его разрешения, для того чтобы проследить, нет ли среди его друзей торговцев наркотиками, не является незаконным, однако может быть расценено как неэтичный поступок по отношению к его друзьям.

Второй неотъемлемой чертой компьютерного шпионажа является тот факт, что если вы служите объектом шпионского интереса, то, как правило, узнаете об этом только после окончания слежки. (В отличие от товарных производителей, шпионы не оставляют на компьютере наклеек вроде «за вами наблюдает соглядатай №39»). Естественно, в некоторых случаях следы шпионской деятельности все-таки остаются, хотя и не столь явно выраженные. Кто бы ни наблюдал за вами, он, как правило, не желает, чтобы вы знали о его присутствии. Исключение в данном случае представляет открытая программа мониторинга деятельности служащих компаний либо же правительственные системы наблюдения за данными ECHELON (которая обсуждается далее в этой главе), о существовании которой также известно – к неудовольствию пользующихся ею правительственные службы.



ECHELON представляет собой наглядный пример «культы секретности». Хотя о существовании данной системы давно стало известно широкой публике, правительство настойчиво отказывается признать этот факт. Более подробно о системе ECHELON и других системах мониторинга рассказывается в главе 13 данной книги.

До сих пор мы постоянно говорили о том, какая информация может интересовать шпионов, но так и не ответили на вопрос Сунь-Цзы о том, кто может выступать в их роли. Это чрезвычайно важно, поскольку позволяет нам изнутри взглянуть на их методы и мотивы деятельности. Попытка поставить себя на место «плохих парней» – полезное упражнение, которое поможет вам обеспечить собственную защиту. Грубо говоря, всех шпионов можно разбить на семь различных категорий:

- экономические шпионы,
- начальники,
- полицейские,
- частные сыщики и консультанты,
- шпионы-«призраки»,

---

\* Программа, сохраняющая в файле последовательность нажатия клавиш. – Прим. ред.

- преступники,
- доносчики,
- друзья и семья.

Давайте вкратце рассмотрим каждую из вышеперечисленных категорий, дабы лучше разобраться, кто и зачем может шпионить за вами.

## Экономический шпионаж

Экономический шпионаж является большой проблемой, о которой тем не менее нередко забывают. Торговые организации и средства массовой информации постоянно предупреждают коммерческие предприятия об опасности экономического шпионажа (ранее называвшегося промышленным) еще с конца 80-х годов XX века. Однако большинство организаций и предприятий по-прежнему остаются глухи к подобным предупреждениям.

Приведем результаты исследования, проведенного в 2002 году Американским обществом промышленной безопасности торговой палаты (American Society for Industrial Security), в котором была собрана информация о 1000 крупных корпорациях и 600 мелких и средних компаниях:

- Около 40% компаний, принявших участие в опросе, сообщили об известных им эпизодических фактах кражи конфиденциальной информации (воспользовавшись шпионской терминологией, можно сказать, что кто-то внутри или извне компании занимался шпионажем и похищал коммерческие тайны).
- Прибыль, недополученная в результате кражи коммерческих секретов и интеллектуальной собственности, составила от 53 до 59 миллиардов долларов.
- Основной целью экономического шпионажа, как правило, являлись документы по разработкам и исследованиям, списки клиентуры и связанной с ней информации, а также финансовые данные.
- Несмотря на потенциальную угрозу денежных потерь из-за успешных атак, только 55% компаний, откликнувшихся на данное исследование, сообщили, что они действительно учитывают эту опасность и принимают соответствующие меры предосторожности. На основании этого можно прийти к выводу, что значительное число руководителей недооценивают либо не понимают возможные риски и стоимость потери данных.

А ведь компании, пострадавшие в результате шпионских атак, несут не только финансовые потери. Они вынуждены мириться с утратой преимуществ перед конкурентами,тратой денег на ведение судебных тяжб и потерей доверия как со стороны акционеров, так и со стороны общества в целом, когда данные факты становятся известны широкой общественности (именно поэтому многие компании и боятся огласки).

Экономический шпионаж, увы, не ограничивается крупными корпорациями. Небольшие компании, начиная от семейных фирм и заканчивая малыми предприятиями, не располагающие значительными денежными резервами, могут страдать от последствий экономического шпионажа в гораздо большей степени.

Чаще всего в роли злоумышленников выступают ваши собственные подрядчики и поставщики, бывшие сотрудники и конкуренты. (Следует заметить, что термины «экономический шпионаж» и «разведка конкурентного рынка» имеют между собой принципиальные отличия. Изучение конкурентов включает в себя законные методы с использованием общедоступных источников информации. Экономический шпионаж подразумевает применение нелегальных методов сбора данных. Разумеется, некоторые методы получения информации невозможno четко отнести к той или иной группе, поскольку их использование скорее связано с этическими нормами, которые тем не менее соблюдаются большинством профессионалов экономической разведки.)



Если вы хотите более подробно изучить различия между легитимной конкурентной разведкой и незаконным шпионажем, посетите веб-страницу Общества профессионалов конкурентной разведки (the Society of Competitive Intelligence Professionals) по адресу [www.scip.org](http://www.scip.org).

Хотя в кино и на телевидении сложился портрет корыстного наемника, умело проникающего во все секреты, на самом деле за факты экономического шпионажа обычно несут ответственность хорошо осведомленные люди, имеющие доступ к несекретной информации. То есть можно говорить о том, что для компаний большую угрозу представляют бывшие сотрудники, действующие из корыстных побуждений либо из мести, чем профессиональные шпионы, нанятые конкурирующими фирмами.

Проблема касается не только мелких клерков компаний. Хосе Игнасио Лопес (Jose Ignacio Lopez), глава отдела снабжений корпорации General Motors, в 1993 году неожиданно подал в отставку, а через некоторое время получил работу в корпорации Volkswagen. Позднее компания General Motors обвинила Лопеса в краже более 20 пакетов документации, содержащих сведения о разработках компании, продажах и финансовой информации. Украденные документы включали планы строительства нового завода для сборки автомобилей, постройка которого должна была помочь отобрать доминирующие позиции на рынке небольших автомобилей у компании Volkswagen. Рассмотрение дела завершилось в 1997 году, когда корпорация Volkswagen отказалась признать неправомерность действий со своей стороны, но при этом уладила тяжбу, заплатив General Motors компенсацию в размере 100 миллионов долларов и предложив приобрести часть компании в течение семи лет за 1 миллиард долларов. Немецкие правозащитники в конце концов сняли с Лопеса обвинение в промышленном шпионаже, однако принудили его пожертвовать четверть миллиона долларов на благотворительность.

## Шпионаж: корпорация Niku против Business Engine

В августе 2002 года полсотни агентов ФБР совершили облаву на офис корпорации Business Engine, компании по производству программного обеспечения из Силиконовой Долины, которая специализировалась на выпуске средств совместной работы в сети Интернет. Рейд был предпринят с подачи конкурирующей компании Niku, обнаружившей, что некто с IP-адреса корпорации Business Engine проник в закрытую сеть корпорации Niku более 6000 раз, пользуясь действующими паролями сотрудников. За время несанкционированных проникновений было украдено более тысячи различных документов, включая информацию о будущих разработках, списки потенциальных клиентов, ориентировочные цены и планы продаж. В результате последующего расследования было выявлено, что, начиная с октября 2001 года, злоумышленники подключались к закрытой внутренней сети корпорации Niku, используя около 15 различных бюджетов и паролей для доступа к документам, представляющим собой коммерческую тайну.

В конце сентября 2002 года ранее процветавшая корпорация Niku очутилась на грани исключения из списка участников торгов на американской фондовой бирже по продаже акций высокотехнологичных компаний (NASDAQ) по причине резко упавшей стоимости своих акций. Нетрудно догадаться, что не последнюю роль в этом деле сыграл факт экономического шпионажа, направленный против компании Niku.

Niku возбудила дело против корпорации Business Engine, за исходом которого, пожалуй, будет весьма интересно наблюдать\*.

Незаконные проникновения в закрытые компьютерные системы сегодня не редкость, и в большинстве случаев они действительно совершаются сотрудниками (бывшими) либо наемниками конкурирующих компаний. Все подобные вторжения можно поделить на две группы:

- **Случайные атаки**, реализуемые при наступлении благоприятного момента. Конкуренты проверяют, насколько доступной является та или иная информация, подобно тому, как мы дергаем за дверную ручку, проверяя, закрыта ли дверь. Если риск раскрытия минимален либо не может понести за собой значительной ответственности, конкуренты могут попытаться выкрасть нужную им

\* В декабре 2002 года еженедельник "Business Journal" сообщил о мирном урегулировании иска: корпорация Business Engine согласилась выплатить корпорации Niku компенсацию в 5 миллионов долларов и пообещала не использовать ее технические секреты в своих разработках. – Прим. ред.

информацию. Примерами таких действий можно назвать прослушивание порта либо использование инструментальных средств для выявления слабых мест в системе защиты корпоративной сети. В случае обнаружения бреши в защите, по отношению к этой сети может быть осуществлена целенаправленная атака.

- **Целенаправленная атака.** Целенаправленные атаки реализуются с намерением выкрасть определенную информацию. Шпионы в данном случае имеют перед собой конкретные цели и прибегают к различным методикам, чтобы добиться желаемого результата. Когда ставка достаточно высока, на операции по наблюдению за конкурирующими фирмами тратятся огромные денежные и другие ресурсы.

Поскольку компьютеры используются для хранения различных видов корпоративной информации, они представляют собой первичную цель для любого экономического шпиона. Сети, мобильные и настольные компьютеры, КПК – все они в той или иной степени уязвимы для хакеров. Причем в разных ситуациях от взломщика требуются разные уровни технических знаний – начиная от умения копирования конфиденциальной информации на дискету и кончая способностью построения сложных технических решений, позволяющих легко обходить защиту брандмауэров для обращения к корпоративной базе данных.



В Соединенных Штатах за экономический шпионаж предусмотрены суровые меры наказания. Более подробно об этом читайте в главе 2.

## Начальство и наблюдение за сотрудниками

Наблюдение за персоналом в США растет быстрыми темпами. Согласно наблюдению, проведенному Американской ассоциацией управления (American Management Association – AMA) в 2001 году, 77,7% наиболее крупных компаний в США используют различные системы наблюдения за деятельностью своих сотрудников на рабочем месте. Эта цифра в два раза больше показателя, обнародованного в 1997 году.

Если вы работаете на кого-то еще, существует немалая доля вероятности, что ваш начальник следит за вами. Это означает, что ваша электронная почта, навигация по Интернету, использование служб мгновенных сообщений, весь ваш жесткий диск и т. п. подвергаются тщательному досмотру. Права сотрудника на неприкосновенность частной жизни в данном случае нередко нарушаются. Работодатели заинтересованы в поиске свидетельств неполной трудовой отдачи с вашей стороны либо каких-то нарушений политики компании.

Как же при этом компании избегают ответственности?

При работе в государственной компании вы обладаете конституционными правами на защиту вашей частной жизни. Когда же речь заходит о

частных предприятиях, действие этих прав (на рабочем месте) на вас не распространяется. Поскольку вам платят за работу, выполняемую на офисной технике, принадлежащей нанимающей стороне, и за рабочее время, вы не вправе ожидать какой-либо конфиденциальности при работе с частной информацией на компьютерах корпорации.

Каждый раз, когда у вашего работодателя возникает непреодолимый интерес к тому, чем вы занимаетесь на работе, дабы убедиться в законности выполняемых вами действий, в полной отдаче с вашей стороны либо из соображений безопасности, – владелец компании имеет право осуществлять мониторинг вашего компьютера, телефона и даже наблюдать за вами во время перерывов, то есть следить за всем, что происходит в его компании.

Наблюдение может выполняться с главного сервера, на котором администраторы просматривают протоколы работы либо изучают содержимое электронных сообщений, либо при помощи настольного компьютера с установленным программным обеспечением для мониторинга клавиатуры.



Программы, предназначенные для перехвата и сохранения в файл всего, что вводится с клавиатуры (называемые keylogger), подробно рассматриваются в главе 8 данной книги.

Как правило, за установку и наблюдение при помощи подобных программ мониторинга ответственным является специальный технический персонал корпорации либо приглашенный консультант; в любом случае такой человек должен обладать глубокими техническими познаниями.

Поэтому учтите, что при попытке защититься от наблюдения на рабочем месте со стороны корпорации-работодателя вы, в конце концов, только привлечете к себе дополнительное внимание и, возможно даже, дождитесь появления замученного системного администратора, пришедшего поинтересоваться, чем же вы тут, собственно, занимаетесь?

Несмотря на то, что практика наблюдения за сотрудниками становится общепринятой, наиболее ответственные корпорации должны четко оговаривать правила игры. Применение программ мониторинга должно быть отражено в уставе компании, договоре о найме и выводимых на экран сообщениях. Нередко тот факт, что сотрудник знает о ведущемся за ним наблюдении, является лучшим сдерживающим фактором от выполнения противозаконных действий, чем скрытая слежка.

Возможно, в ближайшие годы и будут приняты государственные законы, защищающие ваше право на частную жизнь на рабочем месте, но на сегодняшний день вы должны иметь представление о том, что за каждой вашей операцией на компьютере корпорации может следить ваш работодатель. Хотя вы и в состоянии предпринять кое-какие контрмеры против шпионящих боссов, лучшее решение в данном случае – это отделить вашу частную жизнь от задач, выполняемых на рабочем месте.

## Шпионаж: оправданное наблюдение

Ведение наблюдения со стороны работодателей за своими служащими, осуществляемое при помощи видеокамер, записи телефонных звонков либо компьютерного мониторинга, набирает все больший размах в корпоративной Америке.

Основной движущий фактор в данном случае – само законодательство, поскольку в соответствии с множеством местных и федеральных законов работодатели являются ответственными за действия своих сотрудников в рабочее время. Компании используют это в качестве оправдания за применение программ наблюдения за своими сотрудниками. Кроме того, наблюдение за работающим персоналом на их рабочих местах обосновывается как превентивная мера против выполнения служащими незаконных действий, за которые в конечном счете приходится отвечать корпорации в целом.

Уже было рассмотрено немало различных дел, связанных с наблюдением за сотрудниками. Так, например, в 1995 году руководство филиала компании Chevron было обвинено по статье о сексуальной агрессии за распространенное по внутренней сети компании электронное письмо, озаглавленное «25 причин, почему пиво лучше женщин». Дело было урегулировано без суда выплатами в размере 2,2 миллиона долларов со стороны компании Chevron, и с тех пор компания начала вести постоянное наблюдение за содержанием почтовых сообщений своих сотрудников. В июле 2000 года корпорация Dow Chemical уволила 50 своих сотрудников и привлекла к административному наказанию еще 200 человек за посещение порнографических сайтов. В октябре 1999 года 40 работников компании Xerox также были уволены за просмотр запрещенных сайтов (компания Xerox следит за использованием Интернета со стороны более чем 90 000 своих сотрудников по всему миру).

Короче говоря, нравится это работникам компаний или нет, однако наблюдение за ними становится общепринятой практикой.

## Полицейские расследования

Помимо наблюдения со стороны работодателя за сотрудниками компаний в рабочее время, существует еще один вид узаконенного шпионажа, связанный с расследованиями преступлений. Вряд ли большинство полицейских назовут себя шпионами либо посчитают себя участниками шпионской деятельности, но на самом деле разница только в используемой терминологии. Разведывательная деятельность, наблюдение и расследование – все это всего лишь социально приемлемые термины, используемые для обозначения шпионажа.

Правоохранительные органы в первую очередь заинтересованы в поиске доказательств совершенного вами преступления. Причем сбор доказательств может выполняться как до, так и после предъявления вам обвинения в незаконной деятельности.

Если вы находитесь под следствием, за всеми вашими действиями в сети может вестись постоянное наблюдение (это касается электронной почты, служб обмена мгновенными сообщениями и навигации по просторам Интернета), а в определенных обстоятельствах офицеры полиции имеют право на получение физического доступа к компьютеру, чтобы проанализировать хранимую на нем информацию, а также установленное аппаратное и программное обеспечение.

В случае предъявления вам обвинения в преступлении ваш компьютер почти наверняка превратится в объект пристального внимания со стороны правоохранительных органов. При этом технический персонал может просматривать содержимое вашего жесткого диска и других информационных носителей в поисках доказательств вашей причастности к данному преступлению либо другим возможным правонарушениям.



Судебное наблюдение за вашим компьютером представляет собой процесс сбора компьютерных улик, который рассматривается в главе 5 данной книги.

Когда дело доходит до компьютерного шпионажа, правоохранительные органы вынуждены придерживаться достаточно строгих правил. В соответствии с Конституцией граждане имеют различные права, защищающие их от безосновательного вмешательства в частную жизнь со стороны правительственные служб, независимо от того, являетесь вы правонарушителем или нет. Поэтому для проведения полицейского расследования, то есть для наблюдения за вашим компьютером, требуется судебный ордер либо санкция прокурора на обыск.

Тем не менее после террористической атаки 11 сентября 2001 года Конгресс предоставил правоохранительным органам более широкие полномочия в плане проведения расследований.



Расширенные права в соответствии с Патриотическим Актом США (USA PATRIOT Act) в плане компьютерного наблюдения обсуждаются в главе 2 данной книги.

Несмотря на строгость правил, регламентирующих сбор доказательств, известно немало фактов превышения полномочий отдельными представителями правоохранительных органов, как случайных, так и преднамеренных. Примером может послужить секретный меморандум ФБР, просочившийся в средства массовой информации в октябре 2002 года, в котором описываются некоторые ошибки бюро расследований, такие как перехват электронных почтовых сообщений ни в чем не повинных граждан, запись их телефонных разговоров, незаконное видеонаблюдение за подозреваемыми и проведение несанкционированных обысков. Поэтому, хотя в большинстве случаев правоохранительные органы соблюдают правовые нормы, пускай вас не удивляет тот факт, что так бывает отнюдь не всегда.

## Разоблачения: хороший полицейский или плохой полицейский?

Летом 2000 года ФБР занималось расследованием серии атак на коммерческие сайты, с которых была украдена конфиденциальная информация по кредитным карточкам. След указывал на хакеров из России.

Специальный агент ФБР Майкл Шулер разработал спецоперацию по поимке взломщиков. В ноябре 2000 года двое россиян – Василий Горшков и Алексей Иванов прибыли в США, чтобы принять участие в конкурсе на замещение вакантных должностей, объявленном в Сиэтле компанией Invita, занимающейся предоставлением услуг по обеспечению компьютерной безопасности. На собеседовании представители компании Invita попросили гостей из России продемонстрировать свои навыки. В качестве примера они удаленно подключились к своим собственным компьютерам, расположенным в Челябинске. Однако вместо приема на работу российские соискатели угодили за решетку. На самом деле Invita являлась фиктивной компанией, учрежденной ФБР специально для поимки преступников, а в качестве ее сотрудников выступали сами агенты бюро расследований.

Горшков и Иванов не знали, что ФБР установило программу перехвата сетевых пакетов на компьютер, который использовался ими для доступа к своим компьютерам в России. Сразу после их ареста Шулер воспользовался сохраненными именами пользователей и паролями для повторного подключения к компьютерам подозреваемых и загрузил по сети 250 Гб доказательств причастности россиян к проникновению в закрытые системы и краже информации о кредитных карточках.

Шулер стал первым агентом ФБР, прибегшим к электронной технологии «удаленного изъятия доказательств». При этом Шулер не располагал никакими ордерами на обыск до момента загрузки уличающей информации (ордер был выдан уже после свершившегося факта), и никто из представителей ФБР не обращался предварительно за содействием в российские правоохранительные органы. Этим фактом воспользовался адвокат Горшкова, как и фактом нарушения российского законодательства, однако судья решил, что действие российских законов не может распространяться на американских агентов. Приблизительно два года спустя, в августе 2002-го, ФСБ России обвинила Шулера в несанкционированном доступе к компьютерам в России и завела на него уголовное дело. Скорее всего, данное дело будет уложено по дипломатическим каналам, однако на месте Шулера мы бы не стали планировать поездки в Восточную Европу в ближайшем будущем.

В качестве послесловия можно упомянуть о том, что Горшков был приговорен к трем годам тюремного заключения и выплате компенсаций в размере 690 тысяч долларов. Иванов был также признан виновным по многим пунктам обвинения еще в августе 2002 года, и на сегодняшний день суд должен был определить для него окончательную меру пресечения\*.

Компетентность различных полицейских в плане компьютерного шпионажа варьируется в широких пределах. Как правило, в случае недостатка компетентных лиц правоохранительные органы обращаются за помощью к техническим специалистам, обладающим навыками по сбору и анализу электронных улик. Большинство работников полиции не очень хорошо разбираются в компьютерах, а те немногие, кто сведущ в вопросах компьютерной техники, по горло завалены делами, в которых фигурируют электронные доказательства. Сегодняшние тенденции таковы, что полицейские управления вынуждены направлять собственных сотрудников на стажировку, чтобы обучить их использованию новых компьютерных технологий в повседневной деятельности. Из-за высокого уровня доходов частных предприятий, а также вследствие различий в уровне зарплат работников правоохранительных органов и, к примеру, работников высокотехнологичных компаний, совсем немногих опытных компьютерщиков, которые могли бы отлично справиться со сбором электронных улик, привлекает участие в судебных расследованиях.

На практике чем больше полицейское управление, тем выше вероятность наличия в его штате высококлассного компьютерного специалиста. Федеральные управления, такие как ФБР или контрразведка, располагают наиболее квалифицированными кадрами, но, опять-таки, навыки и способности отдельных технарей могут варьироваться в широких пределах.

## Частные сыщики и консультанты – неофициальные расследования

К другой категории шпионов, которые законно или незаконно могут вести за вами электронное наблюдение, относятся частные детективы и технические консультанты. Эти специалисты занимаются поиском улик, связанных с уголовными или гражданскими делами. К их услугам могут прибегать коммерческие компании, правоохранительные органы либо частные лица. Частные сыщики обычно имеют некоторый опыт работы, приобретенный в ходе различных расследований. Консультанты, как правило, обладают узкой специализацией, обычно имеющей отношение к взлому компьютерных сетей и связанных с этим судебных расследований.

\* В августе 2003 года Горшков вернулся на родину после отбытия срока, Иванов продолжает отбывать заключение. – Прим. ред.

## ЧАСТНЫЕ СЫЩИКИ

Хотя стереотип сыщика Сэма Спейда в длинном плаще крепко укоренился в представлении американских обывателей, с течением времени наружность рядового частного детектива претерпела значительные перемены, и теперь их все чаще официально привлекают для расследования компьютерных преступлений. Частные детективы уже давно принимают участие в проведении аудио- и видеонаблюдений, поэтому неудивительно, что с распространением новых технологий, детективы стали привлекаться для наблюдения за компьютерной техникой.

Частные сыщики старшего поколения, как правило, в свое время пришли в частный бизнес из правоохранительных органов и обладают минимальными компьютерными навыками. Конечно большинство частных детективов умеют работать с компьютером, но, как правило, их знания ограничиваются использованием широко распространенных и простых в применении наблюдательных программ. В то же время новое поколение частных сыщиков, выросшее в эпоху компьютеров, изначально является более образованным в плане компьютерной грамотности, чем их отцы и деды.

### Контрмеры: 5 крупнейших судебных расследований

Не стоит думать, что технические консультанты являются собой исчезающий род «вольных художников», обожающих заниматься вопросами компьютерной безопасности. Спрос на услуги компьютерных сыщиков и консультантов растет, и крупные корпорации с удовольствием тратят средства на хороших специалистов в данной области.

К примеру, финансовый гигант Deloitte & Touche содержит в Бостоне исследовательскую лабораторию, прозванную в народе «комнатой войны». Эта лаборатория буквально нашпигована различной шпионской техникой на сумму около полумиллиона долларов, которая используется для наблюдения за компьютерами клиентов. Технические специалисты в состоянии удаленно восстанавливать поврежденные области жестких дисков и в прямом смысле по байтам анализировать обнаруженную информацию. В своих расследованиях специалисты компании сталкиваются со всем спектром преступлений: от административных правонарушений до убийств.

Расследуя около 250 преступлений в год, эта компания процветает.

## Шпионаж: мусорные ворота

В 2000 году гигант по производству баз данных, компания Oracle, наняла сыщиков из IGI (Investigative Group International – Международной группы расследований) для наблюдения за двумя организациями: Независимым институтом (Independent Institute) и Ассоциацией конкурирующих технологий (ACT). (Большинство сотрудников IGI в прошлом являлись агентами ФБР, кроме того, IGI приобрела дурную славу в ходе недавних разбирательств по делу президента Била Клинтона, обвиняемого в связях с Полой Джонс и Моникой Левински.) Это совпало с началом расследования Антимонопольного комитета против компании Microsoft, когда на обе вышеупомянутые бесприбыльные организации, оказывающие всестороннюю поддержку корпорации Microsoft, пали подозрения в финансовой взаимосвязи с Вашингтонской компанией Redmong.

Летом 2000 года женщина, представившаяся как частный сырщик Бланка Лопес, предложила привратникам взятку в размере 700 долларов наличными, чтобы пробраться на территорию офиса компании ACT через ворота, предназначенные для вывоза мусора. Затем Лопес проникла в закрытое здание, воспользовавшись пропуском, принадлежащим Роберту Уотерсу, частному детективу, связанному с IGI, который арендовал офис в том же здании, что и компания ACT, для фирмы под названием Upstream Technologies.

После завершения расследования полицейское управление Вашингтона, округ Колумбия, заявило, что никакого частного детектива по имени Бланка Лопес не существовало. Любопытные журналисты задали вопрос: являлась ли компания Upstream Technologies всего лишь прикрытием для полицейского расследования, чтобы разместиться поближе к офису ACT? Ларри Элисон, генеральный директор компании Oracle, признал факт найма сотрудника IGI, оправдываясь тем, что это помогло разоблачить компанию Microsoft, однако весьма осторожно обошел вопрос проникновения в здание через ворота для вывоза мусора: «Мы просто готовили наш мусор для вывоза в Редмонд, а они избрали его как средство проникновения».

Как и подозревала компания Oracle, компании ACT и Independent Institute, презентовавшие себя как независимые адвокатские группы, на самом деле были связаны с корпорацией Microsoft, пытающейся склонить общественность на свою сторону в антимонопольном расследовании. Некто проинформировал Wall Street Journal про инцидент с вывозом мусора, в результате чего журналистам представилась возможность соопоставить все факты о контактах компаний Oracle и IGI. Представители Oracle заявили, что IGI гарантировала использование полностью законных методов расследования. Этот инцидент привлек внимание национальных средств массовой информации на одну-две недели, после чего вскоре был забыт.

Хотя в своем большинстве частные сыщики не обладают такими глубокими техническими познаниями, как другие категории компьютерных шпионов, они, как правило, преуспевают в искусстве социотехники. То, что частные детективы и компании, ведущие неформальные расследования, называют «социотехникой», представляет собой применение психологических приемов в рамках непринужденной беседы, позволяющих выведывать нужную информацию у нужных людей. А как показывает практика, в некоторых случаях использование слабостей человеческой натуры приносит не меньший успех, чем тщательно подготовленная техническая атака.

## КОНСУЛЬТАНТЫ

Коммерческие предприятия и правоохранительные органы все лучше понимают, что, когда дело доходит до вторжения в закрытые системы с целью сбора необходимой информации, они не в состоянии сами справиться с этой задачей. В связи с этим в последние годы наблюдается грандиозный рост индустрии консалтинговых фирм, работающих в сфере компьютерной безопасности. И все это благодаря увеличению числа атак со стороны взломщиков и активно муссируемому вопросу компьютерной безопасности со стороны массмедиа.

Высококвалифицированные технические консультанты привлекаются для поиска шпионов и обнаружения брешей в защите систем, дабы предотвратить возможную кражу информации. Кроме того, подобные консультанты нередко нанимаются и для проведения обратных действий – то есть для наблюдения и проникновения в компьютерные системы в ходе судебных разбирательств. Обычно подобные консультанты имеют степени в области компьютерных наук либо в родственных областях, а также различные промышленные сертификаты.

Разумеется, навыки, необходимые для поимки компьютерных шпионов, могут сами по себе использоваться в целях шпионажа. Можно утверждать, что большинство консалтинговых компаний и отдельных лиц действуют достаточно этично и в рамках закона, защищающего нас от несанкционированного электронного шпионажа, однако, как и в любом другом бизнесе, находятся отдельные представители, преступающие закон в погоне за выгодой. И, увы, неэтичных консультантов, выступающих в роли шпионов, очень трудно обнаружить, учитывая их глубокие знания по данному предмету и осведомленность обо всей кухне защиты изнутри.

## «Невидимки» – поддерживаемые правительством агенты разведки

Когда вы произносите слово «шпион», многие люди представляют секретного правительственный агента в плаще с поднятым воротником, в низко надвинутой шляпе и черных очках. В шпионской терминологии их

называют «невидимками» или «призраками». Причем эти невидимки, работающие по поручению правительства и являющиеся представителями второй по счету древнейшей профессии, обычно хорошо справляются со своими обязанностями.

На самом деле шпионаж нередко оказывается скучной и нудной работой. Забудьте на минуту о Джеймсе Бонде и тем более об Остине Пауэрсе. Шпионаж связан с методичным сбором различной информации как из открытых, так и засекреченных источников и с проведением изнурительно-анализа для получения целостной картины происходящего на основе отдельных известных фактов. В дальнейшем полученная информация может использоваться для выполнения выгодных правительству операций.

Традиционно разведывательные управления различных стран борются друг с другом, пытаясь защитить свои политические и военные секреты, и не менее традиционно цепляются за новые оправдания своего существования после окончания холодной войны. К двум их новым миссиям теперь относятся экономическая разведка и, с недавних пор, борьба против терроризма, на которой делается наибольший акцент.

Разведывательные операции по сбору информации могут иметь определенные цели либо носить общий характер (к примеру, поиск информации по конкретному виду крылатых ракет либо сбор сведений об оборонной ракетной системе в целом). Если разведывательное управление заинтересовано в информации, которой вы располагаете, все усилия бюро будут направлены на поиск уязвимых мест в вашей системе защиты и нахождение способов скрытого проникновения для получения нужной разведке информации.

Программы, подобные ECHELON, используют «подход пылесоса». Все ваши данные, переписка по электронной почте и другая информация, которой вы обмениваетесь через Интернет, записывается в общую кучу, а затем анализируется по ключевым словам. Вдобавок, поскольку программа ECHELON была изначально предназначена для обмена информацией (в том числе и для межгосударственного), о таких тонкостях, как санкции и ордера на применение наблюдательных программ, нередко забывают. Это имеет место, например, когда речь идет о сборе правительством Австралии сведений о находящихся на ее территории гражданах Соединенных Штатов с последующей передачей данных в разведывательное управление США.



Исчерпывающее обсуждение программы ECHELON и других компьютерных наблюдательных систем, используемых правительством США, ожидает вас в главе 13 данной книги.

Поэтому, если когда-нибудь разведывательное управление заинтересуется вашей компанией, приготовьтесь к тому, что против вас будут направлены огромные людские и технические ресурсы (опытные технари, новейшее аппаратное обеспечение и профессиональные шпионы).

## ВНУТРЕННЯЯ РАЗВЕДКА

Разведывательное Сообщество включает в себя 13 государственных управлений и организаций, занимающихся разведывательной деятельностью для правительства Соединенных Штатов. К организациям, участвующим в шпионаже и контршипионаже, относятся: Государственный департамент, Министерство энергетики, Министерство финансов, Федеральное Бюро Расследований, Национальное разведывательное управление, Национальное управление геодезии и картографии, Разведка корпуса морской пехоты, Военно-воздушная разведка, Морская разведка, Военная разведка, Национальная служба безопасности и Центральное Разведывательное Управление.

До середины 1970-х годов ЦРУ и другие члены Разведывательного Сообщества осуществляли нелегальный шпионаж за американскими гражданами. Несмотря на то, что в соответствии с уставом ему было запрещено заниматься подобной деятельностью, ЦРУ продолжало вести наблюдение за тысячами американских подданных в рамках операции CHAOS, изначально направленной на сбор информации о недовольных, протестующих против войны во Вьетнаме, активистах среди студентов и чернокожих националистах. Комиссия Черча (комиссия штата по расследованиям под руководством сенатора Фрэнка Черча из Айдахо) раскрыла множество фактов подобных злоупотреблений, в результате чего размеры внутреннего шпионажа со стороны правительства за гражданами США значительно сократились. Однако после террористической атаки 11 сентября 2001 года и обнародования Патриотического Акта США, подробно рассматриваемого во второй главе данной книги, разведывательным управлениям были возвращены широкие полномочия на проведение шпионажа за гражданами США. И теперь мы, как в былые времена, снова становимся свидетелями несоблюдения прав на неприкосновенность частной жизни во имя общегосударственной безопасности и превышения разведкой своей власти в отношении отдельных лиц и компаний.



Слушания комиссии Черча охватывали множество аспектов тогдашней политической жизни: террористические попытки со стороны иностранных лидеров, правительственные перевороты, незаконное внутреннее наблюдение со стороны ЦРУ и ФБР. Подробнее об этой комиссии вы можете узнать из книги «ЦРУ – секреты одного из наиболее могущественных разведывательных управлений в мире», написанной Рональдом Кесслером.

Хотя ЦРУ и Управление национальной безопасности заявили о своей непричастности к фактам экономического шпионажа, все, кто были хотя бы мало-мальски связаны с разведкой, знали, что это неправда. В 1995-м, вскоре после того, как глава ЦРУ заявил, что его организация не занимается выведыванием коммерческих секретов, раскрытие которых предоставило бы американским корпорациям конкурентные преимущества, пять агентов ЦРУ были высланы из Франции по обвинению в экономическом

шпионаже. Существует непроверенная информация о том, что Управление национальной безопасности занималось перехватом факсов и телефонных звонков от иностранных компаний, собирая информацию, которая могла бы дать корпорациям Boeing и Raytheon преимущества в конкурентной борьбе на торгах.

Американские разведывательные управлении преуспевают в технике шпионажа. Они отлично справляются с перехватом и сбором информации, в особенности при использовании цифровых носителей и электронных средств связи. По этой причине, кроме современной электронной почты и спутниковых телефонов, террористическая сеть Аль-Каида широко использовала старые, неэлектронные средства общения.

## ВНЕШНЯЯ РАЗВЕДКА

Как вы понимаете, любое государство заинтересовано в том, чтобы его предприятия и компании имели конкурентное преимущество перед иностранными корпорациями. Такие страны, как Китай, Южная Корея, Франция и Израиль, придерживаются такого мнения уже довольно давно и вполне преуспевают в разведывательной деятельности, предназначенней для прикрытия экономического шпионажа, направленного на поддержку их собственных крупных национальных корпораций. При этом следует заметить, что они, в отличие от США, не подходят столь щепетильно к попыткам запрета подобной разведывательной деятельности.

Американское общество промышленной безопасности проводило выборочные расследования фактов промышленного шпионажа, от которых пострадали американские компании. В результате проведенного в 1998 году исследования в качестве государств, представляющих собой основную угрозу безопасности Соединенных Штатов, были названы: Китай, Япония, Франция, Великобритания, Канада, Мексика, Россия, Германия, Южная Корея и Израиль.

Во время холодной войны существовали четкие различия между «своими» и «чужими», которые теперь несколько поистерлись. Многие страны вовлечены в экономический шпионаж, направленный против США и его политических союзников. В соответствии с отчетами французских разведслужб, места первого и бизнес-классов на самолетах компаний Air France оборудованы наблюдательными системами, позволяющими прослушивать частные разговоры, а оставленные американскими бизнесменами в номерах отелей мобильные компьютеры нередко подвергаются тщательному осмотру.

Поэтому, если ваша коммерческая деятельность касается работы с иностранными компаниями, задумайтесь о потенциальной возможности экономического шпионажа.

## Шпионаж: проект РАНАВ

С середины 90-х годов распространились слухи о санкционированной немецким правительством подпольной деятельности организаций по обеспечению компьютерной безопасности, поддерживающих хакеров, которые принимали участие в операции под кодовым названием РАНАВ.

Название РАНАВ эта операция получила в честь библейской проститутки, которая совала нос не в свои дела. По информации различных источников, на протяжении 1987 года внутреннее подразделение Немецкой Федеральной разведывательной службы (Bundesnachrichtendienst, или BND) начало секретную операцию, направленную на проникновение в закрытые сети и базы данных с целью кражи технических и экономических секретов. Предположительно в рамках проекта осуществлялись атаки на компьютеры России, США, Японии, Франции, Италии и Великобритании. Среди главных достижений данной группы – дискредитация корпоративной сети компании DuPont и взлом протокола безопасных транзакций SWIFT, предназначенного для банковской сферы, благодаря чему хакеры могли следить за финансовыми операциями и даже проводить подложные транзакции для перевода денег с одного счета на другой.

О проекте РАНАВ существует очень мало достоверной информации, однако даже если допустить правдивость малой ее части, то мы имели дело с иностранным шпионажем на правительственноом уровне еще в то время, когда крупные корпорации только начинали активное внедрение компьютерной техники.

## Преступники – те, кто ищет собственную выгоду

Хотя преступником считается любой шпион, нарушающий закон, это обозначение обычно применяется к шпионам, занимающимся кражей информации в целях личного обогащения. Для подобных авантюристов компьютерный шпионаж является источником получения незаконной прибыли либо другой личной выгоды. Всех преступников можно разделить на две категории: отдельных представителей шпионского бизнеса и членов организованных группировок.

## ВЗЛОМЩИКИ – КРАКЕРЫ

Взломщиками называют людей, незаконно проникающих в чужие компьютеры. (Я специально использую слово «взломщик» (cracker – кракер) вместо широко распространенного термина «хакер», которое на самом деле обозначает человека с глубокими техническими знаниями, не обязательно нарушающего закон.) Как правило, взломщики заинтересованы в

получении доступа к информации, связанной с финансами, и, в частности, к номерам кредитных карточек, бюджетам и паролям, позволяющим проникать в другие закрытые системы. Нередко взломщики занимаются вредительством – удалением файлов или публикацией конфиденциальной информации. В зависимости от уровня подготовки взломщики могут использовать автоматические средства и сценарии для проникновения в удаленные системы; более опытные взломщики, вроде беспринципных администраторов, провайдеров Интернета, – как автоматические, так и ручные средства; ну а настоящие профессионалы своего дела хорошо разбираются во всей подноготной операционных систем и сетевых протоколов. Естественно, неопытных взломщиков намного больше, чем профессионалов, и их достаточно легко поймать за использованием шпионского программного обеспечения.

## ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ

Хотя вы вряд ли сталкивались с людьми, вовлеченными в компьютерный шпионаж силами The Sopranos, организованная преступность имеет свое будущее, и это будущее заключено в компьютерах. Компьютеры предлагают новые способы незаконного зарабатывания денег, а подслушивание и просматривание чужой информации является одним из таких способов. Организованные преступники заинтересованы в первую очередь в финансовых и других личных данных, которые могут применяться для мошенничества или же планирования других преступлений, необязательно связанных с компьютерами.

Организованная преступность во многом напоминает правоохранительные органы в плане приспособляемости к новым технологиям. Большая часть преступников старшего поколения не обладает достаточными техническими навыками в данной области, однако, по мере того, как им на смену приходит новое поколение, потенциал организованной преступности в плане компьютерного шпионажа возрастает быстрыми темпами. Единственным исключением из этого являются наркокартели, которые всегда имели и имеют в своем штате самых опытных технических специалистов и располагают самыми современными достижениями науки и техники, стоящими на страже их собственной инфраструктуры или используемыми для наблюдения за конкурентами.

## Доносчики, действующие ради всеобщего блага

К еще одному типу шпионов, называемых благожелателями (с учетом того, за кем они шпионят), относятся доносчики, раскрывающие ради общественного блага факты коррупции и сомнительной деятельности. Разумеется, подобные доносчики не смогли бы ничего добиться без помощи средств массовой информации, которые предоставляют им возможность высказаться, а иногда проводят собственные расследования.

## Компьютерный шпионаж в колумбийском стиле

Колумбийские наркокартели затратили миллиарды долларов на создание сложной компьютерной инфраструктуры. В 1994 году колумбийская полиция совершила рейд на комплекс в Кали. В здании был обнаружен майнфрейм-компьютер IBM AS400 стоимостью в 1,5 миллиона долларов с 6 подключенными к нему мониторами. Этот компьютер, получивший название «компьютера Сантакруза» в честь главы картеля в Кали Хосе Сантакруза Лондоно, был отправлен в США для проведения детального анализа. Информация, найденная на этом компьютере, приобрела статус секретной, однако со временем часть ее стала известна общественности.

Компьютер содержал базу данных домашних и рабочих телефонов агентов и дипломатов США (известных и давно подозреваемых правоохранительными органами, разведкой и военными Соединенных Штатов), пребывающих в Колумбии. Кроме того, телефонная компания снабжала картель информацией о телефонных переговорах этих людей (куда звонили они, и кто звонил им). Собственный разведывательный отдел картеля впоследствии использовал написанное ими же программное обеспечение для сравнения предоставленных телефонной компанией сведений с имеющимся у них списком работников правоохранительных органов, агентов гражданской и военной разведки, чтобы получить информацию по входящим и исходящим звонкам. Затем по телефонным номерам устанавливались имена и адреса звонивших, в результате формировался список людей, которые могли подозревать о существовании картеля.

Официальные представители правоохранительных органов так и не сообщили, что произошло с информаторами, список которых был обнаружен в компьютере Сантакруза, однако, учитывая склонность картеля к насилию, можно предположить, что подозреваемые были наказаны или убиты за раскрытие информации. Ни один общественный источник не взялся оценить количество людей, лишившихся жизни по подозрению компьютера.

Шпионами-доносчиками обычно называют работников компаний, оказавшихся свидетелями незаконной деятельности своих работодателей и не имевших сил молчать дальше. В роли «доносчиков» могут также выступать представители массмедиа, ведущие собственные журналистские расследования. Нередко доносчики обладают достаточно глубокими знаниями в области компьютерной техники и Интернета, применяя их для раскрытия фактов правонарушений.

С появлением Интернета доносчики получили возможность распространять известную им информацию, сохраняя при этом свое инкогнито. При помощи временных ящиков электронной почты и программ анонимного перенаправления корреспонденции эта категория шпионов может передавать информацию третьим лицам, не боясь быть разоблаченными. Все чаще через Интернет отправляются электронные письма и краткие сообщения сомнительного содержания, компрометирующие деятельность тех или иных фирм либо отдельных лиц.

Так что, если вы работаете в компании вроде Enron, знайте, что среди ваших сотрудников могут находиться доносчики – это, в конце концов, не самое худшее, что может с вами случиться.

## Шпионаж: Cryptome.org

Один из Нью-Йоркских архитекторов, Джон Янг, свято верит в неприкасаемость частной жизни и поэтому разоблачал тех, кто вмешивался в частную жизнь других людей. Он открыл свой сайт cryptome.org, где выносил на суд общественности информацию, ранее известную только посвященным, касающуюся деятельности разведывательных управлений, правительства, прав на неприкасаемость частной жизни, криптографии, шпионажа и свободы личности.

За период с 1996 года Янг насобирал внушительную коллекцию изобличительных сведений, полученных из анонимных источников. В обнаруженной им информации имеются списки иностранных агентов разведки; списки покупателей оборудования, предназначенного для шпионажа, среди которых замечены представители правительства, армии и правоохранительных органов; копии компрометирующего наблюдательного программного обеспечения; а также различные правительственные документы, полученные из общедоступных и закрытых источников.

Веб-сайт cryptome.org успел приобрести международную известность за публикацию провокационных материалов для людей, изучающих искусство шпионажа. Этот сайт активно посещается частными детективами и адвокатами, поклонниками шпионских романов и даже программами-роботами организаций, занимающихся разведывательной деятельностью (которые передают данные для изучения правительенным аналитикам, дабы выявить каналы утечки информации либо составить общую картину происходящих событий).

## Друзья и семья – с ними только в разведку ходить...

Хотя обычно шпионаж рассматривают в контексте коммерческой либо правительственной деятельности, на самом деле с точки зрения шпиона-жа наиболее уязвимым является ваш домашний компьютер. Однако в этом случае угроза исходит не от взломщиков, проникающих извне, а от ваших собственных друзей и членов семьи.

Возможно, они подозревают вас в чем-то нехорошем и ищут доказательства. Возможно, их просто замучило любопытство: чем это вы занимаетесь на вашем компьютере? А поскольку компьютеры стали неотъемлемой частью нашей жизни, то и часть нашей частной жизни находит свое отражение в них.

Что касается семейного «шпионажа», то наибольшую угрозу для вас могут представлять так называемые keylogger – программы для перехвата и сохранения в файл всего, что вводится с клавиатуры. Подобное наблюдательное ПО подробно рассматривается в главе 8 данной книги.



В большинстве своем друзья и семья обычно обладают наименьшим уровнем технических познаний по сравнению со всеми другими категориями шпионов, и чаще всего они ограничиваются просмотром файлов, с которыми мы работаем, или же использованием простого в установке коммерческого либо свободно распространяемого ПО.

## СОЖИТЕЛИ

Количество совместно проживающих людей (будь то друзья по общежитию, влюбленные пары и т. д.) либо лиц, сдающих комнаты квартирантам, в настоящее время постоянно увеличивается. Если раньше речь шла лишь о совместном проживании в студенческие годы, то сейчас, в связи с тяжелым экономическим положением, даже семейные пары с 20...30-летним стажем, недавно купившие собственный дом, берут к себе квартирантов, дабы хоть как-то разгрузить семейный бюджет.

Поэтому, где бы и с кем бы вы ни жили, незащищенный компьютер становится весьма соблазнительной целью для того, кто хочет сунуть нос в ваши дела.

## НАШИ ВТОРЫЕ ПОЛОВИНЫ

В наши дни понятие «доверие» становится старомодным. Ревнивые партнеры и супруги все чаще ищут в компьютерах своих благоверных доказательства их виртуальных романов.

## Разоблачения: лучшие друзья?

Николас Джей Сучита, 19 лет от роду, проживал в Бэй-Сити, Мичиган вместе со своей 19-летней подругой. Его девушка утверждала, что они с Николасом – лучшие друзья со времени окончания школы.

В январе 2002 года знакомые этой девушки сообщили ей о существовании в Интернете видеоматериалов, в которых она со своим другом занималась сексом в снимаемой ими комнате. После этого девушка залезла в компьютер своего приятеля и нашла собственные снимки в обнаженном виде. Женщина обратилась в полицию, которая обнаружила скрытую веб-камеру, подключенную к ее компьютеру, и четыре видеофайла, содержащие записи их любовных утех.

В мае 2002 года Сучита был привлечен к ответственности по двум статьям: за установку подслушивающего оборудования и за распространение информации, полученной незаконным путем. До этого он уже обвинялся в компьютерном взломе во время работы в местной школе округа. В предыдущем деле Сучита и его родители подали на школу за клевету, вмешательство в частную жизнь, преднамеренное нанесение моральной травмы и крайнюю халатность, в результате которой Сучита был ошибочно назван хакером.

Новое дело должно рассматриваться в конце апреля 2003 года. Если Сучита будет признан виновным, ему грозит до двух лет тюрьмы и крупные денежные штрафы.

Возможно, следует предпринимать меры против полуанонимных виртуальных отношений, которые осуществляются путем электронной переписки, обмена мгновенными сообщениями, участия в чатах и нередко пропагандируются средствами массовой информации, распространяющими сенсационные факты онлайновых любовных романов и киберсекса. Создается впечатление, что даже сама реклама средств аудио- и видеонаблюдения в Интернете заставляет людей сомневаться в верности своих «половинок». Так или иначе, продажа средств шпионажа для наблюдения за своими «вторыми половинами» превращается в процветающий бизнес.

## РОДИТЕЛИ

С ростом популярности Интернета родители забеспокоились о защите своих чад от информации в виртуальном пространстве, рассчитанной на взрослую аудиторию, ведь теперь, помимо веб-сайтов, дети имеют доступ к чатам, службам мгновенных сообщений и личным почтовым ящикам.

В то же время средства массовой информации часто преувеличивают опасности, приносимые Интернетом, что заставляет родителей шпионить за собственными детьми, наблюдая за всеми их действиями за компьютером. Программное обеспечение, позволяющее ограничивать доступ к определенной категории веб-сайтов, нередко содержит в своем составе средства для протоколирования общения в чате либо по электронной почте, а программы типа keylogger активно рекламируются как лучшее средство для родителей, желающих знать, чем занимаются их дети в сети.

## Разоблачения: наблюдательное ПО

В 2001 году Стивен Пол Браун развелся со своей женой Патрицией, однако их развод отнюдь нельзя было назвать полюбовным. Браун установил коммерческую keylogger-программу под названием eBlaster на компьютер бывшей жены. Эта программа сохраняла сообщения электронной почты, посещенные веб-узлы Интернета, журналы чатов, после чего отправляла копию собранной информации на электронный почтовый ящик Брауна. Браун сделал ошибку, упомянув содержимое электронной переписки своей жены. В результате у нее возникли подозрения, которыми она поделилась с подразделением по расследованию технических преступлений, подчиняющимся генеральному прокурору штата Мичиган.

Браун был обвинен в установке подслушивающих устройств, незаконном наблюдении, использовании компьютера в целях совершения преступления и несанкционированном доступе к чужому компьютеру (все вышеупомянутые обвинения являются уголовно наказуемыми). Сейчас ему угрожает пятилетнее тюремное заключение и штрафы в размере до 19 тысяч долларов.

## ДЕТИ

Немалая часть взрослого населения не обладает достаточными познаниями в области компьютерной техники. Конечно, большинство людей умеет, по крайней мере, работать с текстовыми процессорами, отсылать электронную почту или перемещаться по Интернету, однако они не обладают более глубокими знаниями, особенно в плане защиты информации. С другой стороны, их дети, воспитанные на Интернете, с малых лет обладают техническими навыками, намного превосходящими способности их собственных родителей.

Поэтому теперь, как юные шпионы, дети представляют собой немалую угрозу – шпионские средства обсуждаются в электронной почте и чатах, и их легко можно загрузить с веб-сайтов, поддерживаемых профессиональными взломщиками. Смекалистая 12-летняя девочка вполне способна установить программу мониторинга клавиатуры на семейный компьютер

и следить за тем, что делают на компьютере ее мама, папа, братья или сестры. Таким образом она легко может узнавать о проводимых финансовых транзакциях своих родителей, их подключении к другим компьютерам, электронной переписке и навигации в среде Интернет.

## Определите свой уровень паранойи

Вы еще не забыли, что говорил Сунь-Цзы: «Чтобы иметь преимущество в битве, вы должны хорошо знать себя». Итак, вопрос сводится к тому, насколько следует отдаваться во власть паранойи, зная, что за вами может шпионить кто угодно и где угодно.

Частично ответ содержится в том, насколько хорошо вы себя знаете (либо, в случае коммерческого шпионажа, насколько хорошо вы знаете свою организацию). Ниже приводится небольшой тест, который призван помочь вам в этом вопросе. Не старайтесь ответить как можно быстрее, лучше хорошо подумайте над каждым ответом:

- Можете ли вы объяснить различие между высокой вероятностью угрозы для вашего компьютера или сети и безосновательными подозрениями? Если вы хорошо разбираетесь в вертолетах, переворотах и нераскрытых правительственные заговорах, отвечайте «нет».
- Можете ли вы примерить шпионский плащ и воспользоваться оружием шпиона, чтобы пробить брешь в защите вашей компьютерной системы? Умение представить себя на месте неприятеля помогает увидеть собственные слабости. Мы еще предложим вам потренироваться в этом чуть позже.
- Намерены ли вы применять политику безопасности, чтобы гарантировать защищенность вашего компьютера? Политика безопасности чрезвычайно важна, однако она выходит за рамки предмета обсуждения данной книги, в которой мы намерены сосредоточиться на тактике шпионажа и соответствующих контрмерах.
- Будете ли вы следовать определенной вами политике безопасности? Если вы полагаете, что политика безопасности является пустой тряской времени либо слишком сложна для исполнения, отвечайте «нет».
- Относитесь ли вы к тому типу людей, которые согласны вытерпеть небольшие неудобства ради поднятия уровня безопасности? Как показывает практика, при использовании дополнительных мер защиты удобство пользования системой снижается.

Если вы ответили «да» на все вышеперечисленные вопросы, вы отнюдь не пааноик – просто вы хорошо подкованы в данной области и таким образом снижаете шансы на успех у потенциальных наблюдателей за вами.

Если вы дали положительный ответ на большую часть вопросов, обратите внимание на те вопросы, на которые вами был дан отрицательный ответ. Именно с ними могут быть связаны ваши слабые места, делающие вас уязвимыми в плане компьютерного шпионажа.

## Уровень риска: цветовые коды

Полковник Джек Купер, выдающийся инструктор по огнестрельному оружию, разработал широко используемую систему цветовых кодов для обозначения осведомленности и подготовленности, составленную на основе личного опыта, приобретенного во время службы в морской пехоте. (Не так давно правительство Соединенных Штатов утвердило похожую схему для обозначения защитных кодов.) **Итак, в соответствии со схемой Купера уровни риска можно разделить на четыре цветовых группы:**

- **Белый цвет.** Полное неведение о возможных источниках угрозы и незнание информации, которая способна натолкнуть вас на мысль о вероятной опасности. Большинство людей всю свою жизнь пребывают в подобном состоянии.
- **Желтый цвет.** Соответствует состоянию средней осведомленности, напоминающей ваше состояние во время вождения машины. Вам известно ваше окружение, и вы замечаете вещи, оказавшиеся не на месте. Тренируясь, вы можете добиться пребывания в этом состоянии в течение всего вашего рабочего времени.
- **Оранжевый цвет.** Этот цвет соответствует такому уровню осведомленности о потенциальной угрозе, при котором вы начинаете планировать свои защитные действия.
- **Красный цвет.** Соответствует состоянию, когда вы идентифицировали реальную угрозу и берете на себя контроль над ситуацией.

Хотя эти цветовые коды изначально предназначались для обозначения степени готовности к самозащите, их легко можно привязать к компьютерному шпионажу. Итак, хотите ли вы перейти к состоянию желтого цвета в работе с вашим компьютером, чтобы при необходимости обратиться к более высоким уровням защиты?

Если количество ответов «нет» превышает количество ответов «да» и кто-то как раз собирается начать наблюдение за вами, как это ни приискорбно, но он может преуспеть в своем деле. Если вам это не безразлично – немедленно обращайтесь за помощью к специалистам.

Образно говоря, защита от компьютерного шпионажа состоит в поиске золотой середины между пребыванием в блаженном неведении и ношением металлического шлема для предохранения мозга от разрушительного влияния всепроникающих радиоволн.

## Анализ рисков 101

В начале данной главы мы уже цитировали Сунь-Цзы: «Если вы хорошо знаете себя и своего врага, вам не нужно беспокоиться об исходе любого из сотни сражений». Именно к этому сводится задача анализа рисков. Совсем несложно определить наиболее вероятные угрозы, проанализировав слабые места и определив контрмеры, которые могут быть предприняты в целях защиты.

Перед тем как продолжить наше повествование, необходимо разобраться в следующих ключевых терминах:

- **Угроза.** Это нечто, представляющее собой опасность. Основной угрозой, о которой пойдет речь в данной книге, являются шпионы, поскольку они представляют опасность с точки зрения утечки компьютерной информации.
- **Уязвимость.** Подразумевает наличие слабых мест в системе защиты, которыми могут воспользоваться злоумышленники для успешного проведения атаки. Хакеры постоянно занимаются поиском подобных возможностей. К примеру, взломщик может воспользоваться широко известным слабым местом защиты веб-серверов, связанным с переполнением буфера, для получения доступа к файлам корпоративной сети.
- **Контрмеры.** Означают действия, предпринимаемые для предотвращения фактов шпионажа. Примером контрмеры может послужить установка «заплаты», предотвращающей возникновение ошибки переполнения буфера и исключающей возможность проведения хакерской атаки.

Теперь давайте рассмотрим воображаемый пример анализа рисков. Итак, предположим, что ваша тетя Сара придумала рецепт шоколадного пирожного, который выиграл на кулинарном конкурсе главный приз, вызвав зависть кулинаров по всей стране. На смертном одре она сообщила вам рецепт и попросила никогда и никому не раскрывать его ингредиенты. С тех пор вы записали этот рецепт в файл на жестком диске и, несмотря на взятки и угрозы, не стали ни с кем им делиться.

Возможно ли, чтобы правительственные агенты заинтересовались рецептом тетушки Сары? Поскольку в наше время может случиться все, что угодно, не означает ли это, что вам придется достать с антресолей средства самозащиты, нанять вооруженных охранников, установить сканер сетчатки глаза для идентификации людей, подключающихся к вашему компьютеру, и экранировать весь дом, дабы не допустить подслушивания со стороны тайных агентов в черных фургонах, экипированных оборудованием для перехвата фирмы TEMPEST.

Хотя какой-то нечестный агент ЦРУ и может заинтересоваться рецептом тетушки Сары, однако вероятность этого минимальна. Поэтому в данном случае можно смело отбросить угрозу со стороны правительенных агентов и перестать волноваться по поводу сложных средств защиты от государственного шпионажа. Кроме того, вы сможете уволить всех ваших вооруженных охранников, а также выбросить сканер для сетчатки глаза и экранирующее оборудование. (Конечно, ситуация может коренным образом измениться, если настоящее имя вашей тети Сары – Наташа, а у нее на руке имеется небольшая смешная татуировка в виде серпа и молота с тремя буквами КГБ...)

Более реальная угроза в данном случае исходит от вашей невестки Кристины, которая гонялась за этим рецептом много лет. Кристина и ее семья приглашают вас каждый год на День благодарения и Рождество, а когда их детям нечем заняться, вы приглашаете их к себе на работу поиграть в компьютерные игры. Маленький Билли очень смышленый мальчик и хорошо разбирается в компьютерах, и вот во время обеда вы пускаетесь с ним в долгую беседу по поводу уязвимых мест в системе безопасности Microsoft. Вы никогда по-настоящему не доверяли Кристине после того гадкого инцидента со столовым серебром тетушки Сары. Таким образом, вам известен источник угрозы и ваши уязвимые места. Как же вы должны действовать?

Если вы думаете, что мама Билли может поручить ему поиск рецепта тети Сары на вашем компьютере, значит, вы определили наиболее вероятную угрозу. Зная, что Билли хорошо разбирается в операционных системах Microsoft, вы установили игры на компьютер под управлением Windows XP, сохранив рецепт в зашифрованном виде на своем мобильном компьютере под управлением Linux и заперев его в тумбочке в спальне. В данном случае можно говорить о том, что вы выявили собственные слабые места и приняли адекватные контрмеры. (Данная книга целиком посвящена поиску слабых мест в защите систем и применению эффективных контрмер.)

Существуют различные методики выполнения анализа рисков. Кто-то использует математические модели, связывая числовые значения с различными видами и продолжительностью действия рисков. Теория вероятностей поможет вам определить область самых высоких рисков и принять наиболее эффективные меры защиты.

## Пять шагов анализа рисков

Анализ рисков можно обсуждать достаточно долго, однако, поскольку данная книга посвящена в первую очередь компьютерному шпионажу, мы приведем краткую модель анализа рисков, состоящую всего из пяти шагов, которая должна помочь вам в проведении эффективного анализа компьютерных рисков.

Мы поочередно изучим каждый шаг, а затем рассмотрим его реализацию применительно к двум фиктивным компаниям, находящимся в различных условиях:

- к корпорации e4bics, высокотехнологичной компании, занимающейся разработкой протокола передачи голосовых данных через Интернет (VoIP);
- к общественной организации «No More Violence» по защите прав женщин, подвергшихся актам насилия.

### ОПРЕДЕЛИТЕ, К КАКОЙ ИНФОРМАЦИИ МОЖЕТ БЫТЬ ПРОЯВЛЕН ИНТЕРЕС

Для начала подумайте, что на вашем компьютере может представлять ценность для потенциального шпиона. Это может быть информация, хранимая на вашем жестком диске (либо другом цифровом носителе информации) либо данные, передаваемые между компьютерами через Интернет или по локальной сети. Хотя некоторые экономисты утверждают, что оценить в денежном эквиваленте можно все, что угодно, ценность в данном случае необязательно сводится к конкретной сумме. Конечно такая информация, как, например, сведения по кредитным карточкам либо финансовые секреты компаний, имеет четко выраженный денежный эквивалент, но иногда подсчитать стоимость информации бывает достаточно сложно. Ведь речь может идти об уликах, которые в случае разглашения приведут вас в тюрьму или же разрушат отношения с определенными людьми. Попробуем проанализировать ситуацию для двух наших фиктивных организаций:

- Корпорация e4bics только что закончила работу над новым коммуникационным сервером, предназначенным для работы с голосовыми и мультимедийными данными. Разработанное ими программное и аппаратное обеспечение превосходит по своим показателям все имеющиеся аналоги как в плане производительности, так и в плане цены. Официальные бизнес-планы утверждены на шесть месяцев вперед, однако слухи о новом продукте продолжают будоражить рынок. Таким образом, любая информация, касающаяся новых разработок, представляет очевидный интерес для определенных субъектов.
- Для того чтобы систематизировать свою деятельность, организация «No More Violence» начала использовать компьютерную

базу данных для хранения сведений о женщинах, которым оказывается поддержка со стороны организации. Одна из выполняемых организацией миссий заключается в предоставлении временных безопасных мест проживания для женщин, подвергшихся насилию со стороны своих мужей. Разумеется, в базу данных заносятся имена и адреса этих женщин и другая личная информация. Все эти данные являются засекреченными, поскольку их раскрытие может угрожать жизни и здоровью женщин, и поэтому они представляют собой ценность, которую нельзя выразить в денежном эквиваленте.

## **ПОДУМАЙТЕ, КОГО МОЖЕТ ЗАИНТЕРЕСОВАТЬ ЭТА ИНФОРМАЦИЯ**

Теперь вы должны решить, кто может быть заинтересован в получении информации, представляющей собой определенную ценность. В начале данной главы мы привели довольно длинный список категорий лиц, подходящих на роль потенциальных шпионов, и на его основе вы можете обозначить круг подозреваемых. Постарайтесь выявить наиболее вероятного противника, а не просто потенциальных злоумышленников, – таким образом, вы направите вашу энергию в правильное русло, на защиту от *реальной опасности*, а не от того, что *могло бы* когда-нибудь случиться.

- В случае с компанией e4bics любые мелкие и крупные конкуренты заинтересованы в получении информации по новой технологии. Причем это касается как американских, так и зарубежных предпринимателей. К руководству компании неоднократно обращались представители других крупных корпораций, предлагая свое сотрудничество в будущем проекте, однако одностороннее решение о неразглашении в отношении конкурентов соблюдалось самым тщательным образом.
- Бывшим партнерам женщин, поддерживаемых организацией «No More Violence», запрещено приближаться к своим жертвам. Естественно, обуреваемые жаждой насилия либо чувством мести, эти мужчины хотят найти своих бывших жен или сожительниц.

## **РЕШИТЕ, НАСКОЛЬКО ВАШИ ВРАГИ ЗАИНТЕРЕСОВАНЫ В ДАННОЙ ИНФОРМАЦИИ И КАК ОНИ МОГУТ ПОЛУЧИТЬ К НЕЙ ДОСТУП**

Предположим, что ваши враги знают либо подозревают, что интересующая их информация размещена на вашем компьютере. Итак, насколько они нуждаются в этой информации и каким образом могут получить к ней доступ? Отвечая на этот вопрос, поразмыслите над мерами безопасности, которые вы применяете, и о том, насколько эффективными они окажутся

в плане остановки либо задержки вашего противника. Опять-таки, не забывайте отсеять наименее вероятные способы атаки – поскольку объять необъятное просто невозможно, в первую очередь следует сосредоточиться на реальных угрозах.

- Так как новый продукт компании e4bics может существенно повлиять на сложившуюся на рынке ситуацию, компания является весьма вероятным кандидатом на роль жертвы промышленного шпионажа. Главный инженер компании J.D., ранее специализировавшийся на проверке надежности систем защиты для ВВС США, составил длинный перечень возможных способов выведения конкурирующими фирмами коммерческих секретов корпорации e4bics, среди которых: извлечение из мусорных корзин не уничтоженных своевременно конфиденциальных бумаг, использование приемов социотехники, проникновение в офисы в нерабочее время и поиск уязвимых мест в защите компьютерной сети.
- Одна из женщин по имени Сью, которая была взята на попечительство организацией «No More Violence», работает сетевым администратором, имея глубокие знания основ безопасности. В разговоре с руководством Сью обратила внимание на возможность проникновения в офис и кражи файлов базы данных либо целого компьютера. Кроме того, поскольку настольный компьютер под управлением Windows XP подключен к Интернету с помощью кабельного модема, шпионы могут применить способ удаленного проникновения и доступа к базе данных. Руководитель отдела располагает сведениями о том, что бывший муж одной из женщин обвинялся в краже со взломом, а бывший приятель другой женщины шутки ради занимался взломом сайтов электронной коммерции. База данных организации была создана в Access и защищена встроенной системой защиты с помощью паролей. Как опытный администратор, Сью указала на уязвимые места в системе защиты Access и рассказала о собственном опыте подбора потерянных паролей к защищенной базе данных, который занял несколько секунд при помощи свободно распространяемой хакерской программы.

## УЧТИТЕ МАКСИМАЛЬНЫЙ УРОН, КОТОРЫЙ МОЖЕТ НАНЕСТИ КРАЖА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Представьте наихудший вариант развития событий. Ваши враги умудрились украсть конфиденциальную информацию. Каковы вероятные последствия? Попытайтесь учесть все детали вашего настоящего и будущего положения.

- В случае с e4bics все зависит от того, какая именно информация была похищена. Если конкурентам стали известны данные по плану продаж, они могут подстроиться под расчетный бюджет, дабы извлечь выгоду для себя. В случае раскрытия бизнес-планов, конкуренты могут разработать встречную стратегию. Если же конкуренты выкрадут технические данные по новым разработкам, e4bics потеряет часть, если не все свои конкурентные преимущества. В худшем случае компания со всеми своими сотрудниками может оказаться на бирже труда.
- Наихудший сценарий развития событий для организации «No More Violence» очень прост. Если база данных с именами и адресами женщин попадет к «заинтересованным» лицам, это может угрожать безопасности и даже жизни этих женщин.

## ОПРЕДЕЛИТЕ СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ И СТОИМОСТЬ ЕГО РЕАЛИЗАЦИИ

Итак, вы определили, что может представлять ценность для потенциальных шпионов, кто может выступать в роли шпионов и возможные последствия разглашения украденной ими информации. Вам осталось только собрать все имеющиеся факты воедино и составить план по защите данной информации.

Поскольку ваш бюджет не резиновый, вам необходимо принять разумное решение в отношении необходимого уровня защиты информации. Не стоит в этом случае исходить только из стоимости затрат на внедрение тех или иных мер предосторожности. Помните также о том, что существует обратная зависимость между уровнем безопасности компьютерной системы и удобством ее использования. Как правило, повышение уровня защиты затрудняет выполнение ежедневных рабочих обязанностей пользователей, что выливается для компании в дополнительные затраты, которые можно оценить в денежном эквиваленте – например, в понижении эффективности труда.

- J.D. хорошо представляет объем работ, которые необходимо выполнить для обеспечения информационной безопасности компании e4bics. Он первым провел анализ рисков и определил лазейки, которыми могут воспользоваться потенциальные шпионы. Затем он выступил с планом, содержащим серию контрмер, призванных защитить слабые места системы. В конце концов он разработал строгую политику безопасности для защиты информации от физического либо компьютерного проникновения извне. Генеральный директор и учредители согласились с необходимостью защиты информации и утвердили план и бюджет на поддержку политики безопасности, предложенной J.D. (В реальной жизни, как правило, вам придется хорошо постараться, чтобы убедить ваше руководство в необходимости принятия должных мер, но, поскольку мы рассуждаем теоретически, будем считать, что все закончилось благополучно.)

- После разговора с полицейским офицером и Сью, руководитель «No More Violence» запланировал покупку новых замков и системы видеонаблюдения для защиты от физического проникновения в офис организации. Для защиты компьютерной сети от вторжения извне через Интернет был приобретен блок маршрутизатора (он преобразует сетевые адреса и предоставляет прозрачный доступ в Интернет с вашей стороны) и установлены все доступные пакеты обновлений на используемую операционную систему Windows. И наконец, для защиты базы данных была использована популярная и надежная утилита шифрования PGP (Pretty Good Privacy). Поскольку «No More Violence» располагает весьма ограниченным бюджетом, а ее сотрудники не обладают глубокими техническими знаниями, вышеперечисленные меры безопасности наилучшим образом подходят для нужд организации как в плане стоимости, так и в плане простоты, поскольку они не затрудняют работу с системой.

## Заключение

Мы надеемся, что, прочтя данную главу, вы научились более ясно представлять себе потенциальных противников (шпионов), учитывать имеющиеся в вашем распоряжении средства защиты и оценивать возможные риски от последствий компьютерного шпионажа.

Далее мы расскажем вам о различных стратегиях, применяемых шпионами для получения доступа к информации. После того, как вы прочтете о существующих шпионских стратегиях, попробуйте поставить себя на место шпиона и представить, насколько эффективными могут оказаться атаки, направленные против вас лично, вашего бизнеса либо организации. При этом всегда следует разделять атаки вероятные и возможные. По отношению к вам возможно применение любой тактики, о которой рассказывается в данной книге, однако более или менее вероятными в вашем случае являются лишь некоторые из них.

Поскольку почти каждый день обнаруживаются все новые уязвимые места в защите компьютерных систем, которые не сразу становятся известны широкой общественности, создать абсолютно защищенный компьютер невозможно в принципе. Перефразируя одну из старых поговорок, скажем, что полностью защищенным можно назвать компьютер, залианный бетоном и погребенный под толщей земли, – но и в этом случае нельзя дать стопроцентную гарантию его безопасности.

Ваша задача заключается в том, чтобы свести риск компьютерного шпионажа к минимуму. Вы не можете быть на 100% уверены в защищенности вашего компьютера от проникновения шпионов, но вы можете усложнить им работу. В этом случае денежные и временные затраты на извлечение информации могут себя и не окупить, вынудив шпионов подыскать себе другие цели.

## Глава 2

# Шпионаж и закон

«Я сражался с законом, но закон победил».

Бобби Фуллер, The Crickets и другие не менее знаменитые группы

## Законы о шпионаже

Помимо самой тактики компьютерного шпионажа и рекомендуемых контрмер следует учитывать правовую сторону дела. В данной главе будут рассмотрены основные законодательные акты, имеющие отношение к компьютерному наблюдению. Некоторые обсуждаемые здесь вопросы могут показаться вам менее интересными, чем разделы, посвященные шпионской тактике (и тактике противодействия лицам, шпионящим за вами), однако эти юридические сведения нужны для того, чтобы вы могли сориентироваться в следующих ситуациях:

- Если вы считаете себя жертвой компьютерного шпионажа в личном или деловом плане, вам необходимо обратиться в правоохранительную организацию, которая во главе с прокурором обязана заняться расследованием вашего дела и определить, является ли данный факт правонарушения уголовно наказуемым. Базовые знания по законодательным актам, связанным со шпионажем, и в частности по компьютерным преступлениям, помогут вам при работе с окружным прокурором (либо частным поверенным по гражданским делам).
- Если вы полагаете, что по реальным или вымышленным причинам вы оказались под наблюдением у правоохранительных органов, вам необходимо ознакомиться с законами, определяющими их права на подобные действия. Это поможет вам отстоять свои права в случае незаконного шпионажа за вами.
- Если вы работаете в правоохранительных органах, вам необходимо правильно подготовить операцию по компьютерному наблюдению, поскольку, с одной стороны, судьи не слишком благосклонно смотрят на полицейских, которые не хотят играть по правилам; а коллеги-полицейские не хотят видеть, как плохие парни ускользают от правосудия только из-за того, что при сборе улик не были соблюдены все формальности.

- Если вы – шпион или же имеете сильное желание стать им, одумайтесь: в случае поимки вам грозят немалые денежные штрафы и перспектива скоротать лучшие годы жизни за решеткой. Если же вы все-таки предпочитаете преступную жизнь, сейчас самое время позаботиться о хорошем адвокате, знающем некоторые спорные статьи уголовного кодекса, на случай раскрытия ваших шпионских планов.

Цитируя популярный в группе новостей USENET акроним IANAL (I am not a lawyer – я не адвокат), напоминаем: данная глава не заменит вам консультацию юриста. Если вы оказались так или иначе связаны с компьютерным шпионажем, то ли в качестве жертвы, то ли злоумышленника, обращайтесь за консультацией к специалисту. Это может быть юридический советник в вашей фирме, окружной прокурор, если вы работаете в полиции, или же частный адвокат (вы вряд ли сможете найти в «Желтых страницах» много «адвокатов по делам, связанным с компьютерным шпионажем», поэтому ищите хотя бы специалистов в области компьютерных технологий и коммерческих секретов).

Не забывая вышесказанное, рассмотрим основные законы, запрещающие компьютерный шпионаж, и технику их применения к пойманным правонарушителям.

## **Закон об уличной безопасности 1968 года (часть III – телефонное прослушивание)**

Какие законы действовали в докомпьютерную эру в 1968 году и как могла быть связана безопасность улиц с компьютерным шпионажем, спросите вы. После террористических актов, жертвами которых стали Роберт Кеннеди и Мартин Лютер Кинг-младший, Закон об уличной безопасности (Omnibus Crime Control and Safe Streets Act) стал ответом на эти преступления, призванным отобрать оружие у несовершеннолетних, лиц с криминальным прошлым либо умственно неполноценных. В этом законе (в его третьей части, если быть более точным) есть параграф, посвященный прослушиванию телефонных разговоров. На этот параграф часто ссылаются как на часть III или Закон о прослушивании либо, более официально, том 18 Свода Законов Соединенных Штатов (U.S.C.), статьи 2510-2521.

Под прослушиванием телефонных разговоров понимают тайное подключение подслушивающих и записывающих устройств к линиям связи (сегодня мы говорим о каналах передачи данных, но в то время речь шла исключительно о телефонных линиях). В соответствии с этим документом правоохранительным органам предоставляются права на прослушивание линий связи в определенных ситуациях. Закон также запрещает несанкционированное выполнение электронного прослушивания. До принятия этого закона прослушивание телефонных разговоров не было запрещено юридически, то есть за него никто не мог нести ответственности.

В 1967 году в деле Катца против правительства Соединенных Штатов Верховный Суд принял решение о незаконности использования ФБР электронных устройств для прослушивания и записи его телефонных разговоров без соответствующего ордера, поскольку необоснованная слежка и запись телефонных разговоров граждан запрещена в соответствии с четвертой поправкой к Конституции. Это дело послужило основой для формулировки общего критерия законности наблюдения со стороны правительства, превратившегося впоследствии в часть III Закона о прослушивании.

Основная идея данного закона заключается в том, что без четкой регламентации политики в отношении наблюдения за гражданами со стороны правительства нарушаются конституционные права граждан на неприкосновенность частной жизни; с другой стороны, электронное прослушивание может быть вынужденным, поскольку «организованные преступники активно используют линии связи и личное общение в своих преступных целях». Данный закон был призван упорядочить правила использования подслушивающих устройств с учетом гражданских прав, дарованных Конституцией.

В части III Закона подробно описывается, в каких случаях может выполняться прослушивание телефонных переговоров и других линий связи. К примеру, ФБР не имеет права прослушивать ваши телефонные переговоры только потому, что вы не оплатили штрафной талон за неправильную парковку. В соответствии с буквой Закона, прослушивание телефонных разговоров может быть санкционировано только в случае тяжких преступлений: взяточничества, похищения детей, краж со взломом, убийств, подделки ценных бумаг и денежных банкнот, мошенничества, продажи наркотиков или планирования заговоров. (Следует, однако, отметить, что с момента принятия этого закона список преступлений, при расследовании которых может осуществляться прослушивание линий связи, увеличился с 26 до более чем 100 пунктов, – в него были включены такие «тяжкие» преступления, как сообщение неверных данных для получения студентами беспроцентных займов.)

Благодаря появлению данного закона, были регламентированы полномочия правоохранительных органов, в соответствии с которыми полиция не имеет права прослушивать телефонные разговоры всех, кого захочет. Чтобы прослушивать на законных основаниях, вначале требуется получить судебную санкцию. Подслушивание телефонных разговоров всегда должно являться крайней мерой, и доказательства в виде записей переговоров рассматриваются судом только после того, как все альтернативные улики оказываются исчерпанными. Кроме того, представители правоохранительных органов обязаны аргументировать необходимость прослушивания, то есть привести суду какие-либо доказательства для получения разрешения на прослушивание разговоров подозреваемых. Иными словами, полицейским недостаточно просто прийти к судье и сказать: «Дайте нам разрешение, мы хотим проследить за таким-то человеком».

Хотя изначально термин «прослушивание линий связи» касался телефонов, в настоящее время под линиями связи могут подразумеваться

любые каналы передачи данных. К примеру, если полиция расследует дело, в котором вы каким-либо образом замешаны, по этой же статье полицейским может быть выдан ордер на осуществление перехвата вашей электронной переписки. Если же шпионите вы и используете, к примеру, программу перехвата сетевых пакетов для сбора передаваемой по сети информации, учтите, что тем самым вы нарушаете несколько федеральных законов, касающихся прослушивания линий связи, включая Закон о прослушивании.

## Рабочие инструменты: самописцы и отслеживающие устройства

Задолго до того как в нашей жизни появился Интернет, правоохранительные органы уже использовали *самописцы* и *автоматические определители номеров* для прослушивания телефонных линий. Самописцы предназначались для фиксации номеров телефонов для исходящих звонков, а автоматические определители номера – для определения номеров входящих звонков. Ни один из этих приборов не позволял прослушивать сами переговоры – речь шла исключительно о получении информации о номерах телефонов абонентов.

Хотя изначально данная технология использовалась для регистрации телефонных звонков, теперь она находит применение при общении через сеть Интернет, что оговорено в недавно принятом Патриотическом Акте США (USA Patriotic Act). В случае компьютерного подслушивания на маршрутизатор устанавливается специальное программное обеспечение, позволяющее сохранять заголовки электронных сообщений (за исключением строки «тема»), IP-адреса и порты исходящих и входящих сообщений, а также запрошенные в Интернете страницы. Задокументировано может быть практически все, что не связано непосредственно с содержанием письма.

Использование самописцев и отслеживающих устройств требует наличия судебного ордера, для получения которого, однако, правоохранительные органы не обязаны сообщать возможную причину наблюдения, что облегчает процедуру их применения.

Статьи Свода Законов об использовании вышеперечисленных устройств размещены в сети Интернет по следующему адресу:

[www.law.cornell.edu/uscode/18/3121.html](http://www.law.cornell.edu/uscode/18/3121.html)

Нарушение данной статьи ведет к уголовной ответственности и может караться максимум пятью годами лишения свободы и штрафом в размере 10 тысяч долларов.



За более детальной информацией по тематике, связанной с расследованиями компьютерных преступлений и по данной статье Закона в частности, обращайтесь по адресу: [www.usdoj.gov/criminal/cybercrime/usamarch2001\\_2.htm](http://www.usdoj.gov/criminal/cybercrime/usamarch2001_2.htm).

## Закон об иностранной разведке 1978 года

Как вы понимаете, шпионы не обладают необходимыми им для «работы» правами, особенно те из них, которые работают на иностранную разведку, ориентированную на кражу государственных секретов. Однако, поскольку США является демократическим государством, придерживающимся норм Конституции, существует множество малоизвестных юридических документов, касающихся шпионажа и других нечестных действий со стороны иностранных властей.

В 1978 году Конгресс принял Закон об иностранной разведке (Foreign Intelligence Surveillance Act, сокращенно FISA), смотри том 50 USC, статьи 1801-1811. Целью данного закона является разделение уголовных преступлений и разведывательной деятельности, направленной против США, в особенности случаев шпионажа со стороны иностранных организаций. Изначально этот закон касался лишь электронного наблюдения, однако в 90-х годах в него были добавлены статьи о скрытом физическом наблюдении в ходе расследования, а также правила использования самописцев и отслеживающих устройств для каналов передачи данных.

В Законе об иностранной разведке под термином «иностранный разведка» понимается получение любой информации, разглашение которой угрожает способностям Соединенных Штатов защитить себя в случае:

- возможных агрессивных действий со стороны зарубежных организаций либо их агентов;
- саботажа или терроризма со стороны зарубежных организаций или их агентов;
- нелегальной разведывательной деятельности со стороны зарубежных организаций или их агентов.

Особенно часто этот закон применяется в делах, связанных с угрозой национальной системе обороны и безопасности либо связанных с проведением зарубежных операций, инициированных Соединенными Штатами Америки.

В соответствии с четвертой поправкой к Конституции для получения ордера на обыск офицеры полиции должны сообщить о подозрении в совершенном преступлении либо о вероятности совершения такового. В соответствии с Законом об иностранной разведке наблюдение может быть санкционировано и в том случае, если данное лицо подозревается в сотрудничестве с зарубежными организациями, даже если никакого преступления не совершилось и не планировалось. Причем действие этого Закона распространяется не только на представителей других государств, –

даже граждане США, подозреваемые в участии в разведывательной деятельности в пользу других государств, будут отвечать в соответствии с его статьями.

Хотя Закон об иностранной разведке регламентирует сбор информации для расследования деятельности иностранных разведслужб, улики, собранные для доказательства преступлений, ответственность за которые предусмотрена статьями данного закона, могут использоваться и в криминальных процессах. При этом необходимо учитывать требование *минимального объема* разглашаемой информации. Минимизация разглашаемой информации подразумевает передачу следователям и офицерам полиции, занимающимся расследованием уголовных дел, только той информации, которая непосредственно связана с их криминальными расследованиями, и неразглашение данных, касающихся деятельности иностранных спецслужб, что объясняется более широкими полномочиями в плане наблюдения, предоставляемыми Законом об иностранной разведке. Однако, поскольку нередко расследуемые правонарушения подпадают как под действие Закона об иностранной разведке, так и под действие других статей Свода Законов, возникают так называемые информационные стены, когда официальные лица, не задействованные в криминальном расследовании, просматривают информацию, подпадающую под статью Закона об иностранной разведке, а затем передают правоохранительным органам, расследующим уголовные преступления, только те материалы, которые имеют непосредственное отношение к уголовным делам.

Согласно Закону об иностранной разведке был создан специальный судебный орган – Суд по делам об иностранной разведке (FISC – Foreign Intelligence Surveillance Court), в составе семи федеральных судей. Суд по делам об иностранной разведке собирается дважды в месяц, чтобы рассмотреть правительственные запросы на проведение электронного наблюдения с целью сбора информации о деятельности иностранной разведки. (Все запросы на получение санкций в соответствии с Законом об иностранной разведке, независимо от того, из какого управления пришел запрос (не исключая ЦРУ), обязательно должны пройти рассмотрение в Министерстве юстиции. При этом каждый запрос по Закону об иностранной разведке должен быть лично одобрен генеральным прокурором.)

Суд по делам об иностранной разведке – совершенно секретный орган. Это связано с тем, что многие документы по рассматриваемым делам, как правило, закрыты и не доступны даже лицам, обладающим полномочиями для расследования в соответствии с Законом об иностранной разведке. Существует также Апелляционный суд по делам об иностранной разведке (Foreign Intelligence Surveillance Court of Appeals), рассматривающий спорные вопросы в деятельности FISC. Впервые Апелляционный суд по делам об иностранной разведке собирался после ввода в действие Закона об иностранной разведке в сентябре 2002 года для рассмотрения запроса Министерства юстиции о минимальном объеме разглашаемой информации.

## Тактика: CALEA

Аббревиатура CALEA расшифровывается как Communication Assistance for Law Enforcement Act – Закон о сотрудничестве компаний, предоставляющих услуги связи, с правоохранительными органами, датированный 1994 годом (Общие законы 103-414, Свод Законов США, том 47, статьи 1001-1010). Хотя данный закон не связан непосредственно с компьютерным шпионажем, мы не могли упустить его из виду, поскольку в нем присутствует статья об электронном наблюдении.

В Законе о прослушивании линий связи говорилось о том, что телекоммуникационные компании должны «всячески способствовать работе правоохранительных органов по электронному перехвату информации». Однако вопрос о том, обязаны ли подобные компании изначально разрабатывать свои каналы передачи данных таким образом, чтобы они не мешали выполнению электронной слежки, никогда не поднимался.

Закон о сотрудничестве телекоммуникационных компаний с правоохранительными органами вносит поправки в Закон о защите электронных систем связи, требуя, чтобы оборудование, используемое телекоммуникационными компаниями, было совместимо со средствами электронного шпионажа, используемыми правительством. Таким образом, если вы раньше могли видеть на компьютерных комплектующих надпись «Windows-compatible», что означало совместимость с ОС Microsoft Windows, то теперь к компаниям предъявлено требование о совместимости их телекоммуникационного оборудования со средствами электронного наблюдения.

Одно из подразделений ФБР, именуемое CIS (CALEA Implementation Section), то есть подразделение, ответственное за соблюдение Закона о сотрудничестве с правоохранительными органами, сейчас как раз и занимается воплощением в жизнь положений данного закона. К его задачам относятся «создание телекоммуникационных систем, обеспечивающих эффективный сбор информации, и наблюдение для таких приоритетных областей, как судебные расследования и разведывательная деятельность». Итак, ФБР «рассматривает» вопросы совместимости аппаратного обеспечения для прослушивания телефонных разговоров. Но существуют подозрения, что ФБР также ведет переговоры с другими организациями по разработке стандартов о встраивании средств электронного наблюдения в DSL – цифровые абонентские линии, протокол IP-телефонии и беспроводные технологии связи.

Внедрение Закона о сотрудничестве телекоммуникационных компаний с правоохранительными органами США обходится недешево. По самым приблизительным оценкам, за пять лет телекоммуникационные компании в Соединенных Штатах потратили от полумиллиарда до 2,7 миллиарда долларов на приведение своего оборудования в соответствие с требованиями CALEA. Посему неудивительно, что звонок с телефонного автомата в США теперь стоит больше двадцати пяти центов.

Естественно, компании, предоставляющие услуги связи, были отнюдь не в восторге от принятия этого закона и делали все, что в их силах, чтобы опровергнуть его целесообразность. Однако, в конце концов, в июне 2002 года Федеральная комиссия по средствам связи (FCC) потребовала от телекоммуникационных компаний обязательного приведения своего оборудования в соответствие со спецификациями ФБР. Другим промышленным и частным организациям данная директива FCC была направлена еще за три года до этого, однако из-за судебных разбирательств она не соблюдалась. Теперь же, после событий 11 сентября, когда никто не хочет быть обвиненным в антиправительственной направленности либо отсутствии патриотизма, никаких организованных протестов со стороны телекоммуникационных компаний не наблюдается.

Более подробную информацию по Закону о сотрудничестве телекоммуникационных компаний с правоохранительными органами вы сможете прочесть по адресу [www.askcalea.net](http://www.askcalea.net); полный текст самого закона можно найти в сети Интернет по адресу [www.law.cornell.edu/uscode/18/2522.html](http://www.law.cornell.edu/uscode/18/2522.html).



Полный текст Закона об иностранной разведке вы можете найти в сети Интернет по адресу:  
[www.law.cornell.edu/uscode/50/ch36.html](http://www.law.cornell.edu/uscode/50/ch36.html).

## Закон о защите электронных систем связи 1986 года

В 1986 году Конгресс, удививший всех своей проницательностью, расширил действие третьей части Закона о прослушивании линий связи на электронный обмен информацией, включая услуги пейджерных операторов, электронную почту, сотовые телефоны, частные радиочастоты и компьютерную передачу данных. Расширенной редакции закона было присвоено название «Закон о защите электронных систем связи» (английская аббревиатура ECPA – Electronic Communications Privacy Act).

Основные положения закона звучат следующим образом:

- не только правительство или правоохранительные органы, но и частные лица не имеют права заниматься несанкционированным наблюдением, прослушиванием или перехватом цифровой или аналоговой информации, передаваемой по линиям связи;

- неприкосновенность всех видов частного электронного общения, включая передачу текстовой и графической информации между отдельными лицами, гарантируется законом;
- неприкосновенность электронной передачи информации касается не только перехвата сообщений, но и несанкционированного доступа к электронным носителям информации.

В Законе о защите электронных систем связи оговариваются дополнительные ситуации, помимо перечисленных в третьей части Закона о прослушивании линий связи, в которых для наблюдения за электронными коммуникациями не требуется наличия судебного ордера:

- Частные лица могут выполнять электронное наблюдение за своим компьютером самостоятельно или же привлекать на помощь правоохранительные органы, если их компьютер подвергся незаконной атаке со стороны взломщиков. К примеру, если на ваш сервер проник шпион и завел себе ящик электронной почты, чтобы вести переписку с другими правонарушителями, вы можете обратиться к правоохранительным органам с просьбой о проведении наблюдения за его входящей и исходящей почтой с целью сбора доказательств против взломщика-шпиона.
- Если при входе в систему пользователи предупреждаются о том, что данная система принадлежит частному владельцу, то вход в систему подразумевает согласие пользователя на наблюдение за ним; согласие в данном случае распространяется на любые виды электронного наблюдения.
- Последнее исключение позволяет частным лицам следить за работой пользователей в системе для недопущения нанесения ущерба в результате некорректного использования системы, включая мошенничество либо несанкционированный запуск тех или иных служб. Данное исключение действует лишь в том случае, если наблюдение действительно проводится частным лицом, владеющим данной техникой, а не государственной организацией. (Во многих случаях, если одна и более общающихся между собой сторон соглашаются на выполнение мониторинга, он считается легитимным.)

Закон о защите электронных систем связи касается не только перехвата электронных сообщений в реальном времени, но и регламентирует доступ к хранимой информации (часть II Закона о защите электронных систем связи). Эта часть (Закон о хранимой информации – Stored Communications Act) запрещает сторонним лицам получать доступ к записям телефонных переговоров или архивам электронной переписки, к примеру, без соответствующего судебного ордера (для этого правоохранительным органам необходимо иметь ордер на обыск, который значительно легче получить, чем ордер на прослушивание электронных линий связи). Несоблюдение Закона о защите электронных систем связи ведет к гражданской и уголовной ответственности, в зависимости от рода преступления.

Как и в случае с перехватом электронного сообщения, существует ряд исключений, в которых изучение электронных архивов не требует судебной санкции. К этим исключениям относятся:

- **Подразумеваемое согласие.** Если провайдер или работодатель предупреждает о своей политике, допускающей просмотр частных информационных архивов, пользователи системы либо служащие компаний при приеме на работу автоматически соглашаются на мониторинг своей деятельности.
- **Доступ через информационного провайдера.** Провайдер электронных служб связи имеет законное право на просмотр любой информации, сохраненной с использованием предоставляемой им службы.

Что касается компьютерного наблюдения, то некоторые юристы полагают, что формулировка Закона о хранимой информации предоставляет работодателям большие права на доступ к такой информации, как, например, архивы электронной почты, чем на перехват электронных сообщений в реальном времени.

### **Тактика: статистика прослушивания линий связи**

Насмотревшись по телевизору новостей и боевиков, можно подумать, что прослушивание линий связи происходит так же часто, как, например, обмен MP3-файлами без соблюдения авторских прав. В действительности дело обстоит не совсем так. Например, за 2001 год на всей территории Соединенных Штатов было санкционировано всего около полутора тысяч прослушиваний.

В одном из положений Закона о прослушивании линий связи говорится, что Административное Управление судов США обязано публиковать ежегодный отчет о количестве операций по прослушиванию линий связи. Этот отчет выходит в свет весной и содержит немало интересной информации.

В качестве примера приведем общее число санкционированных операций по прослушиванию линий связи. Напоминаем, что ордеры на прослушивание линий связи выдаются для наблюдения за телефонами, пейджерами, факсами, компьютерами и любыми другими средствами электронного общения.

Итак, это число составило:

в 2001 году – 1491;

2000 году – 1190;

1999 году – 1350;

1998 году – 1329;

1997 году – 1186.

Судьи удовлетворили все запросы на проведение операций по прослушиванию (случаи отклонения судьями каких-либо запросов происходят очень редко). Чаще всего операции по прослушиванию линий связи (в 78% случаев) были связаны с контрабандой и торговлей наркотиками.

Более 23 миллионов телефонных разговоров было перехвачено в 2001 году, что повлекло за собой 3683 ареста. Только пятая часть этих арестов завершилась вынесением обвинительного вердикта, что служит доказательством недостаточной весомости подобных улик перед судом присяжных.

В 16 случаях перехвата данных, санкционированных в 2001 году, которые подпадали под местную юрисдикцию либо юрисдикцию штата, полиция столкнулась с шифрованием данных (что интересно, федералы не сообщали о подобных случаях). Ни в одном из этих дел не упоминается о том, что шифрование данных помешало полицейским узнать содержимое перехваченных сообщений. Означает ли это, что правоохранительные органы могут взламывать PGP (свободно распространяемую и, де-факто, надежную утилиту шифрования)? Вряд ли. Скорее «плохие парни» использовали неустойчивые алгоритмы шифрования, легко угадываемые пароли или имели дурную привычку писать пароли на стикерах и клеить их на монитор.

Отчеты о проведенных операциях по прослушиванию очень похожи на захватывающие шпионские романы. Если вы фанат таких романов – можете прочитать их по адресу [www.uscourts.gov/wiretap.html](http://www.uscourts.gov/wiretap.html).

Итак, весьма прогрессивный для 1986 года закон, несмотря на произошедшую за последние 16 лет техническую революцию, был последним существенным нововведением в стандарты неприкосновенности частной жизни в плане электронного наблюдения.



Закон о защите электронных систем связи можно прочесть по адресу [www.law.cornell.edu/uscode/18/pICh119.html](http://www.law.cornell.edu/uscode/18/pICh119.html). Текст Закона о хранимой информации размещен по адресу [www.law.cornell.edu/uscode/18/pICh121.html](http://www.law.cornell.edu/uscode/18/pICh121.html).

## Закон о компьютерном мошенничестве и злоупотреблениях 1986 года

Закон об использовании фальсифицированных устройств доступа, компьютерном мошенничестве и злоупотреблениях (Computer Fraud and Abuse Act – том 18, статья 1030 Свода Законов США) был принят в 1986 году (придя на смену Закону о мошенничестве и злоупотреблении 1984 года).

Этот закон стал, по сути, первым полновесным законом о компьютерных преступлениях, направленным против хакеров. В соответствии с данным законом:

- предусматривается уголовная ответственность за несанкционированный доступ к компьютерам федерального правительства;
- предусматривается уголовная ответственность за несанкционированный доступ к компьютерам, принадлежащим крупным финансовым институтам;
- расследование компьютерных преступлений подпадает под юрисдикцию разведывательных спецслужб (сейчас ведущую роль в этом играет ФБР).

Оригинальный закон использовался всего в нескольких делах, наиболее знаменитым из которых считается дело Роберта Морриса, студента Корнельского университета, чья экспериментальная программа-«червь» вышла из-под контроля и быстро распространилась по сети Интернет. В соответствии с положением данного закона, Моррис был приговорен к трем годам испытательного срока, 400 часам общественно полезных работ на телекоммуникационные компании, штрафу в размере 10 050 долларов и компенсации стоимости затрат на наблюдение за ним.

С 1986 года в этот закон многократно вносились поправки, касающиеся различных нюансов компьютерных преступлений. К примеру, Национальный закон о защите информационной инфраструктуры (National Information Infrastructure Protection Act) расширил употребление понятия «защищенный компьютер» на любой компьютер, подключенный к Интернету.

В соответствии с Законом о компьютерном мошенничестве и злоупотреблениях запрещены следующие действия (любое из них классифицируется как компьютерный шпионаж):

- получение несанкционированного доступа к «защищенному компьютеру» (компьютеру, используемому для внутригосударственных и международных коммерческих контактов);
- несанкционированный доступ к компьютерным системам с последующей передачей секретной правительственный информации;
- компьютерное вымогательство;
- компьютерное мошенничество;
- кража финансовой информации;
- продажа компьютерных паролей с целью повлиять на внутригосударственную торговлю либо сохранность информации на правительственные системах;
- распространение программного кода, способного нанести урон компьютерным системам.

## Разоблачения: Роберт Коноп против компании Hawaiian Airlines

Роберт Коноп работал пилотом в компании Hawaiian Airlines. В 1995 году компания Hawaiian Airlines обсуждала контракты своих пилотов с ассоциацией Air Line Pilots. У Конопа возникло подозрение, что некоторые совершенные в процессе переговоров уступки являются нечестными по отношению к работникам компании, поэтому он открыл в сети Интернет свой веб-сайт с ограниченным доступом, пароли к которому предоставил только некоторым своим коллегам. Все пользователи, просматривающие сайт Конопа, должны были согласиться с перечисленными условиями перед входом в систему. Одним из таких условий являлся запрет на разглашение имеющейся на сайте информации администрации компании Hawaiian Airlines.

Вице-президент компании Джеймс Девис, узнав о существовании этого сайта, убедил имевшего к нему доступ пилота предоставить Девису возможность войти в систему при помощи своей учетной записи и пароля. Девис загрузился под именем пилота 34 раза, согласившись, таким образом, с представленными условиями.

Девис передал сведения о Конопе и размещенную на его сайте информацию президенту компании Hawaiian Airlines и Союзу пилотов. Представитель Союза связался с Конопом и выразил свое недовольство по поводу существования подобного веб-сайта, не раскрывая своих источников информации. Сыграв роль детектива, Коноп вычислил Девиса с помощью системных журналов.

В конце концов, Роберт Коноп подал в суд на компанию Hawaiian Airlines за несанкционированный доступ к своему веб-сайту, что являлось нарушением Закона о прослушивании линий связи и ряда других законов. Окружной суд отклонил это заявление, однако в январе 2001 года Федеральный апелляционный суд девятого созыва взялся за пересмотр дела, полагая, что имевший место просмотр содержимого защищенного веб-сайта без разрешения владельца действительно является нарушением Закона о прослушивании линий связи и Закона о доступе к хранимой информации.

Тем не менее спустя девять месяцев тот же суд неожиданно отозвал свое решение. В августе 2002 суд заявил, что Закон о прослушивании линий связи не нарушался, поскольку его действие касается только перехвата данных, а не доступа к хранимой информации. Однако, по мнению суда, компания Hawaiian Airlines все же нарушила Закон о хранимой информации.

Подробности данного дела и связанные с ним судебные постановления вы можете прочесть в Интернете по адресу [www.ca9.uscourts.gov/ca9/newopinions.nsf/DD51CB5C3834F00F88256C1E0002A94D/\\$file/9955106.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/DD51CB5C3834F00F88256C1E0002A94D/$file/9955106.pdf?openelement).

С точки зрения судебно-исполнительных органов этот закон можно назвать основным орудием против хакеров и компьютерных шпионов. Минимальная ответственность за нарушение статей данного закона оценивается штрафом в размере 5 тысяч долларов. Естественно, эта сумма, как правило, значительно возрастает, особенно в случае нанесения кому-либо морального или физического ущерба, что подразумевает оплату лечения пострадавшего, либо при угрозе национальной безопасности Соединенных Штатов. Максимальное наказание за нарушение Закона о компьютерном мошенничестве и злоупотреблениях может достигать 20 лет тюремного заключения и штрафов в размере 250 000 долларов.



Полный текст Закона о компьютерном мошенничестве и злоупотребленияхсмотрите на сайте [www.law.cornell.edu/uscode/18/1030.html](http://www.law.cornell.edu/uscode/18/1030.html).

## Закон об экономическом шпионаже 1996 года

До 1996 года отсутствовал единый федеральный закон, который бы касался похищения коммерческих секретов. Хотя в законодательстве отдельных штатов присутствовали подобные законодательные акты, однако правительство США не располагало законами, по которым можно было бы судить экономических шпионов. Ситуация изменилась с принятием Закона об экономическом шпионаже (Economic Espionage Act – Свод Законов США, том 18-й, статьи 1831-1839).

Закон содержит два ключевых положения:

- Закон разрешает ФБР вести расследования дел, когда в похищении экономических секретов Соединенных Штатов подозреваются другие государства. Хотя ФБР всегда играло ведущую роль в делах, связанных с иностранным шпионажем, до 1996 года Федеральное Бюро занималось только расследованием преступлений, связанных с угрозой национальной безопасности, не затрагивая случаи экономического шпионажа.
- Закон переопределяет термин «изделия, товары или имущество» в федеральных законах, связанных с воровством, добавляя к нему пункт «экономическая информация, принадлежащая фирме». Такая поправка позволяет расширить область применения многих федеральных законов.

Нарушение Закона об экономическом шпионаже ведет к серьезной ответственности – до 15 лет лишения свободы и 500 000 долларов штрафа для частных лиц или до 10 000 000 долларов штрафа для организаций, уличенных в поддержке актов экономического шпионажа. Следует отметить, что действие данного закона распространяется не только на случаи экономического шпионажа со стороны других государств, но также и на внутригосударственный шпионаж американских компаний, направленный друг против друга.

С момента принятия закона ФБР серьезно взялось контролировать его исполнение, в отличие от некоторых других «бумажных» законов. К примеру, в 1997 году за нарушение данного закона была арестована пара из Флориды, которая занималась прослушиванием и записью телефонных переговоров компании House Newt Gingrich. В результате они были оштрафованы на 500 000 долларов каждый. Всего с момента появления Закона об экономическом шпионаже нарушение статей Закона рассматривалось в более чем 35 судебных разбирательствах, многие из них закончились вынесением суровых обвинительных вердиктов, предусматривающих значительные штрафы и тюремное заключение.



Марк Халлиган, адвокат, специализирующийся по делам, связанным с похищением коммерческих секретов, посвящает свободное время сбору информации по преступлениям, нарушающим Закон о компьютерном шпионаже. Полный текст закона, а также информацию по произведенным арестам и предъявленным обвинениям вы можете прочесть по адресу:

<http://my.execcps.com/~mhalligan/indict.html>.

## Законы штатов

Несмотря на важность федеральных законов, подавляющее большинство дел решается на уровне штатов либо местных управлений. Многие штаты имеют законы, аналогичные федеральным, которые затрагивают вопросы компьютерных преступлений, прослушивания линий связи, и неприкосновенности частной жизни. (Существуют некоторые весьма строгие законы, например Закон о неприкосновенности частной жизни в Калифорнии, который содержит положения, обеспечивающие большую защиту от вмешательства в частную жизнь граждан, чем это предусматривается федеральным Законом о прослушивании.)

Однако область действия законов штата ограничивается гражданскими и криминальными искаами, не выходящими за пределы юрисдикции данного штата. Когда речь заходит о компьютерном шпионаже, который часто бывает связан с удаленным наблюдением из одного штата за другим, правительство штата не может выполнять экстерриториальное преследование, то есть давать ордеры на обыск в другом штате, вызывать в суд и т. д., – в этом случае в действие вступают федеральные законы.

Если было нарушено как законодательство штата, так и федеральное законодательство, прокуроры штатов или местные окружные прокуроры

встречаются с региональным представителем генерального прокурора США и отдельно по каждому делу принимают решение о том, по каким законам судить виновного.

Хотя законодательства разных штатов различаются формулировками и структурой законов, однако меры пресечения в большинстве случаев очень похожи. Практически все законы предусматривают уголовное наказание за несанкционированный доступ и/или использование компьютеров и баз данных, применение компьютера в качестве инструмента мошенничества, совершенные или предполагаемые акты компьютерного саботажа. Если у вас есть немного времени, и при этом вы планируете заняться прослушиванием линий связи либо уже занимались этим и попались в роли шпиона, изучите эти различия (к примеру, в Виргинии только одной из сторон достаточно дать согласие на прослушивание своих переговоров, тогда как в Мэриленде согласие должно быть получено от обеих сторон).



Рассмотрение законодательства отдельных штатов по компьютерному шпионажу выходит за рамки данной книги. Каждый штат имеет свой официальный веб-сайт, на котором, как правило, доступны онлайновые версии законов с возможностью быстрого поиска нужной информации. В качестве альтернативных источников информации можем порекомендовать вам сайт Национального собрания законодательных органов штатов ([www.ncsl.org/programs/lis/CIP/surveillance.htm](http://www.ncsl.org/programs/lis/CIP/surveillance.htm)), на котором собраны законы, связанные с наблюдением и шпионажем, а также сайт Национального института безопасности (<http://nsi.org/Library/Compsec/computerlaw/statelaws.html>), на котором размещены ссылки на законы штатов о компьютерных преступлениях.

## Патриотический Акт 2001 года

В ответ на террористический акт 11 сентября 2001 года президент Буш подписал Патриотический Акт США, вступивший в действие с 26 октября 2001 года. (Английское название закона USA Patriot Act одновременно является акронимом от «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism» – Акт об объединении и усилении Америки средствами, необходимыми для борьбы с терроризмом.) Закон вносит поправки в 15 положений других законов, включая только что рассмотренные нами федеральные законы.

Патриотический Акт США содержит два положения, касающиеся компьютерного шпионажа:

- Закон предоставляет правительству более широкие полномочия на проведение расследований и связанных с ними наблюдений, что вызвало беспокойство многих борцов за права на неприкосновенность частной жизни.

- В соответствии с новым законом предусматриваются более суровые меры наказания за ряд действий, связанных с компьютерным шпионажем.

Такие организации, как Центр демократии и технологий, Организация электронных границ, Союз американских гражданских свобод и Информационный Центр защиты электронной информации, выступили за пересмотр закона в Конгрессе, поскольку многие положения Закона были сформулированы под влиянием эмоциональной атмосферы, царившей в стране после событий 11 сентября. В конечных положениях самого Закона сказано, что многие поправки, касающиеся электронного наблюдения, будут действовать до 31 декабря 2005 года, однако, поскольку выиграть войну против терроризма в течение ближайших трех лет представляется маловероятным, скорее всего, действие закона будет продлено.

Год спустя после подписания данного закона, юридический комитет Палаты представителей обнародовал ответ Министерства юстиции на запрос о пересмотре Патриотического Акта США (с текстом данного письма вы можете ознакомиться по адресу [www.house.gov/judiciary/patriot-responses/101702.pdf](http://www.house.gov/judiciary/patriot-responses/101702.pdf)). Министерство юстиции засекретило большую часть этой информации, после чего многие организации обратились в суд по поводу нарушения Закона о свободе слова в попытке прикрыть некоторые нюансы воплощения Закона в жизнь. Этот Закон навсегда останется спорным, и, скорее всего, возможные будущие террористические атаки, направленные против Соединенных Штатов, вызовут внесение еще больших изменений в законодательство, которые способны привести к еще большим разногласиям.

В следующих параграфах мы обсудим некоторые ключевые изменения, вносимые Патриотическим Актом в различные законы, касающиеся компьютерного шпионажа.



Патриотический Акт США имеет объем более 300 страниц и содержит огромное количество поправок для действующих законов. Обширную аналитику по данному закону вы можете найти в сети Интернет по адресу [www.cdt.org/security/010911response.html](http://www.cdt.org/security/010911response.html).

## Законы о прослушивании линий связи и доступе к хранимой информации

С принятием Патриотического Акта в Закон о прослушивании линий связи и Закон о хранимой информации (рассмотренные в начале данной главы) были внесены важные поправки, связанные с компьютерными преступлениями:

- Кабельные компании должны привести свое оборудование в соответствие с правительственными требованиями в плане возможностях выполнения наблюдения, подобно телефонным компаниям и

провайдерам услуг Интернет. До этого кабельные компании, предоставляющие услуги Интернета, подпадали под другой свод правил, в отличие от телефонных компаний.

- Терроризм и нарушение Закона о компьютерном мошенничестве и злоупотреблениях теперь добавлены в список преступлений, для расследования которых может быть санкционировано прослушивание линий связи.
- Регистраторы входящих/исходящих адресов сообщений теперь могут применяться к трафику в сети Интернет.
- Для получения доступа к голосовой почте теперь достаточно иметь ордер на обыск, а не санкцию на прослушивание линий связи (тем не менее прослушивание сообщений, хранимых на автоответчике, по-прежнему считается перехватом телефонных разговоров, и в этом случае граждане остаются более защищенными в плане неприкасаемости частной жизни).
- Правительство избавило себя от ответственности за перехват без соответствующего ордера по запросу провайдера данных, передаваемых взломщиками и другими правонарушителями.
- В соответствии с поправкой, внесенной в Закон о защите электронных систем связи, ордер на обыск для поиска улик на электронных носителях информации, как, например, архивов электронной почты, выданный судом, имеющим право на расследование подобных преступлений, теперь действителен на всей территории Соединенных Штатов (ранее действие ордера ограничивалось юрисдикцией данного суда).

## Закон об иностранной разведке

Поскольку главной целью Патриотического Акта являлось расширение полномочий правоохранительных органов для борьбы с международным терроризмом, часть поправок коснулась также Закона об иностранной разведке:

- **Прослушивание любых линий связи.** Обычно, в случае представления ордера на перехват сообщений по линиям связи, в ордере уточнялось, о прослушивании каких линий связи идет речь: телефонных либо подключений к Интернету. В соответствии с поправками, вносимыми Патриотическим Актом, Закон об иностранной разведке теперь позволяет выполнять «прослушивание любых линий связи в разведывательных целях». Это означает, что один и тот же ордер позволяет выполнять как прослушивание телефонных переговоров, так и перехват электронного сообщения без указания конкретного типа наблюдения в ордере. Кроме того, в таком случае подразумевается, что при выполнении наблюдения другие лица, использующие данное

средство связи, но не связанные с расследованием дела о шпионаже, также могут быть прослушаны. К примеру, если подозреваемый по делу о терроризме использует подключение к Интернету в общественной библиотеке, ФБР имеет право отслеживать все обращения к Интернету из данной библиотеки. Другое положение Закона запрещает администрации библиотеки или же любой другой третьей стороне, которая привлечена правительством для сотрудничества, сообщать о ведущемся наблюдении своим пользователям. (Американская ассоциация библиотек даже опубликовала советы библиотекарям на своей официальной веб-странице [www.ala.org/alaorg/oif/usapatriotact.html](http://www.ala.org/alaorg/oif/usapatriotact.html)). Частные адвокаты заявили о серьезном нарушении четвертой поправки к конституции Соединенных Штатов.

- **Устройства регистрации входящих/исходящих IP-адресов или телефонных номеров.** Согласно Закону об иностранной разведке, правительство должно предоставить Суду по делам об иностранной разведке достаточные доказательства того, что объектом наблюдения будет агент иностранной разведки, перед получением санкции на использование подобных регистрирующих устройств. Патриотический Акт отменил это требование, и теперь правительство может применять подобные средства наблюдения «для проведения любых расследований с целью сбора информации об иностранной разведке». Однако к этому закону добавлено еще одно положение, которое запрещает использование подобных устройств по отношению к гражданам США, поскольку это нарушает четвертую поправку к Конституции, касающуюся их прав и свобод. Это означает, что, даже если вы носите мусульманское имя, но нет никаких доказательств вашей причастности к шпионской деятельности, запрос на применение подобных устройств регистрации для наблюдения за вами будет отклонен.
- **Увеличение числа судей в Суде по делам об иностранной разведке.** В соответствии с данным актом, в состав Суда по делам об иностранной разведке вводятся дополнительные пять судей для обеспечения эффективной работы с возросшим объемом дел и более тщательной обработки поступающих запросов.
- **Стандарты на проведение наблюдений.** До сих пор разрешение на наблюдение в соответствии с Законом об иностранной разведке выдавалось в тех случаях, когда первоначальной или единственной целью наблюдения являлось расследование того или иного преступления. В настоящее время, если дело в «значительной мере» сводится к сбору информации об иностранной разведдеятельности, запрос на проведение наблюдения будет удовлетворен. А поскольку словосочетание «в значительной мере» звучит весьма расплывчато, подобная двусмысличество вызывает некоторую беспокоенность.

## Закон о компьютерном мошенничестве и злоупотреблениях

Помимо четко определенных поправок к законам о терроризме Патриотический Акт включает положения, касающиеся статей Закона о компьютерном мошенничестве и злоупотреблениях. Многие защитники прав электронной собственности высказывают протесты против подобных изменений, рассматривая их как попытку правительства ужесточить законы в отношении компьютерных преступлений, прикрываясь борьбой против терроризма.

Следующие положения Закона касаются вопросов электронного наблюдения:

- «Попытка совершения правонарушения» теперь приравнивается к «совершению правонарушения», что влечет за собой одинаковые меры пресечения.
- В случае повторного совершения преступления, нарушающего положения данного Закона, возможно ужесточение меры наказания.
- Действие данного Закона может распространяться на компьютеры, расположенные за пределами Соединенных Штатов, если экономический ущерб был нанесен американским компаниям или организациям.
- Законом предусматривается увеличение максимальной меры пресечения за нарушение данного Закона – до 10 лет за первое нарушение и до 20 лет за повторное.
- В определение «потерь» включается: время, потраченное на восстановление и покрытие нанесенного ущерба, восстановление данных, программ, систем или информации; потеряная прибыль; дополнительные затраты и потери в результате иных последствий нанесенного урона. (Благодаря чему оказывается довольно легко достичь максимального штрафа в 5000 долларов.)
- Компьютерные преступления, представляющие собой угрозу национальной безопасности либо приведшие к разрушениям, вызвавшим физический ущерб, включая прекращение медицинского обслуживания и опасность для жизни и здоровья людей, классифицируются как террористическая атака.

В ранней редакции Закона любые, даже незначительные, вторжения в компьютерные системы и нанесение ущерба веб-сайтам также приравнивались к террористической угрозе, однако из окончательной версии Закона эти положения были убраны.

## Разоблачения: злоупотребления Законом об иностранной разведке

Министерство юстиции США выступает за более тесный обмен информацией между правоохранительными органами и разведывательными службами, что противоречит концепции **минимизации**, обсуждавшейся в начале данной главы (минимизация подразумевает практику неразглашения информации, касающейся деятельности разведки, правоохранительным органам, занимающимся расследованием уголовных преступлений). Расширение обмена информацией между полицией и разведслужбами необходимо для упрощения процедуры получения разрешений на проведение наблюдений для правоохранительных органов, чтобы они могли заявлять об угрозе со стороны других государств, а не мелких воришек. С другой стороны, управляя двумя ветвями расследования, правоохранительные органы легко могут злоупотребить положениями Закона об иностранной разведке, применив их к лицам, никак не связанным с подозрениями в терроризме или шпионажем на пользу других государств.

Несмотря на желание Министерства юстиции ограничить действие правила минимизации, Суд по делам об иностранной разведке имеет на этот счет иное мнение. В августе 2002 года решение, принятное еще в мае Судом по делам об иностранной разведке, наконец-то стало известно широкой общественности.

Председательствующий судья Суда по делам об иностранной разведке, глава окружного суда Ройс Ламберт заявил, что ФБР допустила большое число ошибок при использовании санкций на обыск, выдача которых аргументировалась угрозами национальной безопасности в дела, посвященных расследованию случаев терроризма начиная с 2000 года. «Практически во всех случаях некорректные заявления правительства, упущения в Законе об иностранной разведке и нарушения применения судебных ордеров включали несанкционированную передачу и распространение информации отделам, занимающимся расследованием уголовных преступлений и обвинителям». Это было достаточно жесткое заявление.

Генеральный прокурор Джон Ашкрофт продолжил движение в этом направлении, заявив о необходимости обмена информацией для защиты национальной безопасности и подав свое дело на рассмотрение в Апелляционный Суд по делам об иностранной разведке в надежде на отмену решения по Закону об иностранной разведке. 18 ноября 2002 года Апелляционный Суд вынес свое первое решение, предоставляющее Министерству юстиции новые полномочия в плане прослушивания линий связи при расследовании уголовных преступлений. Таким образом, Апелляционный Суд отменил предыдущее решение Суда по делам об иностранной разведке, ограничивающее вышеуказанные полномочия (что никак не было связано с соблюдением права на частную жизнь граждан).

## Другие положения

В Патриотическом Акте 2001 года содержится также ряд других положений, среди которых много статей, касающихся терроризма, но никак не связанных с компьютерным шпионажем. Тем не менее следует упомянуть о ряде положений Акта, которые противоречат многим федеральным законам о наблюдении. К таковым относятся следующие положения Патриотического Акта:

- Доступом к информации, полученной от членов большого жюри или в результате прослушивания линий связи, теперь обладает большее количество правительственные учреждений и официальных лиц.
- Расширена сфера применения судебных повесток, и теперь занимающиеся расследованием правоохранительные органы имеют право на получение сведений о подписчиках Интернета, в том числе, к примеру, о способах оплаты ими счетов, времени и продолжительности пребывания в сети Интернет, и временно назначенных им сетевых адресах.
- Провайдеры Интернета (и не только) обладают правами на просмотр информации, хранимой на принадлежащей им технике, например электронной почты или любой другой информации о своих клиентах, если у провайдера имеются «обоснованные подозрения» в том, что данные сведения могут представлять «угрозу жизни и здоровью людей».
- Правила проведения тайных обысков в ходе расследования любых преступлений стали более либеральными по отношению к правоохранительным органам, которые теперь не обязаны сообщать подозреваемому на ранних стадиях расследования о наличии ордера на обыск. Обычно при проведении большинства уголовных расследований подозреваемому предъявлялись копии ордеров на обыск. При помощи «секретного ордера» суд получил возможность ставить субъекта в известность «в свое время», если немедленное раскрытие планов может помешать ведению расследования.

## Законы штатов

Хотя Патриотический Акт является законом федерального значения, многие штаты также решили привести свои законы в соответствие с данным документом. Законы «о защите отечества», «о борьбе с терроризмом» и с «другими словами, используемыми в политических играх» начали появляться как грибы после дождя сразу после подписания Патриотического Акта. Эти законы в своем большинстве дублировали положения Акта об объединении и усилении Америки средствами, необходимыми для борьбы с терроризмом, расширяя полномочия правоохранительных

органов в плане проведения слежки и ужесточения мер пресечения. Обязательно ознакомьтесь с законодательством вашего штата, чтобы представлять себе всю ситуацию целиком.



Полный текст Патриотического Акта можно найти по адресу <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:%5D>.

## Реалии соблюдения законодательства

Эффективность законов напрямую связана с их соблюдением. Несмотря на то, что компьютерный шпионаж является незаконным в соответствии с целым рядом документов, вы не услышите на каждом углу о проведении связанных со шпионажем судебных разбирательств. Это странно, в особенности если учесть количество людей, занимающихся шпионажем.

Среди причин, по которым правоохранительные органы редко проявляют всю строгость по отношению к нарушителям законов о шпионаже, можно перечислить следующие:

- общая перегруженность судебного делопроизводства;
- недостаточное количество квалифицированных офицеров полиции, способных принимать участие в расследовании дел, связанных с компьютерным шпионажем;
- сложность обнаружения шпионских действий;
- недостаток весомых доказательств;
- нежелание пострадавших сообщать о случаях шпионажа из-за боязни того, что публичное разглашение может опорочить их репутацию и нанести экономический ущерб;
- наибольшее внимание и ресурсы в настоящее время привлечены на борьбу с терроризмом, в результате чего другим преступлениям, среди которых и компьютерный шпионаж, уделяется меньше внимания.

Однако не стоит ошибочно полагать, что шпионаж – это такое же безопасное занятие, как, например, езда со скоростью 60 км/ч в зоне с ограничением скорости до 50 км/ч. Количество судебных разбирательств на уровне штатов и округов, посвященных расследованиям дел о компьютерном наблюдении, постоянно увеличивается. И хотя подобные разбирательства могут показаться незначительными на фоне громких дел по компьютерному и промышленному шпионажу государственного уровня, они тем не менее создают прецеденты, облегчая обвинителям рассмотрение последующих дел. Постепенно обученные компьютерной грамоте

представители правоохранительных органов и обвинители, подкрепленные политическими мотивациями «дать твердый отпор преступникам», уделяют все больше внимания компьютерным преступлениям.

## Контрмеры: добрые, галантные агенты ФБР

ФБР признает, что кибер-преступления, включая компьютерный шпионаж, представляют собой растущую угрозу. В октябре 2002 года, выступая перед лицом торгово-промышленной группы, глава ФБР Роберт Мюллер заявил слушателям, что лишь треть компьютерных преступлений становится известной Федеральному Бюро. Зная о том, что многие корпорации не спешат обращаться в правоохранительные органы, дабы не допустить огласки, Мюллер постарался успокоить их представителей, сказав следующее:

«Позвольте мне в первую очередь рассказать вам о том, чего не случится, если вы сообщите о фактах компьютерных преступлений либо проникновений. Ваши офисы не будут окружены толпой агентов в черных комбинезонах с вышитыми буквами ФБР. Мы прекрасно понимаем недопустимость подобных действий с нашей стороны. Мы приедем вам на помощь, как пострадавшей стороне, а не станем вас преследовать. Наши специалисты в гражданской одежде, возможно под видом консультантов или ваших деловых партнеров, будут присутствовать рядом с вами в нужное время и в нужном месте.

Мы не станем проводить пресс-конференций или публиковать пресс-релизы. И уж ни в коем случае не станем разглашать подробности дел, находящихся в процессе рассмотрения. Что касается утечек информации – все лица, ответственные за подобные происшествия, будут отвечать лично передо мной.

Мы не будем вмешиваться в работу вашей системы в нуждах следствия либо подключать дополнительные компьютеры к вашей сети.

И мы не станем изучать ваши файлы, чтобы узнать о ваших бизнес-планах. Заверяю вас, что нас не интересует ваша конфиденциальная информация».

Таким образом, ФБР всячески пытается убедить торгово-промышленные компании в необходимости немедленно сообщать о фактах компьютерного шпионажа, для чего Федеральному Бюро вначале нужно завоевать их доверие. Преуспеют ли они в этом – мы вскоре увидим сами.

Кроме того, если вы намерены заняться некоторым видом наблюдения или прослушивания, хорошо подумайте, не могут ли ваши действия

быть классифицированы как террористическая деятельность, пусть даже в самом отдаленном контексте. Учтите, что под данную категорию нередко подпадают даже обычные безобидные занятия. К примеру, летом 2002 года Федеральное Бюро Расследований запросило информацию обо всех членах организаций по спортивному погружению и о людях, прошедших курсы ныряльщиков и посещавших в последнее время магазины спортивного инвентаря с целью приобретения собственного обмундирования. Причиной для таких действий послужило предположение, что даже ныряльщики с минимальными навыками, находящиеся на отдыхе в США, могут совершить попытки подрыва судов в портах; однако эта теория была вскоре опровергнута как самими ныряльщиками, так и профессионалами по обеспечению безопасности.

Поэтому помните, что даже если вы не платите членские взносы в Аль-Каиду, но при этом совершаете незаконные операции при помощи компьютера, то в случае раскрытия вашей деятельности вы можете предстать перед судом штата или же федеральным судом.

## Гражданский и уголовный суд

До сих пор мы рассматривали вопросы, связанные с уголовным законодательством. Однако когда разговор заходит о промышленном шпионаже, помимо уголовного преследования, существует немалая вероятность того, что данное дело может быть подано на рассмотрение и в гражданский суд.

Гражданское судопроизводство начинается тогда, когда физическое или юридическое лицо (компания, организация либо правительство) подает иск на другое физическое или юридическое лицо за нанесение ущерба, требуя выплаты компенсации через суд. Каждая сторона при этом нанимает своих собственных адвокатов, а судья либо жюри присяжных принимают окончательное решение. Например, если шпион, работающий на конкурирующую компанию, был пойман с поличным, пострадавшая компания может подать в суд как на шпиона, так и на нанявшую его сторону, дабы потребовать возмещения ущерба, нанесенного действиями злоумышленника.

Между уголовным и гражданским судопроизводством существуют два главных отличия:

- **Наказание.** В уголовном суде это может быть тюремное заключение, денежные штрафы либо и то и другое вместе. В гражданском суде речь может идти только о денежных компенсациях.
- **Факты, требующие доказательства.** В уголовных разбирательствах обвинители должны располагать уликами, которые «не вызывают сомнения в виновности» подсудимого. Это означает, что доказательств должно быть достаточно для того, чтобы обычный человек мог сказать: «Да, на основании подобных

доказательств я считаю, что подсудимый виновен». В гражданском судопроизводстве не используются такие строгие стандарты для доказательства чьей-то вины, здесь суд руководствуется так называемым правилом преобладающих доказательств. То есть если количество улик, говорящих о пользу виновности той или иной стороны, превышает количество доказательств, говорящих в ее защиту, то сторона считается виновной. Классический пример судебного разбирательства по правилу преобладающих доказательств – дело О. Джей Симпсона. В 1995 году в уголовном суде жюри присяжных признало Симпсона невиновным, поскольку против него не было собрано достаточно улик, которые бы «не вызывали сомнений в виновности». Однако в 1997 году в ходе рассмотрения дела Симпсона в гражданском суде жюри присяжных посчитало, что в данном случае доказательств достаточно, чтобы считать Симпсона ответственным за смерть Рональда Голдмана и Николь Браун Симпсон, и обязало его выплатить 8,5 миллиона долларов семьям пострадавших.

Следует заметить, что гражданский суд имеет право на выдачу ордеров на арест и конфискацию имущества в гражданском делопроизводстве. Например, если судья решил, что ответчик (лицо, которое должно будет выплачивать компенсацию, если его признают виновным) хранит доказательства своей шпионской деятельности на корпоративном сервере, суд может арестовать технику, выдав ордер офицерам правоохранительных органов или представителям истца (лица, требующего выплаты компенсации). Арест компьютерной техники в данном случае подразумевает также арест и изъятие хранимой на ней информации. К примеру, корпорация может затеять дело «против некоего Джона До» – и добиться от провайдера услуг Интернета сообщения информации обо всех клиентах этого провайдера, которые могут быть связаны с текущим расследованием.

### Разоблачения: налетчики потерянной Амазонки

В ноябре 1999 года компания Alibris, специализирующаяся на онлайновой продаже книг через Интернет, урегулировала федеральный иск фирмы Amazon.com о проведении наблюдения при помощи электронной почты и незаконного использования компьютерных паролей. Фирма Amazon.com столкнулась с десятью случаями нарушения Закона о защите компьютерных систем и одним фактом кражи пароля для использования в целях личного обогащения. Несмотря на то, что обвинение по каждому пункту предусматривает штраф размером до 250 000 долларов, компания Alibris смогла урегулировать дело всего за один штраф размером в 250 000 долларов.

Предшественник компании Alibris, расформированная корпорация под названием Interloc Inc., также представляла собой онлайновый магазин по продаже книг, который, вдобавок, владел дочерней компанией Valinet, занимающейся предоставлением услуг Интернета. На протяжении 1998 года Interloc осуществила перехват и сохранение нескольких тысяч электронных писем, пришедших с Amazon.com клиентам компании Valinet, многие из которых также торговали книгами. Хотя случаев раскрытия финансовой или личной информации зафиксировано не было, суд посчитал, что одной из целей перехвата сообщений являлось предоставление конкурентных преимуществ компании Alibris. (Обвинители также заявили, что Interloc незаконно хранила копии конфиденциальных паролей и список клиентов конкурирующих провайдеров Интернета.)

Поскольку веб-сайту Amazon был нанесен незначительный ущерб, никаких дополнительных исков, гражданских или уголовных, компании Alibris предъявлено не было. Когда директору Alibris напомнили о недавних разбирательствах, он в ответ заявил: «Сейчас мы совершенно другая компания, которая хочет покончить с дозволенностью подобных методов». В настоящее время компания Alibris по-прежнему при делах и даже является одним из лидеров онлайновой торговли редкими книгами.

## Начальство и подчиненные – узаконенный шпионаж

В соответствии с Законом о защите информационных систем, работодатель не имеет права прослушивать телефонные разговоры либо просматривать электронную почту нанимаемых в тех случаях, когда работник вправе рассчитывать на невмешательство в свою частную жизнь. В каких случаях работник вправе рассчитывать на невмешательство в частную жизнь, спросите вы, – работодатель не может устанавливать камеры слежения в общественных уборных, например. Тем не менее тот же самый Закон позволяет работодателям вести наблюдение за своими подчиненными, предварительно поставив их в известность об этом, в тех случаях, когда, по мнению руководства, существует угроза интересам компании. Такая формулировка допускает двусмысленную трактовку, поэтому не стоит рассчитывать на какую-либо конфиденциальность на своем рабочем месте, ведь практически за всеми вашими действиями за компьютером может вестись наблюдение. Тем не менее существуют некоторые исключения:

- **Госслужащие.** Согласно первой, четвертой и четырнадцатой поправке к Конституции, государственные служащие имеют права и привилегии, действие которых не распространяется на сотрудников частных компаний. К примеру, в государственных учреждениях, учреждениях штата и местных учреждениях руководство обязано соблюдать ваши права на свободу волеизъявления и, как правило, не имеет права вести необоснованное наблюдение за вами либо без веских оснований арестовывать технику и данные.
- **Союзы рабочих.** Национальный закон о трудовых взаимоотношениях (National Labor Relation Act – NLRA) действует по отношению к организованным либо организуемым рабочим местам. В соответствии с ним, коллективные договоры могут ограничивать права работодателя на наблюдение за своими сотрудниками, даже если федеральный Закон о прослушивании линий связи либо другой закон штата позволяют выполнять подобные действия. Закон о трудовых взаимоотношениях также ограничивает полномочия работодателей в плане наблюдение за своими подчиненными, если это противоречит праву служащих на «самоорганизацию» либо «согласованную активность».

Несмотря на то что в настоящее время отсутствуют федеральные законы о соблюдении невмешательства в частную жизнь на рабочем месте, прежде чем осуществлять мониторинг деятельности своих подчиненных, проконсультируйтесь со своим адвокатом о полном соответствии ваших действий текущему законодательству. В некоторых штатах существуют дополнительные законы, отстаивающие право граждан на частную жизнь, как, например калифорнийский Закон о невмешательстве в частную жизнь (California's Privacy Act); в других штатах подобные законодательные акты находятся на стадии рассмотрения. Поскольку общественный интерес к вопросам невмешательства в частную жизнь в последнее время активно возрастает, советуем вам отслеживать текущие изменения законодательства.

Хотя сегодняшние законы чаще отстаивают интересы работодателя, осторожные коммерческие компании вынуждены продумывать дополнительные меры предосторожности, призванные обезопасить их от потенциальной возможности преследования за нарушение законов о невмешательстве в частную жизнь. Три простейших, не требующих особых затрат способа приводятся ниже:

- **Использование неявного согласия.** Сюда относится использование информационных баннеров во время загрузки, надоедливых напоминаний (которые выводятся программами, вроде keylogger) или любых других визуальных методов оповещения сотрудников компании о том, что за всей их электронной почтой, навигацией по Интернету и другими компьютерными операциями может вестись наблюдение со стороны работодателя.

- **Использование явного согласия.** Здесь подразумевается добавление в трудовое соглашение либо другой документ пункта, касающегося возможности наблюдения за сотрудником на его рабочем месте.
- **Использование подписей в электронных сообщениях.** Добавление абзаца в конце исходящих сообщений, в котором оговаривается, что данное сообщение может быть перехвачено и просмотрено работодателем. Хотя подобная практика кому-то может показаться излишней, но при этом получатели извещаются о том, что их переписка с отправителем заведомо не является конфиденциальной.

Учтите, что, благодаря обнародованию вашей политики мониторинга, вы не только защитите себя от судебных преследований, но и предостережете ваших пользователей от применения предоставленных ресурсов не по назначению. Если пользователь знает, что за его действиями ведется наблюдение, он дважды подумает, прежде чем решиться, например, на кражу информации.

## Внутрисемейные судебные разбирательства

В 1976 году Национальная Комиссия по пересмотру федеральных и местных законов, связанных с прослушиванием линий связи и электронным наблюдением, сообщила о том, что 68% всех случаев прослушивания, о которых им стало известно, были связаны с наблюдением супругов друг за другом по личным причинам. Еще 11% стали результатом «родительской опеки». Короче говоря, около 80% всех случаев наблюдения сводились к внутрисемейным «разборкам». Хотя этот отчет увидел свет еще в докомпьютерную эру и касался он исключительно подслушивания телефонных разговоров, полагать, что в наше время ситуация резко изменилась, будет, по меньшей мере, наивно. Просто теперь склонные к подозрительности супруги или родители могут не только прослушивать телефонные переговоры, но и шпионить за компьютерами друг друга при помощи программ, сохраняющих последовательность нажатия клавиш в файл, либо же посредством перехватчиков сетевых пакетов.

Значительное количество рассматриваемых дел связано с супружеским шпионажем, и хотя большинство из них касается тайной записи телефонных разговоров, учтите, что Закон о прослушивании линий связи также применим и для компьютерного наблюдения. Несмотря на отсутствие (пока что) громких дел, связанных с использованием программ для сохранения в файле последовательности нажатых клавиш либо программ перехвата сетевых пакетов, которые могли бы выступать в качестве

юридического прецедента, результаты предыдущих разбирательств, связанных с прослушиванием телефонных переговоров, также учитываются прокурорами и судьями при вынесении окончательного вердикта.

Как правило, в случае нарушения Закона о прослушивании линий связи супругами, суд может действовать двумя способами:

- **Не допуская исключений.** В 1976 году в деле Соединенных Штатов против Джонса Федеральный Апелляционный Суд отменил решение окружного суда по делу супруга, занимавшегося подслушиванием телефонных разговоров своей раздельно проживающей жены, которое создавало прецедент для исключения из Закона о прослушивании линий связи. Суд заявил: «Если Конгресс намеревается создать еще одно исключение к Закону о прослушивании, запрещающему проведение любого несанкционированного прослушивания телефонных переговоров, они могли бы включить в закон специальное исключение для супружеских пар». И хотя в федеральных судах подобные дела рассматриваются очень редко, в большинстве из этих немногих судебных разбирательств на уровне штатов или даже федеральном уровне при вынесении вердикта принималось во внимание окончательное решение по делу Джонса.
- **По правилу исключения для супругов.** В 1974 году в деле Симпсона против Симпсона (ни одного из участников разбирательства не звали О. Джей или Гомер\*), в котором муж тайно записывал телефонные разговоры своей жены, Федеральный Суд ввел исключение для «внутрисемейных дел» к Закону о прослушивании линий связи, полагая, что действие Закона не может распространяться на личные отношения супругов, хотя подобной оговорки нет в самом Законе. Решение по делу Симпсона против Симпсона использовалось в качестве юридического прецедента при вынесении нескольких других судебных вердиктов.

Поэтому, если вы используете программу, сохраняющую в файл последовательность нажатия клавиш для наблюдения за своей супругой (супругом), а также любите заниматься чтением электронных сообщений, предназначенных вашей половине, знайте, что вы играете с законом. Единственное, что однозначно определено в обоих случаях, – любое наблюдение со стороны третьего лица за супругой (-ом) по поручению второго супруга однозначно нарушает Закон о прослушивании линий связи. (Если отношения с вашей половиной не оформлены юридически, и при

---

\* О. Джей Симпсон – обвиняемый в уголовном деле, рассматривавшемся в уголовном и гражданском производстве. Это дело обычно используется в качестве примера различия в подходах к признанию обвиняемого виновным уголовным и гражданским судами. Говард Симпсон – одно из действующих лиц мультсериала «Симпсоны». – Прим. ред.

этом вы любите за ней шпионить, учтите, что вы ступаете на тонкий лед, особенно если ваша половина обладает сутяжническим характером.)

Не означает ли это, что незаконным считается даже наблюдение за собственными детьми со стороны родителей, – спросите вы? Здесь также существуют прецеденты, подавляющее большинство которых связано с делами о разводах, в ходе которых родители тайно записывали разговоры своих детей со своим супругом/супругой. Многие суды допустили возможность исключения для дел между детьми и их родителями, поскольку в данном случае затрагивались отношения опекунства. Фактически суд заявил, что родитель-опекун может прослушивать переговоры своего ребенка, если он имеет основания полагать, что подобное наблюдение служит интересам ребенка. Опять-таки, приведем пример с программой keylogger: хотя в самом Законе о прослушивании нет пункта, исключающего ответственность родителей, юридически в случае компьютерного наблюдения за вашим чадом вы рискуете гораздо меньше, чем шпиона за своей второй половиной. Однако, как только ваш ребенок достигает совершеннолетия, все меняется. (Замечание для детей, которые любят шпионить за своими родителями: ваш возраст служит вам защитой от попадания в тюрьму в том случае, если вас, в конце концов, поймают, когда вы будете наблюдать за мамой и папой. Однако учтите, что родители, собравшиеся наказать своего ребенка, могут оказаться менее терпимыми, чем судьи.)

## Заключение

Как видите, существует целый ряд федеральных законов и законов на уровне штата, по которым могут быть предъявлены обвинения в компьютерном наблюдении. Не нужно быть адвокатом, чтобы иметь общее представление об этих законах, однако рассмотрение отдельных подробностей и нюансов все же следует поручить вашему поверенному. Следует помнить о трех важных моментах, когда речь заходит о судебных разбирательствах (независимо от того, связаны они со шпионажем или нет):

- **Законодательство не поспевает за техническим прогрессом.** Существующие законы и юридические прецеденты не поспевают за бурным техническим прогрессом в области компьютерных сетей, аппаратного и программного обеспечения. Как правило, отставание исчисляется, по крайней мере, несколькими годами, когда речь заходит о применении злоумышленниками новейших технологий. Естественно, юристы пытаются угнаться за сегодняшними техническими реалиями, однако принятие новых технологий всегда занимает некоторое время.
- **Законы не всегда безупречны.** Идея Закона, стоящего на страже интересов общества, к сожалению, звучит несколько наивно («вы должны нам верить, поскольку мы знаем, как будет лучше

для вас»). Патриотический Акт США прошел через Конгресс с минимальными поправками из-за царившего тогда общего эмоционального настроя. Закон о защите отечества, принятый в декабре 2002 года, содержит еще больше положений, связанных с электронным наблюдением, которые не требуют наличия повесток или судебного контроля. Черновики нового закона, помеченные как конфиденциальные, под рабочим названием «Закон о повышении внутренней безопасности», получившего в народе название «Патриотический Акт №2», увидели свет в феврале 2003 года. Согласно этому закону правительство получает в свое распоряжение еще большую власть в плане электронного наблюдения. Поэтому любителей новых технологий, скорее всего, ожидает закон, который (цитирую Спока) «кажется абсолютно нелогичным».

- **Изменение законов.** Перемены неизбежны, и это в полной мере касается законодательства. Хотя смена законодательства не происходит столь стремительно, как, например, технологические изменения, завтра законы могут приобрести новое звучание. Новые законы и судебные решения, юридические прецеденты, по-иному толкующие старые законы, не позволяют адвокатам терять бдительность. То же самое должно относиться и к вам, и к другим сотрудникам вашей организации. Сегодняшний Закон об электронном наблюдении может кардинально измениться за ближайшие несколько лет.

Теперь, после краткого ликбеза по юриспруденции, мы можем, наконец, перейти к более интересным темам книги (попрошу юристов не обижаться): как правильно заниматься шпионажем и как обезопасить от шпиона себя.

## Глава 3

# Тайные проникновения

«Я работаю по ночам».

Анонимный агент ФБР, сотрудник секретного подразделения, отвечая на вопрос о том, что он делает, чтобы заработать средства к существованию.

## Взгляд изнутри

Под тайными проникновениями подразумеваются действия ФБР по несанкционированному вторжению в чужие жилища с целью сбора информации, доказательств либо установки электронных «жучков». Американский термин для обозначения тайных проникновений звучит как «*black bag job*», что в дословном переводе означает «работа с черными сумками». Этот термин возник еще во времена Второй мировой войны, когда агенты ФБР использовали черные кожаные докторские сумки для доставки и выноса оборудования с места операции. Политически корректный термин для обозначения подобных действий правоохранительных органов по нелегальному проникновению в жилища и офисы звучит как «тайные проникновения».

Хотя тайные проникновения в места, где вы не имеете права находиться, и похищение чужих секретов практикуются на протяжении всего времени существования человечества, первые случаи организованного проникновения в разведывательных целях начались в 20-х годах XX века, когда ВМФ США профинансировало ряд операций по тайным проникновениям, направленным против японского правительства. Общими усилиями государственной и Военно-морской разведки, ФБР и полиции Нью-Йорка было организовано проникновение агентов в японское консульство на территории Нью-Йорка, в ходе которого был взломан сейф и сфотографирован Журнал морских кодов Японии. Благодаря данному рейду, США обрели существенное преимущество в довоенные годы, получив возможность читать зашифрованные сообщения японской разведки. Несанкционированные проникновения, направленные против Японских представительств, продолжались до 1939 года, и за это время было совершено несколько успешных операций по проникновению в офисы Японских представительств в Нью-Йорке.

С тех времен, благодаря развитию науки и техники, методы проникновения стали более изощренными. По всему миру существуют правительственные и частные школы, обучающие специальным навыкам тайных проникновений военных, работников правоохранительных органов и разведчиков. Часто полученные в подобных школах навыки затем используются частными детективами, в роли которых выступают бывшие агенты.

Проникновение может считаться законным, если суд предоставил правоохранительным органам соответствующую санкцию на проведение операции по проникновению с целью сбора доказательств, либо, к примеру, в случае проведения коммерческой компанией расследования на своей территории, о котором не должны знать ее сотрудники. Проникновения будут считаться незаконными, если операция проводится без соответствующих санкций. (Помните о том, что, если вы занимаетесь подобными действиями незаконно, вам могут предъявить обвинение по статье о краже со взломом и незаконному проникновению в чужое жилище, которая предусматривает уголовную ответственность и к нарушению которой полиция и суды относятся достаточно щепетильно.)

Тайные проникновения отлично подходят для проведения компьютерного шпионажа по целому ряду причин:

- Из-за большого количества данных, хранимых в электронном виде, а также относительной легкости и быстроты их копирования в результате тайного проникновения за короткий промежуток времени может быть получена информация огромной ценности.
- С технической точки зрения, поскольку устойчивые системы шифрования становится весьма сложно, а иногда и просто невозможно взломать, то скрытые проникновения в офисы или жилые помещения, например, для установки «жучков» на клавиатуру, как в деле гангстера Никодермо Скарфо, остаются последней надеждой правоохранительных органов на поимку преступников. (Упрощение правил получения разрешений на проведение подобных операций по прослушиванию в соответствии с Патриотическим Актом США может привести к росту числа таких операций в ближайшие годы.)



Более подробно о деле Никодермо Скарфо-младшего вы узнаете из восьмой главы данной книги.

В этой главе мы поговорим о различных видах несанкционированных проникновений, способах их проведения и о некоторых мерах, которые помогут вам защититься от аналогичных действий, направленных против вас.

## Физические и сетевые проникновения

Тайные проникновения могут осуществляться где угодно: в жилых помещениях, офисах, машинах либо комнатах отеля. К примеру, во время расследования ФБР по делу Гарольда Николсона, агента ЦРУ, подозреваемого в шпионаже на пользу России, сотрудники ФБР тайно проникли в его спортивный автомобиль Chevrolet Lumina и обнаружили в нем личный ноутбук Гарольда. Агенты скопировали образ жесткого диска и позднее нашли на нем секретные файлы ЦРУ. Кроме того, в машине была найдена дискета с информацией об агентах, с которыми сотрудничал Николсон, а также об американских гражданах, часто путешествующих за границу и поставляющих информацию для ЦРУ. Эти улики сыграли решающую роль в признании виновности Николсона.

Когда речь заходит о компьютерном шпионаже, можно говорить о двух основных видах тайных проникновений:

- **Физическое проникновение.** Здесь мы подразумеваем традиционное проникновение со взломом в помещения, где мы не имеем права находиться. Отмычки, системы сигнализации, и Том Круз, висящий вниз головой на трапеции над компьютером. С физическим проникновением связан наибольший риск разоблачения со стороны людей, подозревающих о ваших намерениях. Кроме того, правоохранительные органы достаточно «набили руку» в расследовании подобных дел, поскольку преступления, связанные со взломами и кражами личной собственности и собственности организаций, происходят достаточно часто.
- **Сетевое проникновение.** Вместо взлома замков и физического проникновения в чужие помещения, шпионы могут осуществлять удаленные сетевые проникновения для сбора интересующей их информации. При правильном подходе, сетевые вторжения представляют гораздо меньший риск для взломщиков, чем физическое проникновение, поскольку скрыть свои следы в виртуальном пространстве гораздо легче, чем в реальном мире. Вдобавок правоохранительные органы еще не обладают достаточным опытом, навыками или персоналом для расследования электронных преступлений, в отличие от расследования физических краж со взломом. Недостатком сетевых атак является возможность получения доступа только к той информации, которая хранится непосредственно на компьютере, тогда как в случае физического проникновения вы можете собирать все виды интересующей вас информации, не обязательно хранимой в цифровом виде.



Поскольку данная глава посвящена в первую очередь физическим проникновениям, техника, применяемая шпионами для проведения несанкционированных сетевых атак, будет описана отдельно в главе 10 этой книги.

## Разоблачения: Уотергейтское дело

Самое известное тайное проникновение в истории было осуществлено в рамках Уотергейтского дела в штаб-квартиру Национального Комитета демократической партии в Вашингтоне, округ Колумбия, размещенную в Уотергейтском гостинично-офисном комплексе. Взлом, санкционированный руководством Белого дома, был совершен 17 июня 1972 года. Белый дом и до этого занимался поддержкой несанкционированных проникновений при помощи своего подразделения для специальных расследований, занимающегося предотвращением утечки секретной информации, в состав которого входили бывшие разведчики и представители правоохранительных органов.

Пять человек, назначенных на выполнение Уотергейтской операции, были снабжены специальными приборами, используемыми ЦРУ, включая камеры слежения, наборы отмычек, миниатюрные газовые баллончики, подслушивающую аппаратуру и радиопередатчиками. Они проникли в комплекс в течение уик-энда, предшествовавшего Дню павших в гражданской войне, установили «жучки», однако затем вынуждены были вернуться, обнаружив, что один из поставленных ими «жучков» не работает. Хотя все члены спецподразделения являлись сотрудниками ЦРУ, ФБР или были ранее так или иначе связаны с этими службами, незначительная небрежность при выполнении работы привела к их поимке. Один из них забыл убрать с дверной защелки ленту,держивающую дверь в открытом состоянии, в результате чего охранник их обнаружил и вызвал полицию. Остальное, включая отставку Ричарда Никсона, – уже история.

Эжен Р. Мартинез, один из взломщиков, написал отличный рассказ об этом проникновении со всеми подробностями. Прочесть его вы можете в сети Интернет по адресу:  
[www.watergate.info/index.php?itemid=18](http://www.watergate.info/index.php?itemid=18).

## Запланированные и случайные проникновения

Тайные проникновения бывают двух видов: предварительно запланированные и совершенные при благоприятном стечении обстоятельств. Одна из главных задач, преследуемая в случае тайного проникновения, заключается в том, чтобы целевой объект шпионажа никогда не узнал о совершенной операции (или, по крайней мере, до того момента, пока не станет слишком поздно). Итак, при выполнении тайных проникновений применяются два подхода:

- **Запланированное проникновение.** Отличительной особенностью хорошо подготовленной атаки является экстенсивное планирование. Вся операция предварительно тщательно продумывается.

Важность планирования тем выше, чем сложнее предстоящая операция, особенно если в ходе ее выполнения предстоит столкнуться с системами сигнализации, охранниками, собаками и другими строгими физическими мерами обеспечения безопасности. Чем больше сил брошено на защиту объекта, тем более точное планирование и тем больше ресурсов необходимо для осуществления проникновения. (Естественно, даже при тщательно составленном плане и наличии опытного персонала операция все равно может сорваться: вспомним хотя бы Уотергейтское дело.)

- **Случайное проникновение** (при благоприятном стечении обстоятельств). Когда обстоятельства благоволят шпиону, и по тем или иным причинам объект временно становится легко доступным, злоумышленник может осуществить тайное проникновение, даже если изначально оно не планировалось. Проникнув, шпион может заняться целенаправленным поиском нужных ему данных либо выкрасть всю доступную информацию в надежде, что его нынешний или потенциальный работодатель заинтересуется ею. В этой ситуации планирование операции сводится к минимуму. Шансы успешного исхода подобного мероприятия невелики, если на объекте шпионажа соблюдается соответствующая политика безопасности. Более подробно о возможных контрмерах мы поговорим немного позже.

И наконец, окончательное решение по началу либо отмене операции принимается, исходя из конкретного экономического расчета. В определенных обстоятельствах возможная прибыль от операции может не оправдывать экономических и временных затрат на ее проведение либо существующего риска.

## Шпионская тактика

В последующих главах нашей книги вы еще не раз встретите параграфы с подобным названием: в них будут описываться действия, предпринимаемые шпионами для получения доступа к конфиденциальной информации. Достаточно часто мы будем просить вас поставить себя на место шпиона, чтобы лучше понять ход мыслей противника. В некоторых случаях вы должны будете притвориться хорошим парнем, в других ситуациях – очень плохим. Только научившись думать как шпион, вы сможете построить эффективную систему защиты.

## Шпионские игры

Первое, что вам понадобится сделать в данной ролевой игре, это представить себя в роли консультанта компании, специализирующейся на тестовых проникновениях в закрытые компьютерные системы. Подобные

тестирования проводятся для оценки физической или компьютерной защищенности систем. Вооруженные силы и правительство успешно применяют подобный вид тестирования в течение многих лет для доступа к секретным объектам, представляющим собой радиационную угрозу военным учреждениям либо закрытым сетям. «Команды тигров» или «красные команды» занимаются целенаправленными атаками против секретных объектов или компьютерных сетей для проверки возможности незаметного проникновения и оперативности реагирования. После проведения операции пишется отчет, в котором подводятся итоги, указываются сильные и слабые места систем безопасности и необходимые контрмеры для предотвращения подобных атак в будущем. Проникновение в компьютерные сети с целью проверки их устойчивости против взлома в последнее время набирает обороты и среди частных фирм, поскольку коммерческие компании не меньше, чем правительство, заинтересованы в защите своих секретов от взломщиков-кракеров.

Итак, ваша цель – подразделение по подготовке специалистов в сфере продаж компании, занимающейся разработкой программного обеспечения. Офис компании расположен в шестиэтажном здании в нескольких километрах от штаб-квартиры корпорации. Вице-президент по продажам обеспокоен тем фактом, что их конкуренты каким-то образом узнали о готовящемся выходе новых продуктов и воспользовались полученной информацией для получения конкурентных преимуществ. Отдел продаж нанял представителей вашей компании, чтобы провести внутреннее расследование. В то время как другая команда занялась поиском уязвимых мест в защите компьютерной сети, вашей задачей является физически проникнуть в само здание и попытаться попасть в офис отдела продаж.

Поскольку вы проникаете в здание хотя и тайно, но санкционировано, вас в принципе не должна беспокоить возможность поимки – разве что, дабы сохранить уважение коллег, никто из которых до сих пор не попадался в ходе подобных операций.

Так как для вас это ново, перед тем как начать планирование предстоящей операции, уделите время изучению чужого опыта. Внимательно прочтите следующие параграфы: быть может, у вас появятся собственные оригинальные идеи.

## **Проникновения, санкционированные правительством: взгляд изнутри**

Подобные проникновения называют тайными именно потому, что широкой публике о них мало что известно. Скорее всего, причина в том, что люди, которые занимаются подобными операциями (военные, работники правоохранительных органов и разведывательных служб), любят беречь в тайне свои «источники и методы». Подумайте сами – если технология проведения таких операций будет раскрыта, «плохие парни» могут либо сами воспользоваться этой методикой, либо принять соответствующие контрмеры. (Разумеется, требование держать детали таких операций в

тайне себя оправдывает, однако нередко случается так, что соблюдение мер предосторожности означает полную неосведомленность законопослушных граждан и компаний о происходящем, делая их беззащитными против нелегальных вторжений.)

Вес Сверинген, работавший агентом ФБР с 1951-го по 1977 год и принимавший участие во многих несанкционированных вторжениях по заданию Бюро, написал обличительную книгу под названием «*Секреты ФБР: разоблачение агента*». В своей книге и в последующих интервью средствам массовой информации он поведал подробности «базовой подготовки операций по тайному проникновению». Хотя эта информация кажется несколько устаревшей и касается преимущественно проникновения в частные дома граждан, однако многие из описанных в книге приемов применяются и по сей день, так что книга может служить в качестве практического пособия по проникновению в чужие дома, офисы, предприятия и другие учреждения.

## ОПЕРАТИВНЫЕ ГРУППЫ

ФБР, правоохранительные органы и разведуправления обычно используют для проведения операции несколько групп, каждая из которых отвечает за свой фронт работ. Хотя нередко всю операцию в состоянии осуществить единственный агент, намного безопаснее привлечь к участию несколько человек для выполнения различных задач. Для проведения операции могут быть задействованы до пяти отдельных команд, а именно:

- **Команда надзора**, члены которой обязаны незаметно следить за интересующими ФБР людьми (проживающими в здании, являющимся целью операции, либо посещающими его), когда те выходят за пределы здания. Команда надзора должна сообщать другим командам о местонахождении и перемещении этих людей, чтобы те не могли неожиданно вернуться и застать агентов.
- **Внутренняя команда** (команда проникновения). Именно она занимается проникновением в помещения, установкой подслушивающей аппаратуры либо сбором доказательств. В зависимости от поставленных целей в состав команды могут быть включены специалисты по электронному наблюдению, по компьютерам, по фототехнике и другим отраслям.
- **Транспортная команда**. Эта команда привозит команду проникновения в выбранное для начала операции место, где появление агентов пройдет наименее заметно, а по окончании операции увозит агентов восвояси.
- **Команда наблюдения**. В обязанности команды входит наблюдение за окрестностями атакуемого объекта, дабы вовремя предупредить о приближении людей или действиях соседей, которые могут привести к срыву операции.

- **Команда управления.** Отвечает за руководство операцией и координирование действий агентов на расстоянии. Иногда члены этой группы также принимают участие в наблюдении за резиденцией.

## Тактика: секретные команды ФБР по проникновению

В 1996 году в книге «Над законом» ее автор Дэвид Бернхем кратко описал программу работы тайных подразделений ФБР по проникновению. Эта программа включала в себя подготовку высококвалифицированных агентов, которые специально обучались тактике тайных проникновений в различные места для сбора доказательств и установки подслушивающих устройств. Вообще, ведением наблюдения в ФБР официально занимаются два отдела: SOG (Special Operation Group) – Специальная оперативная группа, отвечающая за физическое и электронное наблюдение, и TTA (Technically Trained Agents) – Техническое подразделение, специалисты которого обладают соответствующими знаниями в плане электронного наблюдения и компьютерными навыками, необходимыми для проведения этих операций.

Хотя ФБР отказывается обсуждать программу секретных проникновений, исходя из различных свидетельств, ставших известными широкой публике, мы знаем, что данная программа доказала свою эффективность. В нашумевших делах, связанных со шпионажем, как, например, в случае с Элдриком Эймсом, Робертом Хансеном, Анной Белен Монтес и Брайаном Рейганом, так и в ходе уголовных расследований, например, в деле Никодермо Скарфо, ФБР осуществляло операции по проникновению в жилые помещения, офисы и транспортные средства с целью сбора доказательств против подозреваемых.

Все эти операции, инициируемые со стороны ФБР, Администрации по контролю над соблюдением законов о наркотиках и других федеральных бюро, выполнялись в соответствии с судебными санкциями.

- Отраслевой отдел ФБР или другое федеральное агентство, собирающееся заняться электронным наблюдением, сообщают о своих намерениях в судебные органы.
- Технические специалисты тайно изучают целевой объект (здание), собирая архитектурные чертежи и схемы.
- Команда проникновения подготавливает необходимые приспособления и аппаратуру, включая специально разработанные средства наблюдения.
- Осуществляется операция по проникновению.

Программа секретного подразделения ФБР по проникновению активизировала свою деятельность после событий 11 сентября. В бюджете на 2003 год ФБР запросило финансирование в размере 12 162 000 долларов на так называемые тактические операции. Предназначение этой статьи бюджета описывается следующим образом: «...для повышения подготовленности ФБР в плане выполнения обысков и для своевременного реагирования на технологические изменения путем проведения исследований, разработок и проектирования».

Вдобавок ФБР заинтересовано в развитии своих программ подготовки технических специалистов, поэтому соответствующая строчка в бюджете имеет вид: «В связи с широким внедрением цифровых коммуникационных технологий, их распространением среди частных лиц и компаний, а также из-за повсеместного использования систем шифрования ФБР брошен серьезный технический вызов. Террористы активно используют современные технологии для прикрытия своей незаконной деятельности, не давая правоохранительным органам возможности обнаружить себя. В поданном на утверждение бюджете 2003 года предполагается выделение 10 027 000 долларов на оплату услуг технических специалистов, администрирование всех функций наблюдения и обеспечение необходимым оборудованием существующих технических подразделений. Сюда же включены расходы на обучение и повышение квалификации технических подразделений, которые позволяют поддерживать на должном уровне навыки специалистов, а также быстро и эффективно реагировать на бурное развитие техники».

С принятием Патриотического Акта многие гражданские группы по защите свобод всерьез обеспокоились увеличением полномочий правоохранительных органов в плане проведения наблюдений и слежки, что, как видно из истории, всегда приводило к злоупотреблениям в данной области. Со времен Второй мировой войны и до середины 1970-х годов ФБР осуществило сотни, если не тысячи тайных рейдов, направленных против политиков, активистов, организаций по защите гражданских прав и свобод и обычных граждан страны. Только время покажет, повторится ли эта история снова.

Количество людей в каждой команде зависит от поставленной задачи и конкретных обстоятельств. К примеру, в простом случае на одного человека могут быть возложены обязанности по управлению операцией и ведением наблюдения за объектом, тогда как в ходе серьезной операции только для наблюдения иногда бывают задействованы несколько групп, чтобы контролировать объект как с земли (пешими и на транспорте), так и с воздуха.

## АНАЛИЗ И ПЛАНИРОВАНИЕ

После принятия решения о необходимости проведения тайного проникновения (и выдачи санкции на проведение операции со стороны суда), агенты немедленно, но без лишней спешки, приступают к подготовке операции. Часто в рамках подготовки к такой операции требуется потратить немало времени на изучение обстановки и продумывание детального плана. Между потенциальным риском неудачи и качеством планирования существует обратная зависимость: чем тщательнее вы подготовитесь к рейду, тем меньше риск его срыва, и наоборот. Хотя свести вероятность риска к нулю просто невозможно, детальное изучение и разработка плана помогут повысить ваши шансы на успех.

На этапе анализа и планирования операции вы должны располагать следующей информацией:

- **Предстоящая цель.** Вам необходимо определить, против кого будет направлена данная операция. Затем на этого человека готовится досье, составленное по материалам наблюдений и записей, куда включаются его обычные маршруты передвижения, регулярно посещаемые встречи и мероприятия, привычки и поведенческие стереотипы, знание которых помогает легко следовать за выбранным объектом.
- **Тип цели и место работы.** Проникновение в жилище субъекта обычно производится во время его пребывания на рабочем месте. Поэтому вам необходимо знать, где и по какому графику он работает.
- **Соседи и постоянные визитеры.** Перед непосредственным началом операции команда агентов должна убедиться в отсутствии в доме посторонних лиц. Нужно выяснить количество людей, проживающих в одном здании с объектом наблюдения, на каждого из которых также необходимо составить краткое досье.
- **Домовладелец** (если объект не имеет собственного дома). Благодаря мистическому ореолу, окружающему ФБР, люди часто идут навстречу агентам, даже если у тех отсутствует соответствующий ордер. Отдельные законопослушные домовладельцы могут запросто позволить агентам войти в снимаемую объектом собственность.
- **Информация о самом помещении,** в которое необходимо проникнуть. Сюда относятся фотографии и письменные описания здания, сведения об установленных дверях, замках, освещении, планы дома, наличие домашних животных, соседей и любая другая информация, которая может пригодиться при разработке операции. Причем все эти сведения должны быть собраны скрытно, дабы интересующий вас объект не заподозрил, что он находится под наблюдением.

После анализа имеющейся информации составляется план решения конкретной задачи, например установки «жучка» либо тайного копирования информации с компьютера. Затем разрабатывается запасной план на случай непредвиденных обстоятельств. Определяются средства и оборудование, необходимые для проведения операции; требуемое количество агентов, включая специалистов в конкретных областях; составляется список агентов в составе команды проникновения.

## ПРОБНАЯ ОПЕРАЦИЯ

Только практика позволяет совершенствоваться, а ведь ФБР требует, чтобы все операции по тайному проникновению проходили как можно более гладко во избежание разоблачения. Поэтому следующим этапом на пути подготовки операции является проведение пробного рейда. Обычно пробный рейд происходит следующим образом:

- Команда надзора следует за объектом и другими людьми, проживающими в этом доме. В зависимости от обстоятельств не менее двух агентов задействуется для слежки за каждым человеком. Это необходимо для того, чтобы один агент мог подменить другого, в случае если первый окажется разоблачен.
- Все члены команды надзора постоянно поддерживают радиосвязь между собой. В случае потери связи операция прекращается. (Чтобы избежать подслушивания переговоров, все сеансы радиосвязи проводятся с использованием предварительно оговоренных кодов, в тех случаях когда шифрующие радиопередатчики недоступны.)
- Операция по пробному проникновению начинается после того, как объект и все его соседи по жилплощади покидают помещение.
- Агенты делают фальшивые звонки соседям, которые могут видеть вход в здание, дабы отвлечь их от проводимой операции. Точное время звонков определяет руководитель операции, также выступающий в роли наблюдателя.
- Люди, остающиеся снаружи (члены команды управления), выводят «внутреннюю команду» на позицию и информируют команду надзора о непосредственном начале операции. Во время пробного проникновения используется команда из двух человек, один из которых взламывает замок и отключает сигнализацию, а другой поддерживает связь по радио с другими агентами. (К участию в пробном рейде, в зависимости от обстоятельств, могут быть дополнительно привлечены технические специалисты.)
- Транспортная команда, которая в данном случае может состоять из единственного агента, подвозит «внутреннюю команду» в заранее определенное место, где высадка агентов из машины должна пройти незамеченной, после чего немедленно покидает место будущей операции.

- «Внутренняя команда» подбирается ко входу и пытается определить явные признаки сигнализации. В случае отсутствия сигнализации либо после ее успешного отключения, команда проникает в помещение. (Если обнаруженную сигнализацию невозможно отключить на месте, команда сообщает об этом, операция прекращается, и данный вопрос разрабатывается при подготовке последующих операций.) Затем человек из внутренней команды, отвечающий за переговоры с наружной группой, сообщает о моменте проникновения внутрь помещения. (При общении по радио агенты нередко используют в качестве кодов бейсбольный жаргон, например, «игроки на поле» означает, что команда проникла в нужное место. Разумеется, как правило, для разных групп коды отличаются.)
- Пробный рейд начинается с поиска во всех помещениях кого-либо, чье присутствие в доме могло пройти незамеченным. «Внутренняя команда» передает сообщения агентам снаружи по мере своего продвижения по зданию. В ходе рейда могут быть сделаны фотографии доказательств или документов для подготовки к основной операции (особенно когда речь идет об установке подслушивающих устройств; возможно, понадобится изготовление «жучка» специальной формы, который можно было бы встроить в некоторую деталь интерьера, к примеру). С учетом того, что внутренней команде необходимо некоторое время для эвакуации, команда надзора посредством постоянно работающей связи должна своевременно предупредить «внутреннюю команду» о возвращении хозяев домой.
- Внутренняя команда отчитывается о своих действиях через каждые несколько минут, и как только дело будет закончено, на место операции вызывается транспортная группа.
- После того как команда проникновения освободит помещение, руководитель операции связывается со всеми агентами, ведущими слежку за жителями дома, сообщает об окончании операции и необходимости возвращения их в офис.

## ОСНОВНАЯ ОПЕРАЦИЯ

После завершения пробного рейда команда проникновения рассказывает об увиденном; все возникшие в ходе проникновения неувязки учитываются при подготовке основной операции, разработка которой начинается с этого момента. Как правило, основная операция разрабатывается в соответствии со схемой пробного рейда, с добавлением, при необходимости, дополнительных технических специалистов в команду проникновения.

Успешность и тайность совершения проникновения требует определенных навыков, опыта и высокой организации. Не каждая организация обладает такими ресурсами и навыками для выполнения подобных операций. Даже ФБР располагает ограниченным числом агентов, достаточно

квалифицированных для выполнения этой работы. Из-за значительных временных затрат и относительной дороговизны операций тайные проникновения проводятся только в тех случаях, когда другие методы сбора доказательств исчерпали себя либо на них нельзя рассчитывать.

## Использование уязвимых мест

Теперь, когда вы узнали, как действуют профессионалы, давайте вернемся к нашему тестовому сценарию проникновения и подумаем над тем, как спланировать и реализовать операцию против клиента вашей компании по производству программного обеспечения. Мы не станем вдаваться в детали по поводу того, как обмануть сенсоры сигнализации либо взломать надежный замок фирмы Medeco (хотя в данном параграфе будут приведены некоторые ссылки на интересующую вас информацию). Вместо этого мы сосредоточим наше внимание на изучении основных, часто встречающихся уязвимых мест. Везде, где вы встретите текст, выделенный курсивом, речь будет идти о чем-то, непосредственно связанном со сценарием проникновения.

В известном смысле, тайные проникновения в здания и офисы являются аналогом сетевых атак хакеров, нацеленных на компьютерные системы: вы ищите слабые места и анализируете, как можно ими воспользоваться. Однако физические проникновения организовать намного сложнее, поскольку необходимо преодолеть большее количество уровней защиты, для обхода которых недостаточно только программных средств.

## Анализ и планирование операции

Подобно старому правилу шести «п» – «правильная предварительная подготовка предотвращает плачевые последствия», существует также правило шести «т» (в английском варианте это target, time, talk, tools, tactics, tale), связанных с планированием секретных проникновений.

В русском варианте эти т-правила звучат так:

- **Цель.** Против кого или чего будет направлена данная операция. Вы всегда должны четко представлять себе цели и задачи операции и заранее подготовить всю доступную информацию о ней. Эти сведения могут включать личные привычки жителей, разновидность установленной системы сигнализации, модель дверного замка, тип компьютера, используемого объектом.
- **Время.** Поскольку, как правило, максимальная длительность тайного проникновения ограничена, необходимо определить, сколько времени может занять каждая часть операции. Хотя время и не самая важная, но все же достаточно существенная характеристика плана.

- **Переговоры.** Под переговорами подразумевается радиосвязь с использованием секретных кодов либо шифрования, а также проверка того, что все члены команды получили детальные инструкции и ясно представляют свою роль и ответственность в рамках операции.
- **Средства.** Вы должны убедиться в том, что в вашем распоряжении имеются все необходимые инструменты. Для проведения компьютерного шпионажа вам нужен диск с программными утилитами, позволяющими обходить защиту операционной системы и приложений, анализировать содержимое файлов или же копировать информацию с жестких дисков (и других электронных носителей информации). Вдобавок вам может понадобиться аппаратное или программное обеспечение для мониторинга клавиатуры или же перехвата сетевых пакетов.
- **Тактика.** Тщательно продуманный план обязательно должен учитывать вероятность возникновения непредвиденных обстоятельств и предусматривать вариант действий на этот случай.
- **Прикрытие.** Вы всегда должны иметь наготове хорошо отрепетированное правдоподобное объяснение ваших действий на случай вашего разоблачения.

*Пришло время применить некоторые ваши знания и составить сценарий тайного проникновения на заданный объект. Для проведения пробного рейда вам выделили двух помощников. Об объекте проникновения вами была собрана следующая информация:*

- *Офисное строение имеет два входа: через главный холл на первом этаже и через подземный гараж. Чтобы проникнуть через любой из входов, вам требуется иметь электронные пропуска для открытия замков. Замки с устройствами для считывания электронных пропусков защищают лифты в нерабочие часы и закодированы с учетом информации о месте нахождения вашего офиса, то есть, если у вас пропуск человека, работающего на четвертом этаже, лифт поднимет вас только на четвертый этаж. Двери лестничной клетки находятся под сигнализацией и всегда закрыты для доступа извне, кроме случаев срабатывания пожарной сигнализации.*
- *В рабочее время, т. е. по будним дням с 7:30 до 18:00, в главном вестибюле работает консьерж. Если вы не являетесь сотрудником какого-либо из офисов в этом здании, консьерж может либо провести вас через закрытые двери (опять-таки, воспользовавшись электронным пропуском), либо позвонить по телефону, чтобы кто-нибудь из работающих в здании спустился и провел вас к месту назначения.*
- *В нерабочее время в главном вестибюле находится охрана. Место дежурного оборудовано тремя мониторами, к которым*

подключены две видеокамеры в противоположных сторонах подземного гаража и одна камера, расположенная перед въездом на парковку. В вестибюле дежурит только один охранник, который совершает обход здания раз в час. В перерывах между обходами он сидит в дежурном помещении, смотря телевизор или играя в компьютерные игры.

- Уборка помещений производится каждый будний день около 22:00 наемным персоналом, работающим по контракту.
- Отдел обучения продажам занимает весь четвертый этаж административного здания. Все сотрудники отдела имеют отдельные, запираемые на ключ кабинеты. Большинство сотрудников находится в достаточно солидном возрасте, имеют семьи, и потому редко задерживаются на рабочем месте, в отличие от сотрудников других отделов.

Вы начинаете думать о том, какая еще информация может понадобиться и какие способы физического проникновения в офис являются наиболее удобными.

## Проникновение в офис

Очевидно, что для того чтобы начать поиск интересующей вас информации либо доказательств, вам необходимо вначале получить физический доступ к компьютеру. В некоторых случаях выполнение поиска может оказаться вполне тривиальной задачей либо, наоборот, делом весьма непростым, поскольку вам понадобится обойти несколько уровней физической защиты, чтобы получить доступ к нужным данным. В нашем примере необходимо проникнуть через главный вход, подняться по лестнице или на лифте, проникнуть в нужный офис и, наконец, взломать двери кабинета.

Вообще-то, для проникновения в нужное помещение используется три способа. В порядке увеличения риска при реализации того или иного подхода их можно расположить так: использование «своих людей» в офисе, социотехника (подкуп/шантаж/уговоры сотрудников) и банальный взлом с проникновением.

## ИСПОЛЬЗОВАНИЕ «СВОИХ ЛЮДЕЙ»

Под своими людьми подразумеваются клерки, которые на самом деле работают в компании; людей, проживающих в этом здании либо имеющих другие реальные причины находиться в том месте, куда вы намереваетесь проникнуть. Когда дело касается доступа к секретной информации, данный способ является самым лучшим, поскольку свои люди:

- уже имеют доступ к офису и информации,
- они знают или просто знакомы с другими сотрудниками в этом офисе,

- вы намного меньше рискуете, чем в случае отправки на задание «чужаков».

Когда разведки разных стран мира пытаются завербовать людей для шпионажа против их родной страны, они делают ставку на Деньги, Идеологию, Компромат и Эго, которые вместе или по отдельности могут служить мощными мотиваторами, чтобы заставить человека стать шпионом. В нашей ситуации к сотрудникам, которые могут представлять интерес для целей вербовки, относятся следующие типы:

- Недовольные сотрудники.** Имеются в виду служащие компании, не добившиеся продвижения по службе, подвергшиеся дисциплинарным наказаниям либо пострадавшие в результате недавнего сокращения заработной платы и льгот.
- Морально уязвимые сотрудники.** Сотрудники с огромными долгами, имеющие наркотическую или алкогольную зависимость, любовные приключения на стороне, психические проблемы либо проблемы во взаимоотношениях с коллективом.

## Разоблачения: шпионское мышление

Роберт Хансен стал одним из самых знаменитых шпионов в истории Америки. До того как его разоблачили в 2001 году, высококлассный агент ФБР продавал в течение 20 лет национальные секреты Советскому Союзу, а потом и России, заработав на этом более 1,4 миллиона долларов наличными и в драгоценных камнях.

Хансен также стал первым шпионом, который был разоблачен из-за экстенсивного использования Интернета. Пользователь Linux, настоящий фанат новых технологий, он часто отсыпал запросы в группу новостей USENET по проблемам аппаратного обеспечения, устройствам системы глобального позиционирования, КПК, цифровым камерам (а также некоторые рассказы эротического содержания о своей жене). Хансен не растерялся с приходом эпохи компьютерных технологий, и поэтому никого не удивил тот факт, что с некоторого времени он начал передавать информацию русским под своим собственным именем или псевдонимом через внешне невинно выглядевшие сообщения USENET.

Запросы Хансена до сих пор хранятся в архивах USENET. Если вы хотите изучить ход мыслей шпиона, зайдите на сайт <http://groups.google.com> и задайте поиск по любым из электронных адресов Хансена: [hanssen@orion.clark.net](mailto:hanssen@orion.clark.net), [hanssen@nova.org](mailto:hanssen@nova.org), [hanssen@amelia.nas.nasa.gov](mailto:hanssen@amelia.nas.nasa.gov), [rphanssen@earthlink.net](mailto:rphanssen@earthlink.net) или [TBERRR1@aol.com](mailto:TBERRR1@aol.com).

- **Работники по контракту.** К ним относятся: уборщики, охрана, консультанты или ремонтный персонал, не столь лояльные к фирме, как сотрудники, занятые полный рабочий день.

Хотя вербовка шпионов путем подбора правильных мотивов традиционно применялась в организации шпионажа на уровне государств, она не хуже работает и на примере корпоративного экономического шпионажа.

«Treason 101» (измена 101) – весьма любопытный веб-ресурс, поддерживаемый военной Службой Безопасности США. Здесь рассказывается о том, почему люди становятся шпионами, обсуждаются последние нашумевшие дела, связанные со шпионажем, приводятся примеры угрозы со стороны завербованных «своих людей». Кроме того, здесь вы сможете узнать, как же удается поймать шпионов, прочесть демографическую и статистическую информацию о людях, избравших для себя путь шпиона. Для этого рекомендуем вам посетить веб-сайт по адресу:

[www.dss.mil/training/csg/security/Treason/Intro.htm  
#Treason%20101.](http://www.dss.mil/training/csg/security/Treason/Intro.htm#Treason%20101)

## «ВЫТАГИВАНИЕ ИНФОРМАЦИИ» – СОЦИОТЕХНИКА

Термин, известный в сфере компьютерной безопасности как «социотехника», в шпионской терминологии называют «вытягиванием информации». Эта техника включает ряд приемов, позволяющих в ходе внешне невинной беседы незаметно выведать у собеседника нужные сведения.

Данная техника основывается на использовании простых слабостей человеческой натуры:

- Большинство людей хотят казаться вежливыми и полезными, поэтому не любят уклоняться от заданных вопросов, даже если их задает совсем незнакомый человек.
- Люди также любят показать себя важными и хорошо проинформированными, поэтому нередко говорят больше, чем следует.
- Людям нравится, когда их ценят и когда они чувствуют свою причастность к чему-то важному и полезному. Поэтому они становятся открытыми, когда хвалят их работу.
- Поскольку американской культуре свойственна открытость и честность, люди неохотно скрывают информацию, редко лгут или подозревают кого-либо в нечестных мотивах.

Применяемые опытным человеком приемы социотехники кажутся частью обычного социального или профессионального разговора и могут использоваться где угодно – на рабочем месте, во время проведения некоторого мероприятия, в ресторане, на конференции или же во время визита к кому-то домой. Определенные типы приемов можно считать абсолютно законными, когда шпион по кусочкам собирает информацию, полученную от разных людей, и использует ее как инструмент для получения доступа к секретным данным.

Приемы социотехники используются в телефонных разговорах (что намного безопаснее для вас) либо при личностном контакте. Вы можете, к примеру, разыграть из себя ремонтного рабочего, работника службы доставки, представителя коммунальной службы, сотрудника, то есть того, кто может достаточно близко подобраться к цели (при этом вам необходимо привести себя в соответствующий вид и запастись фальшивыми пропусками, дабы впоследствии благополучно выбраться из офиса). Личное и телефонное общение с использованием приемов социотехники может являться частью общего плана получения доступа к нужной информации.



Всестороннее обсуждение приемов социотехники проведено в книге Кевина Митника и Уильяма Саймона «Искусство обмана: контроль человеческого фактора в безопасности» (издательство Wiley, 2002).

## ПРОНИКНОВЕНИЕ СО ВЗЛОМОМ

Последний, наиболее рискованный способ получения доступа к интересующей информации – проникновение со взломом. Данная операция подразумевает взлом дверных замков, кражу ключей, отключение сигнализации и применение других воровских методов. Главное отличие от обычной кражи со взломом состоит в том, что рядового вора в первую очередь интересуют материальные ценности и меньше всего беспокоят признаки совершенного преступления, тогда как шпион, как правило, не желает оставлять видимых следов своего присутствия, чтобы жертва не догадалась о ведущемся за ней наблюдении. (В некоторых случаях проникновение с целью шпионажа маскируется под обычную кражу со взломом, чтобы отвлечь внимание от настоящей цели проникновения.)

Электронные пропуска, кнопочные дверные замки, защищенные от несанкционированного доступа системы сигнализации, охранники, биометрические системы идентификации – все эти меры безопасности, применение которых начиналось с объектов повышенной секретности, приобретают все большее распространение. Наличие подобной защиты бросает серьезный вызов шпионам. В очередном варианте бюджета, поданном на рассмотрение в Конгресс, ФБР запросило дополнительные денежные средства на проведение исследований и разработок, аргументируя это тем, что осуществлять тайные проникновения в административные и жилые помещения из-за бурного развития систем безопасности становится все сложнее.

Когда дело доходит до проникновения со взломом, в защите нуждаются не только двери и окна. В сложных операциях, связанных с серьезными преступлениями, специальные секретные подразделения могут проникать даже через стены, потолки или пол. Затем команды высококлассных специалистов по восстановлению могут быстро заделать повреждения, придав интерьеру первоначальный вид, как будто никаких разрушений и не было.



Если вас интересует, как работают замки (и как их взламывать), начните с изучения ответов на часто задаваемые вопросы в группе USENET *alt.locksmithing* по адресу <http://www.faqs.org/faqs/locksmith-faq/>. Здесь вы найдете массу интересной информации, включая ссылки на пользующееся дурной репутацией «руководство по взлому замков» от Массачусетского технологического университета *“MIT Guide to Picking Locks”*.

Если вы хотите узнать больше, обратитесь к книге Марка Тобиаса *«Замки, сейфы и безопасность»*, англоязычная версия которой доступна как в печатном виде, так и на CD-ROM. Это иллюстрированное издание объемом в 1400 страниц представляет собой исчерпывающий справочник по замкам и сейфовым системам и способам их взлома. Книга эта стоит недешево, поскольку она предназначена для профессионалов своего дела. Получить дополнительную информацию по книге и просмотреть доступную для поиска сокращенную онлайновую версию вы можете по адресу [www.security.org](http://www.security.org).

*Возвращаясь к нашему сценарию, подумаем над тем, какой метод следует вам избрать для проникновения в здание? Существует множество различных вариантов, однако при подготовке операции можно воспользоваться следующим обстоятельством.*

*В качестве дополнительных льгот сотрудникам компании предлагается членство в клубе здоровья, принадлежащем компании. В результате наблюдения вы выяснили, что один из менеджеров по продажам занимается в этом клубе каждый день после работы. (Его имя и фотографию вы нашли в статье журнала, выданной поисковым сервером на запрос «отдел обучения продажам». Известно также, что у него даже имеется зарезервированное место для стоянки, с написанным на нем именем, поэтому проследить за ним и выяснить его привычки не составило особого труда для вашего коллеги.) Вы добились временного членства в клубе и как будто случайно завели разговор с этим менеджером по продажам – естественно, не говоря, кто вы такой на самом деле. Выяснив, что он любит играть в теннис, в следующий раз вы прихватили с собой ракетку, чтобы сыграть пару матчей. Впереди три выходных дня, и он рассказывает вам о планируемой поездке в Британскую Колумбию, чтобы покататься на лыжах.*

*Менеджер по продажам и не подозревает о том, что вы собираетесь украсть его пропуск из раздевалки клуба за день до поездки, пока он будет находиться в душе. Вы предполагаете, что, поскольку его мысли в это время будут всецело заняты предстоящей поездкой, он либо вообще не заметит исчезновения своего пропуска, либо не станет беспокоиться о пропаже до возвращения из путешествия во вторник.*

*Итак, вы благополучно выкрали его пропуск и в субботу утром, в первый день трехдневных выходных, высадившись в квартале от офиса по продажам, пешком направились к парковочному въезду. Рядом с вами очаровательная спутница, а у вас в кармане находится настоящий украденный пропуск и его подделка с вашей фотографией, на вид неот-*

личимая от настоящего пропуска. Вы пригибаете голову, чтобы не попасть в поле зрения наблюдательной камеры, доставая настоящий пропуск и проводя его через дверной замок. Двери открываются, вы проникаете на территорию парковки, а затем точно так же используете пропуск, чтобы войти в лифт и подняться на четвертый этаж. Оказавшись внутри, вы прячете украденный пропуск в карман и прикрепляете на свой пиджак поддельный пропуск с вашей фотографией. Вы и ваша спутница экипированы миниатюрными радиопередатчиками с практически незаметными наушниками. Таким образом вы постоянно поддерживаете связь с людьми снаружи, наблюдающими за входом в здание. Ваши люди следят за парадным входом и охранником в вестибюле, читающим газету.

## Документирование обстановки

После успешного проникновения в помещение, перед началом обыска нужно задокументировать обстановку. Вам необходимо записать все, что имеет отношение к цели проникновения (эти записи, естественно, могут быть использованы против вас в качестве улик в случае вашей поимки). Можно применять следующие приемы документирования:

- **Описательный.** Полицейских учат вести записи всего происходящего в ходе операции, поскольку, при необходимости дачи показаний в суде, начинает действовать правило «чему нет письменных подтверждений, того никогда и не было». Вам следует придерживаться того же принципа и делать письменные заметки о любой найденной вами информации или доказательствах, будь то в целях расследования или просто для памяти.
- **Фотографический.** Вам необходимо также сфотографировать кабинет или комнату, в которую вы проникли, для того чтобы использовать фотографию в качестве доказательств, и не выдать своего присутствия. Если вы что-либо передвигали, вы обязаны вернуть этот предмет на свое место. Хотя большинство людей не слишком наблюдательны, человек может что-то заподозрить, если заметит отсутствие или перемещение своего любимого предмета. Несмотря на то, что цифровые фото- и видеокамеры неплохо подходят для документирования обстановки, предпочтительнее использовать, например, фотоаппарат типа Polaroid, поскольку он позволяет вам сразу получить твердую копию, которую вы можете держать в руках для сравнения обстановки до и после операции.

*После того как вам удалось незаметно проникнуть в здание и подняться на четвертый этаж, что вы станете делать дальше? Здесь возможен следующий вариант развития событий.*

*Первое, что вам придется сделать, это пройти по коридорам, проверяя, не остался ли кто-то случайно в одном из офисов. Ваша спутница в*

это время остается сидеть на кушетке в холе, делая вид, что читает газету. Она молода, привлекательна, носит весьма свободную одежду и к тому же хорошая актриса. Если во время обхода ее увидит охранник, она может представиться вашей женой и сказать, что ожидает вас, поскольку вам понадобилось забрать из офиса некоторые документы для работы на дому. Затем ваша очаровательная спутница должна затеять с ним непринужденную беседу. Если в офисе появится кто-либо из сотрудников отдела продаж, она может сказать, что ее муж вообще-то работает на пятом этаже, но ей наскучило ожидать его, поэтому она решила побродить по зданию. В любом случае присутствие спутницы и ее действия дадут вам время закончить начатое, чем бы вы там ни занимались, а затем выйти к ней. В ее сумочку встроен небольшой микрофон с радиопередатчиком, чтобы вы могли постоянно ее слышать. (Если нас читает женщина, она может представить на месте женщины мужчину-актера.)

У вас с собой имеется набор отмычек для взлома замков, однако на этот раз они вам даже не понадобились. Двери большинства кабинетов оказались незапертыми. Вы делаете письменные заметки по этому поводу, отмечая также другие обнаруженные вами уязвимые места системы безопасности. Затем вы достаете небольшую цифровую камеру и начинаете снимать обстановку кабинета, фотографируя также книжную полку, с которой вы намерены начать осмотр.

## СБОР ИНФОРМАЦИИ

Главной целью тайного проникновения, как мы уже говорили, является сбор данных либо доказательств. В оставшейся части книги мы будем обсуждать многочисленные способы и примеры того, как это нужно делать, особенно если вы обладаете физическим доступом к компьютеру. В ходе планирования операции вам необходимо определить, какую цель вы ставите перед собой, – то ли вас интересует конкретная информация, то ли вы хотите найти что-нибудь, что может вам пригодиться.

Поскольку легче всего скопировать цифровую информацию, вам необходимо запастись различными видами цифровых носителей: начиная от целого жесткого диска для создания образа жесткого диска целевого компьютера до набора дискет или CD-RW для копирования отдельных файлов.

Даже если основной вашей целью является компьютерный шпионаж, не забывайте и о других возможных источниках информации. Потратьте время на осмотр стола, оргтехники и т. д. на предмет наличия клочков бумаги с записанными паролями либо другой секретной информацией. Все, что вы найдете, обязательно должно быть задокументировано. Следует осмотреть и другие места, где может находиться полезная для вас информация, например:

- мусорные корзины и контейнеры,
- ящики стола,

- картотечные шкафы,
- доски для записей,
- доски объявлений,
- настольные картотеки Rolodex,
- настенные календари,
- органайзеры.

*Компьютер вашей жертвы оказался включен, и вы видите на дисплее знакомый «хранитель экрана». Пошевелив мышью, вы попадаете на рабочий стол Windows Me. По счастливому стечению обстоятельств, перед вами оказывается открытый файл, описывающий программу обучения продавцов продажам продукта, поставки которого намечены на ближайшие полгода. Сбоку на мониторе прикреплен стикер с паролем. Вы достаете дискеты и начинаете копировать некоторые интересные файлы, одновременно просматривая содержимое незапертых ящиков стола. Кроме того, вы не забываете записывать все ваши действия и наиболее любопытные находки.*

## **ПРИВЕДЕНИЕ КАБИНЕТА В ПОРЯДОК И УХОД ИЗ ОФИСА**

Переписав информацию, за которой вы сюда пришли, необходимо навести после себя порядок, чтобы скрыть следы своего присутствия. Вы должны расставить все предметы в точности по своим местам, в чем вам помогут предварительно сделанные фотографии, поскольку человеческая память может подвести, особенно в стрессовых ситуациях.

Все, что вы принесли с собой, вы должны забрать. Если вы применяли специальные программные утилиты для копирования файлов на дискеты или CD-ROM либо для создания образа жесткого диска, все они должны быть удалены с целевого компьютера. Некоторые специалисты записывают все, что они приносили с собой, дабы не оставить в офисе ничего лишнего, что могло бы возбудить подозрение.

Последний этап операции по тайному проникновению заключается в том, чтобы покинуть здание, не привлекая к себе внимания. Причем эта часть операции не менее рискованна, чем проникновение вовнутрь, поэтому необходимо оставаться собранным до самого конца операции.

*Итак, вы собрали достаточно доказательства того, что физические меры безопасности офиса оставляют желать лучшего. Если кто-либо, работающий на ваших конкурентов, сможет проникнуть внутрь, он легко получит доступ к служебной информации, способной скомпрометировать вас перед конкурентами.*

*Вы просматриваете сделанные перед началом осмотра кабинета снимки, убеждаетесь, что все на месте. Затем дважды проверяете список вещей, которые вы принесли с собой, еще раз удостоверяетесь, что ваш мобильный компьютер, ручка, видеокамера, пять дискет и два CD-RW находятся в вашей сумке. Затем сообщаете вашей партнерше о своей готовности.*

Вы рассчитывали провести в офисе максимум полчаса, но уложились всего за 20 минут. Используя кодовые слова, вы сообщаете вашему коллеге снаружи о том, что вы направляетесь к лифту и спускаетесь в подвальный этаж. Он подбирает вас в квартале от офисного строения, после чего вы втроем возвращаетесь в офис, где вас тщательно опрашивают по выполненному заданию. Позднее вы заходите в клуб здоровья и оставляете пропуск менеджера по продажам в бюро находок, утверждая, что обнаружили его в раздевалке.

На следующий день вы начинаете работу над отчетом обо всех обнаруженных вами уязвимых местах системы безопасности, включая упоминание о стикерах с паролями, прикрепленных к монитору, включенном компьютере с открытой служебной информацией, незапертых дверях кабинета и ящиках картотеки. К отчету вы прилагаете распечатанные копии файлов программы продаж в качестве доказательств. Ваш босс должен быть вами доволен.

## Контрмеры

Как же вы намерены предотвращать тайные проникновения? В этом параграфе мы поговорим о контрмерах общего плана, которые вы в состоянии предпринять в роли руководителя компании по производству программного обеспечения. (В других главах книги возможные контрмеры будут рассматриваться более подробно, однако поскольку тема физической безопасности слишком объемная, чтобы ее можно было изложить в одной главе, то здесь мы приведем только общие концепции. Кроме того, обратите внимание на ряд ссылок на онлайновые и книжные источники, из которых вы сможете почертнуть дополнительную информацию.)

Одна из главных ошибок, которую часто допускают сетевые администраторы, состоит в поддержке сетевых мер защиты информации при отсутствии должных мер безопасности против физического проникновения.

Если ваша оценка риска выявляет реальную угрозу проникновения, которое может привести к разглашению секретной информации, это должно послужить вам стимулом для укрепления физических мер безопасности в вашем жилище или офисе. Даже если вы не считаете себя потенциальной жертвой несанкционированного проникновения, вам не помешает провести проверку вашей системы безопасности на предмет наличия слабых мест при помощи заказного пробного проникновения.

## Физическая безопасность

К физической безопасности относится все, что касается охраны помещения, в котором размещен компьютер, электронных и других накопителей либо сетевого оборудования (кабелей, коммутаторов и маршрутизаторов) от природных катаклизмов, внешних условий (пожаров, наводнений или

ураганов), несчастных случаев, случаев саботажа и шпионажа. Когда речь заходит о шпионаже, физические меры безопасности служат одной или нескольким из перечисленных ниже целей:

- **Препятствование.** Любая мера, реализация которой препятствует физическому проникновению, например, охранники, видеокамеры наблюдения, освещение, либо системы сигнализации. Насколько эффективной окажется данная мера препятствования, зависит от того, насколько решительным является шпион.
- **Обнаружение.** Любая мера, дающая возможность обнаружить несанкционированное вторжение, например, сенсоры сигнализации, мониторы, подключенные к видеокамерам наблюдения, либо охрана, проверяющая пропуска на входе.
- **Защита.** Любая мера, предотвращающая либо затрудняющая проникновение злоумышленника внутрь здания, будь то замки, бронированные двери или звуковая сигнализация. Говоря о контрмерах, следует заметить, что время в данном случае работает на вас; и чем больше времени придется затратить взломщику, чтобы проникнуть в помещение и выполнить свою миссию, тем выше вероятность того, что он откажется от своих замыслов или будет пойман.

Исходя из указанных целей, все физические меры безопасности можно поделить на несколько категорий:

- **Контроль доступа.** К этой категории относятся меры безопасности, направленные на контролирование доступа в здание различных лиц. Персональные пропуска или жетоны, различные биометрические устройства вроде сканеров для проверки отпечатков пальцев, считающие устройства для электронных пропусков (с помощью которых могут отпираться двери) – все это может выступать в качестве компонентов системы по контролю доступа в помещение.
- **Электронные системы безопасности.** Подобные системы сигнализируют о проникновении злоумышленников на ранних этапах операции. Обычно эти системы безопасности оборудованы различными сенсорами (такими, как датчики перемещения, электромагнитные детекторы или детекторы давления), связанными с сигнализацией. В качестве оповещения о срабатывании сигнализации могут служить звуковые сирены или звонки, либо же сигнализация может срабатывать бесшумно, оповещая полицию либо частную охранную компанию. Системы видеонаблюдения, передающие информацию по кабельным сетям, также могут использоваться для наблюдения за помещениями в здании.

- **Архитектурные особенности здания.** Некоторые архитектурные элементы также способны повысить уровень безопасности (бронированные двери; стены, возвышающиеся над потолочными перекрытиями; вентиляционные каналы, слишком узкие для того, чтобы через них мог пролезть даже ребенок, и продуманная прокладка кабелей, ограничивающая доступ к ним со стороны неавторизованного персонала).
- **Охранники.** В роли охранников выступают специально подготовленные люди, чьей основной задачей является наблюдение за входами, камерами слежения и выполнение регулярных обходов здания.
- **Освещение.** Освещение подразумевает наличие снаружи здания светильников, освещдающих входы, что затрудняет задачу шпиона по проникновению в темное время суток.
- **Замки.** Эти системы включают установку безопасных замков у входов в здание и отдельные помещения, а также запирание на ключ картотек, столов и сейфов.
- **Защитные барьеры.** Эти барьеры выступают в качестве дополнительных препятствий на пути злоумышленника – например, высокие изгороди и ворота, образующие безопасную зону вокруг здания.

Как правило, в целях защиты применяется сочетание различных мер безопасности, формирующее интегрированную систему безопасности. Поддержание физических мер безопасности на должном уровне обходится недешево, поэтому следует предварительно оценить степень риска и вывести соотношение цена/защищенность, соответствующее уровню защиты, в котором вы нуждаетесь, перед тем как начать проведение защитных мероприятий.

Также не лишним будет потратить время на определение адекватности существующей системы безопасности. Это относится не только к мерам защиты против шпионажа, но и к планам восстановления информации в случае стихийных бедствий, если вы, к примеру, храните резервные копии за пределами офиса. (В этом случае необходимо позаботиться о соответствующей защите этих копий, поскольку они могут оказаться для злоумышленников более легкой добычей, чем информация в главном офисе.) Если вы не располагаете достаточным опытом в плане организации мероприятий для обеспечения физической безопасности, мы советуем вам посетить следующие онлайновые источники информации:

- **Американское общество обеспечения промышленной безопасности (ASIS).** ASIS является главной профессиональной ассоциацией специалистов по обеспечению корпоративной безопасности. Более подробно узнать об этой организации, а также увидеть другие интересные документы по безопасности вы сможете на веб-узле [www.asisonline.org](http://www.asisonline.org).

- **Путеводитель для покупателя систем безопасности.** Это издание, выпущенное обществом ASIS, представляет собой справочник практически по всем существующим на сегодняшний день системам безопасности и услугам, которые вы только можете себе представить. Бесплатная онлайновая версия и версия для печати размещены на веб-странице [www.sibgonline.com](http://www.sibgonline.com).
- **Меры физической безопасности «FM 3-19.30».** Данное руководство, предназначенное в первую очередь для военных, касается физических мер защиты, к тому же оно было совсем недавно пересмотрено. Хотя издание имеет четкую военную направленность, если у вас нет проблем со знанием акронимов, то многие базовые концепции и технологии, почерпнутые из этой книги, могут быть применены вами в мирное время. Электронную версию издания можно загрузить по адресу:  
[www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm](http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm). (Учтите, что, поскольку военное руководство и правительство любят менять адреса веб-сайтов, способных представлять угрозу национальной безопасности, вам могут потребоваться услуги поискового сервера, если вы столкнетесь с сообщением о том, что данный сайт больше не существует.)
- **Программа по замкам Министерства обороны.** Эта программа включает военные и правительственные спецификации, информацию по различным видам замков и другим физическим средствам защиты. Найти ее вы сможете в сети Интернет по адресу <http://locks.nfesc.navy.mil>.
- **Требования к физической безопасности секретной информации в соответствии со стандартами Управления национальной безопасности.** Этот несекретный документ 1979 года, касающийся вопросов обеспечения физической безопасности, утечка которого в свое время произошла через Интернет. Несмотря на то что он является относительно старым, из него вы можете почерпнуть немало интересной информации по обеспечению максимальной физической безопасности. Документ размещен в сети Интернет по адресу [www.cryptome.org/nsa-skif.htm](http://www.cryptome.org/nsa-skif.htm).

## Политика безопасности

Если бы перед вами встала необходимость выбрать единственную контрмеру для защиты против возможной шпионской угрозы, что бы вы избрали? Вооруженных охранников, устойчивую систему шифрования, биометрическую аутентификацию или, может быть, лазерную сигнализацию? Нет, наиболее эффективной, хотя и достаточно скучной, контрмерой является, прежде всего, четко оговоренная политика безопасности.

## Риски: путешествие за границу

Хотя большие корпорации обычно в состоянии обеспечить в своих офисах соответствующую политику безопасности, существует одна сфера деятельности, в которой сложно обеспечить защиту информации, и касается она командировок за пределы Соединенных Штатов.

Не забывайте о проведении многочисленных операций по промышленному и экономическому шпионажу, спонсируемых иностранными правительствами, которые направлены против заезжих бизнесменов. Подобные попытки шпионажа нередко смотрятся достаточно грубо: например, обыск номеров в отелях, незаконное копирование информации с оставленных без присмотра ноутбуков.

Национальная служба контрразведки ([www.ncix.gov](http://www.ncix.gov)) предлагает предпринимателям, планирующим деловую поездку за границу, ознакомиться со следующими мерами предосторожности во время поездки:

- Постоянно держите всю не подлежащую разглашению секретную документацию под вашим присмотром.
- Не используйте комнаты в гостиницах или помещения ресторанов для деловых переговоров. Если возможно, проводите все встречи на открытом воздухе, в местах, где вас сложно подслушать.
- Учтите, что ваш мобильный компьютер является главной целью для шпиона. Если вы не можете обойтись без него во время поездки, всегда перевозите его как ручную поклажу, не сдавая в багаж. Оставлять компьютер в комнате гостиницы или сейфе отеля – тоже не лучшее решение. Если вы вынуждены оставить мобильный компьютер в комнате, закройте его в портфеле, чтобы он не бросался в глаза потенциальному шпиону в первую очередь, пока вы отсутствуете или спите. Если возможно, скопируйте важные материалы на дискеты, CD-RW либо переносной жесткий диск, удалив их с диска компьютера еще перед поездкой. Во время поездки держите электронные носители всегда при себе, но отдельно от компьютера.
- Если вы имеете доступ к оборудованию для проведения безопасных переговоров, используйте его при любых важных встречах. Не используйте компьютеры или оргтехнику в отелях для обработки или копирования важной информации.
- Применяйте шифрование для защиты важных файлов и папок.

- Используйте утилиты удаления файлов без возможности восстановления. В случае кражи вашего мобильного компьютера злоумышленники не смогут восстановить интересующую их информацию.
- Тщательно оберегайте важную документацию до того момента, когда ее можно будет безопасно уничтожить (CD-RW должны быть сожжены, дискеты и бумаги порезаны на мелкие кусочки).

Политикой мы называем четкий, структурированный и исчерпывающий набор правил и практических мер, связанных, в нашем примере, с защитой информации. Тогда как плохо составленная политика безопасности может служить примером никому не нужной бюрократии, правильным образом написанная политика, понятная для сотрудников и четко ими соблюданная, представляет собой великолепный организационный барьер против информационных воров.

В политике безопасности вашей компании может быть, к примеру, оговорено, что все доски должны быть вытерты после проведения совещаний, важные документы не должны оставляться на столе без присмотра, а конфиденциальные бумаги – обязательно уничтожаться с помощью специальной машины. В соответствии с этой политикой все картотеки должны закрываться на ключ, для защиты важной информации должны использоваться устойчивые системы шифрования, постоянно работающие компьютеры, находящиеся без присмотра, должны быть защищены «хранителями экранов» с паролями.

Обычно слабые места политики безопасности заключаются в следующих двух моментах: подкуп сотрудников и несоблюдение ими оговоренной политики. Постарайтесь разъяснить вашим подчиненным, почему меры безопасности, описанные в распространенном среди сотрудников меморандуме о политике безопасности, настолько важны. Теоретически все работники компании вполне могут оказаться на бирже труда, если предпринятые неэтичными конкурентами действия приведут к краху компании. Поэтому, если вы не будете следить за выполнением установленной политики безопасности, ее эффективность снизится, и дальнейшая разработка политики окажется пустой тратой времени. Если же вы никогда раньше не следили за соблюдением политики и, в конце концов, вынуждены были уволить кого-то за утечку информации, которую можно было предупредить, придерживаясь установленных правил безопасности, это тревожный признак для вашей компании.

Письменное оформление политики безопасности организации в виде меморандума является одновременно искусством и целой наукой, поэтому за помощью в ее разработке вам следует обратиться к квалифицированным консультантам. Ниже приводятся ссылки на некоторые полезные ресурсы, из которых вы сможете почерпнуть для себя полезные идеи по структуре политики безопасности:

- **Защитите ваши ноу-хау, практические советы по обучению электронной безопасности.** Этот учебник по безопасности для начинающих, написанный простым и доступным языком, предназначен для администраторов и менеджеров компаний. Он был издан Национальным центром образовательной статистики (предложите эту книгу вашим коллегам, не имеющим технического образования). Онлайновая версия книги доступна по адресу в сети Интернет <http://nces.ed.gov/pubs98/safetech/>.
- **Национальная программа промышленной безопасности. Справочное руководство (NISPOLM).** Здесь перечислены все требования, ограничения, уровни секретности и советы по недопущению разглашения секретной информации неавторизованными источниками. Хотя это руководство, прежде всего, предназначено для сотрудников правительственныех служб и коммерческих охранных компаний, полагаем, оно будет небезынтересно для всех остальных читателей, обеспокоенных защитой своей организации от шпионской деятельности. Загрузить данное руководство можно с веб-страницы [www.dss.mil/isecc/nisprom.htm](http://www.dss.mil/isecc/nisprom.htm).
- **Руководство по безопасности Управления национальной безопасности.** Данное руководство, предназначенное для сотрудников Управления национальной безопасности, скорее всего, просочилось в Интернет по недосмотру, и его с высокой степенью вероятности можно считать настоящим документом. В любом случае это руководство может послужить отличным примером несоблюдения политики безопасности. Найти его вы можете по адресу [www.cl.cam.ac.uk/ftp/users/rja14/nsaman.pdf](http://www.cl.cam.ac.uk/ftp/users/rja14/nsaman.pdf).
- **Справочник по безопасности сайтов (RFC2196),** написанный отделом безопасности IETF (проблемной группы проектирования Internet). Этот документ описывает разработку политик компьютерной безопасности и процедур защиты систем, подключенных к Интернету. Загрузить его вы можете по адресу [ftp://ftp.isi.edu/in-notes/rfc2196.txt](http://ftp.isi.edu/in-notes/rfc2196.txt).

## Заключение

Многие люди уделяют внимание исключительно обеспечению сетевой безопасности, напрочь забывая о должных мерах физической безопасности, отсутствие которых позволяет шпионам легко проникать в само здание и похищать конфиденциальную информацию.

На самом деле взломщики, получившие физический доступ в жилые или офисные помещения, представляют большую опасность, чем злоумышленники, проникшие через незащищенную сеть, поскольку в этом

случае они получают доступ не только к компьютеру, но и к бумагам, документам, фотографиям и другим нецифровым носителям информации.

Сложные операции по тайному проникновению обычно проводятся правоохранительными органами, правительственными службами либо частными лицами, участвующими в экономическом шпионаже высокого уровня. Даже если вы не считаете себя потенциальной жертвой подобных операций, вам все равно следует уделять внимание обеспечению физической безопасности. Ведь методы, направленные на борьбу с организованным шпионажем, не менее действенны против обычных воров, которые заинтересованы не столько в вашей информации, сколько в продаже вашей аппаратуры ради сиюминутной выгоды.

## Глава 4

# Проникновение в систему

«И когда обрушаются стены...»

Деф Лепард, исполнитель «тяжелого металла», «Когда обрушаются стены», *Все*

Тот факт, что вы преодолели все физические преграды на пути к интересующему вас компьютеру, еще не означает, что вы сможете прочесть хранимую на нем информацию. Следующими камнями преткновения для шпионов, заинтересованных в оберегаемой от посторонних глаз информации, должны стать инструменты аутентификации на уровне системы, такие как пароль при загрузке компьютера или диалог входа в Windows.

Несмотря на изрядные усилия производителей аппаратного и программного обеспечения, существуют различные способы проникновения в защищенные компьютерные системы, о которых пойдет речь в этой главе. Вы узнаете об уязвимых местах систем, а также инструментах и технологиях их обнаружения и использования (некоторые из них достаточно тонкие, как для открытия дверного замка при помощи отмычки; другие же как для выламывания входных дверей домкратом). Кроме того, мы расскажем вам об основных контрмерах, использование которых затруднит проникновение в ваш компьютер всякого рода шпионов.

## Шпионская тактика

На этот раз вы должны будете примерить на себя облик агента КГБ, вынужденного бедствовать из-за сложной экономической ситуации в стране. (Строго говоря, КГБ был расформирован с распадом Советского Союза в 1991 году, а бывшее Первое управление КГБ по делам внешней разведки было переименовано в Службу внешней разведки (СВР) Российской Федерации.) Уровень моральных принципов и оплаты труда за последние годы в российских спецслужбах достиг низшей отметки, поэтому многие коллеги соблазняют вас выгодными перспективами в частном бизнесе. До сих пор вы специализировались на экономическом шпионаже для КГБ/СВР в Управлении Т (отвечающем за сбор стратегической, военной и промышленной информации по западным странам), поэтому обладаете навыками тайных физических проникновений и взлома компьютерных систем. Когда ваш друг рассказал о крупной европейской корпорации,

набирающей людей с опытом «в сфере обеспечения безопасности», вы предусмотрительно отправили несколько запросов и немедленно получили предложение (с авансом), в котором вам предлагалось обучить ремеслу экономического шпионажа нескольких негласных наемных сотрудников фирмы. Предложенный гонорар, разумеется, намного превзошел ваш государственный оклад: как полковник вы получали несколько сотен долларов в месяц, плюс то, что имели возможность получить на стороне. Вы подали в формальную отставку и спустя всего несколько недель начали читать лекции студентам в Парижском конференц-зале.

Сейчас вы держите в руках традиционную русскую игрушку – матрешку, сравнивая обеспечение компьютерной безопасности с этой матрешкой. Чтобы проникнуть внутрь и добраться до самой информации, необходимо последовательно пройти все уровни защиты. Иногда, по ходу действия, вы обнаруживаете, что некоторые меньшие матрешки раскрашены точно так же, как предыдущие (такова загадочная русская манера объяснять, что одни и те же пароли могут использоваться на разных уровнях защиты системы). Затем, отложив матрешку в сторону, вы говорите, что ваш сегодняшний урок будет посвящен изучению двух внешних уровней защиты – пароля загрузки компьютера, устанавливаемого в BIOS, и пароля, требуемого для входа в операционную систему.

## Использование слабых мест

Перед тем как начать использование уязвимых мест на внешних уровнях компьютерной защиты, необходимо определить характеристики компьютера, с которым нам придется работать, а именно:

- **Тип BIOS.** Вы должны располагать сведениями о типе BIOS и его версии, поскольку от этого зависит применение некоторых инструментов и технологий. При включении компьютера на экране, как правило, отображается производитель BIOS и номер версии, после чего выводится информация о процессоре и памяти. Если эти данные не отображаются на экране, зайдите в настройки BIOS (если он не защищен паролем). Чтобы попасть в окно настроек BIOS, как правило, необходимо удерживать нажатой определенную клавишу в начале загрузки компьютера (например, Del). У разных производителей компьютеров эти клавиши могут различаться. Помимо версии BIOS вы должны выяснить производителя компьютера и его модель.
- **Тип операционной системы.** Как и BIOS, различные версии операционных систем имеют свои слабые места, поэтому немаловажно заранее выяснить версию Windows, с которой вам придется иметь дело. Определить версию ОС можно во время ее загрузки либо по внешнему виду рабочего стола.

Располагая вышеперечисленной информацией, учтите, что при атаке компьютера возможны два варианта начальных условий задачи: когда компьютер оказывается включенным и когда он обесточен. В зависимости от состояния компьютера вам придется использовать различные средства и методы, чтобы проникнуть в систему.

## ПАРОЛЬ BIOS

BIOS (Basic Input/Output System – базовая система ввода/вывода) представляет собой низкоуровневую программу, отвечающую за выполнение основных функций управления компонентами системы – клавиатурой, монитором, дисковыми накопителями, последовательными портами и другой аппаратурой. Параметры BIOS, такие как дата, время и информация о системных настройках, хранятся в памяти CMOS (КМОП – комплементарный металлооксидный полупроводник), как правило, в микросхеме часов реального времени RTC (Real Time Clock).



Уим Бервоец является автором весьма любопытного справочного сайта, который может заинтересовать желающих глубже разобраться в тонкостях BIOS. Этот сайт размещен по адресу: [www.wim bios.com](http://www.wim bios.com).

В самой BIOS есть два средства обеспечения защиты системы, которые могут быть включены на раннем этапе загрузки компьютера:

- **Пароль загрузки компьютера.** Если это средство работает, то без ввода пароля вы не сможете запустить компьютер. Этот пароль обычно называют пользовательским (user password).
- **Пароль изменения настроек BIOS.** Этот пароль необходим для просмотра и изменения настроек BIOS, таких как конфигурация оборудования, управление питанием, время и дата. Этот пароль называют паролем администратора (supervisor password).

Оба пароля хранятся в CMOS вместе с другими настройками BIOS.

Хотя пароли BIOS могут показаться надежной мерой безопасности, на самом деле они малоэффективны против опытных взломщиков. Установленный в BIOS пароль может отпугнуть разве что заурядного злоумышленника, создавая минимум неудобств для более опытного вора с соответствующими знаниями и средствами.

Спросите ваших студентов о том, как можно обойти защиту системы при помощи пароля в BIOS. Получив пару ответов, вы начинаете вспоминать о том, как в прошлом вы это делали сами.

## Тактика: загрузка компьютера

Прежде всего, разберемся, что происходит во время загрузки компьютера. Последовательность операций при этом следующая:

1. Процессор считывает код программы из BIOS и запускает серию POST-тестов (Power On Self Test – самотестирование при включении питания), проверяя, чтобы все компоненты системы функционировали корректно. Во время POST-тестов программа BIOS выполняет следующие действия:
  - инициализирует системное оборудование и регистры микросхем;
  - инициализирует управление питанием;
  - тестирует память (RAM);
  - включает клавиатуру;
  - проверяет функционирование параллельных и последовательных портов;
  - инициализирует контроллеры гибких и жестких дисков;
  - выводит информацию о системе.
2. Защищая в BIOS программа сравнивает во время самотестирования системную конфигурацию с настройками, сохраненными в CMOS. (Обновление CMOS происходит каждый раз при смене какого-либо оборудования.)
3. После выполнения операций POST BIOS осуществляет поиск программы-загрузчика операционной системы. Обычно в первую очередь поиск производится на приводе гибких дисков (A:), а затем на жестком диске (C:) (хотя последовательность может быть изменена).
4. На этом этапе управление работой компьютера переходит от программы BIOS к операционной системе (например, Windows). В результате в дальнейшем загружаются настройки ОС, драйверы устройств и программа аутентификации при входе в систему (для Windows NT/2000/XP).

После успешного завершения всех этапов загрузки операционной системы запускаются все остальные программы, включенные в список автозагрузки.



Некоторые методы обхода защиты с помощью паролей в BIOS предполагают аппаратные решения (вскрытие компьютера). Однако если вы не обладаете опытом открытия и разборки компьютера, попробуйте обойтись программными средствами. Статическое электричество и безудержный энтузиазм способны легко вывести из строя чувствительную электронную технику. Даже внесение изменений в BIOS при помощи программных утилит может привести к непредвиденным последствиям, если вы не будете соблюдать осторожность.

**АНАЛИЗ.** Вы начинаете рассказ с того, что любому типу проникновений в шпионских целях должен предшествовать этап тщательного анализа объекта вашего внимания. Во время планирования атаки на компьютер, защищенный при помощи пароля в BIOS, ваш анализ должен включать:

- Поиск на веб-странице производителя компьютера информации о способах отключения либо сброса пароля в BIOS.
- Выяснение информации о способах обхода пароля из первых рук, с помощью звонка в службу технической поддержки производителя материнских плат. Однако будьте готовы к тому, что от вас могут потребовать информацию, подтверждающую, что именно вы являетесь законным обладателем этого компьютера, для чего вам, возможно, придется прибегнуть к некоторым приемам социотехники.
- Использование поисковых серверов (например, Google) в Интернете. Задайте в строке запроса, например, «компьютеры Dell, пароль BIOS». Результаты поиска могут вывести вас на архивы утилит или сведений по способам обхода защиты в BIOS.

Информация, собранная на этапе анализа, поможет вам сберечь немало времени в ходе самой операции проникновения в систему, защищенную паролем BIOS.

**ЗАПАСНЫЕ ПАРОЛИ.** Запасные пароли BIOS не являются тайной. Люди забывчивы по своей природе, и заботливые производители компьютеров не позволят покупателю оказаться у неработоспособного компьютера из-за собственной рассеянности. По этой причине большинство производителей BIOS встраивают в свои продукты запасные пароли, при помощи которых может быть получен доступ к системе. Поставщики компьютеров нередко включают дополнительные пароли для входа в BIOS или загрузки компьютера. (Производители BIOS передают производителям материнских плат утилиты, с помощью которых те могут менять некоторые настройки для своих собственных систем.) Если вам удалось загрузить компьютер при помощи запасного пароля, то в дальнейшем вы можете либо задать новый пароль пользователя, зайдя в BIOS, либо расшифровать существующий пароль программными средствами из Windows.

В таблицах 4.1, 4.2, 4.3 и 4.4 приводятся списки запасных паролей для BIOS разных производителей, которые успешно применяются для взлома защищенных таким образом систем.

**Таблица 4.1. Пароли для AMI (American Megatrends, Inc.) BIOS**

A.M.I	AAAMMMIII	Aammii	AM
AMI	AMI!SW	AMI.KEY	AMI.KEZ
AMI?SW	AMI_SW	AMI~	AMIAAMI
AMIDEDECOD	Amipswd	AMIPSWD	AMISETUP
BIOS	BIOSPASS	CONDO	HEWITT RAND
LKWPETER	PASSWORD		

**Таблица 4.2. Пароли для Award BIOS**

?award	_award	01322222	01322222
256256	589589	589721	595595
598598	Admin	Alfarome	ALFAROME
Ally	aLLY	ALLy	ALLY
APAf	Award	Award	AWARD PW
AWARD SW	AWARD?SW	AWARD_SW	Awkward
AWKWARD	BIOS	Biosstar	Biostar
BIOSTAR	CONCAT	Condo	cONDO
CONDO	d8on	Djonet	g6PJ
h6BB	HELGA-S	HEWITT RAND	HLT
j09F	j256	j262	j322
j322	j64	KDD	Lkw peter
Lkwpeter	LKWPETER	LKWPETER	PASSWORD
Pint	PINT	SER	Setup
SKY_FOX	SWITCHES_SW	Sxyz	Syxz
SYXZ	SZYX	t0ch20x	t0ch88
TTPTHA	Tzqf	Wodj	ZAAADA
Zbaaaca	ZBAAACA	ZJAAADC	

**Таблица 4.3. Пароли для Phoenix Technologies BIOS**

Phoenix	PHOENIX	CMOS	BIOS
---------	---------	------	------

**Таблица 4.4. Пароли для BIOS других производителей**

Производитель	Пароль
Biostar	Biostar
Compaq	Compaq
Dell	Dell
Epox	xo11nE
Erox	Central
Freetech	Posterie
IBM и VOBIS	Merlin
IBM (Aptiva)	удерживать обе кнопки мыши во время загрузки
Iwill	Iwill
Jetway	Spooml
Packard Bell	bell9
QDI	QDI
Siemens	SKY_FOX
TMC	BIGO
Toshiba	Toshiba

Подбор запасных паролей может занять много времени, и никто не может дать гарантию, что эти пароли вообще будут работать на конкретном компьютере (запасные пароли предназначены в основном для настольных систем; в настоящее время отсутствуют распространенные списки паролей для мобильных компьютеров). Учтите также, что некоторые системы могут иметь дополнительные меры защиты. Например, компьютеры производства Dell выключаются после трех неудачных попыток ввода пароля, что делает процесс его угадывания весьма нудным и длительным.

**УГАДЫВАНИЕ ПАРОЛЯ.** Если ни один из запасных паролей не позволяет загрузить систему, вы можете пойти по пути угадывания пароля. О том, как можно угадать пароль, и о других способах взлома защиты BIOS вы прочтете в шестой главе.

**ВОССТАНОВЛЕНИЕ ПАРОЛЯ.** Как правило, пароль в BIOS защищается при помощи простых алгоритмов шифрования, поэтому его легко можно взломать с помощью специальных программных средств. Некоторые утилиты, перечисленные в параграфе «Средства проникновения в систему» данной главы, позволяют выяснить пароль BIOS в том случае, когда система уже загрузилась и работает.

**ИЗВЛЕЧЕНИЕ ЖЕСТКОГО ДИСКА.** Один из простейших способов обхода защиты при помощи пароля в BIOS заключается в извлечении жесткого диска из системного блока одного компьютера и подключения его к другому компьютеру. Поскольку защита BIOS встроена в материнскую плату, она не позволяет загрузить сам компьютер, однако не влияет на жесткий диск или другие носители информации. (Тем не менее уже существуют некоторые версии BIOS на новейших мобильных системах, которые блокируют доступ к жесткому диску, делая невозможным просмотр его содержимого на другом компьютере.)

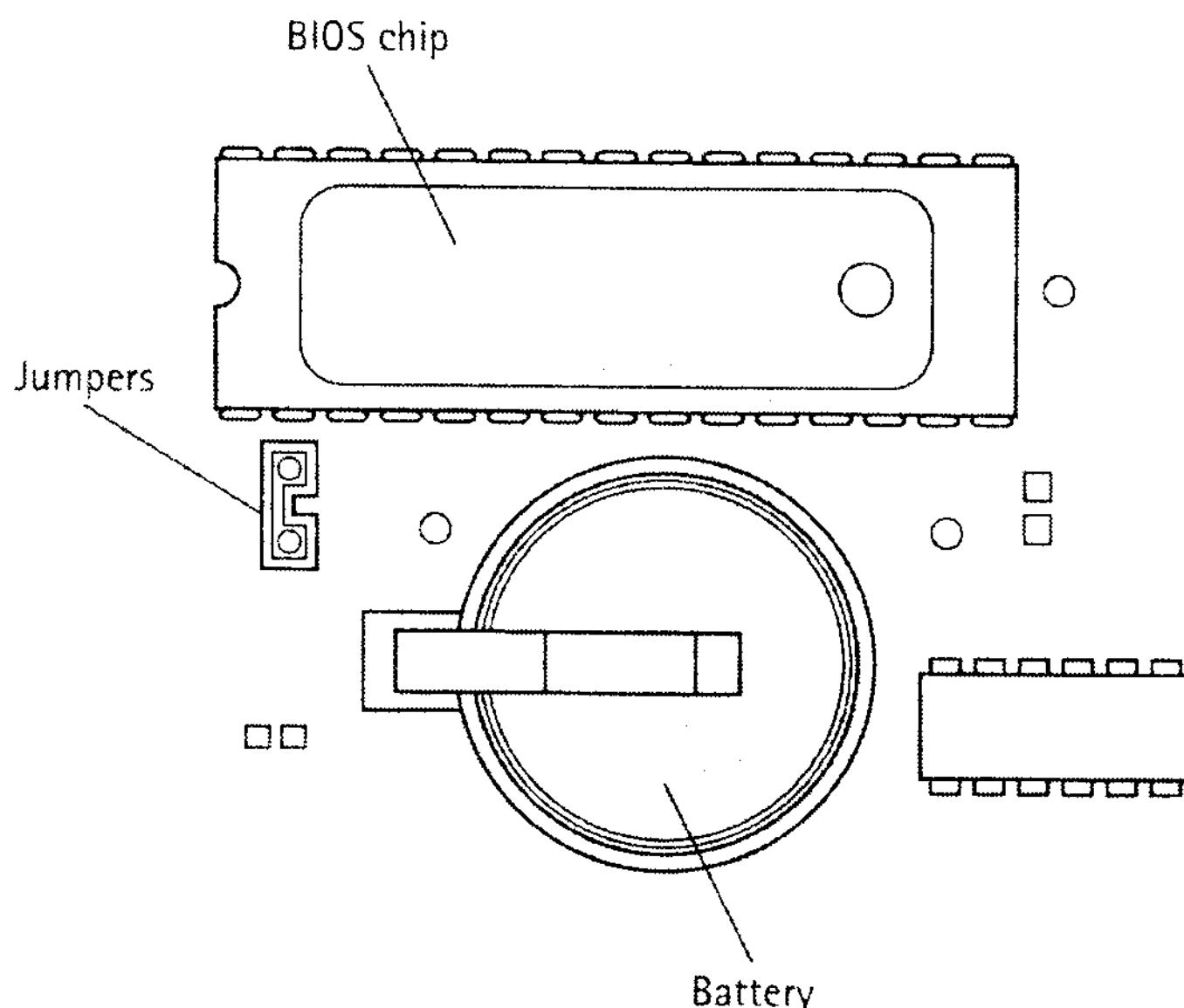
Еще одна мера безопасности, о которой вы должны иметь представление, касается опции «chassis intrusion detection» (обнаружение вскрытия корпуса), особенно важной, например, для серверов сети. Если компьютер вскрывался после установки данной опции, то во время загрузки выводится соответствующее сообщение. В будущем следует ожидать внедрения в корпоративные компьютеры технологии уведомлений (Alert Standard Format – ASF), включающей в себя возможность отправки подключенными к сети компьютерами сообщений о своем статусе на сервер. К примеру, если посреди ночи вы вскроете офисный компьютер, чтобы вытащить из него жесткий диск, вас может удивить внезапное появление охранников, прочитавших сообщение от BIOS компьютера. (Отключение сетевого кабеля и полное выключение питания компьютера в принципе позволяют обойти защиту ASF, однако теоретически оба действия могут вызвать срабатывание других средств защиты).

**ОБНУЛЕНИЕ CMOS.** Другой аппаратный способ отключения защиты паролем в BIOS заключается в обнулении CMOS. Когда хранимая в CMOS информация оказывается запорченной, при включении компьютера загружаются настройки по умолчанию, в том числе и отключение защиты паролем. Вы можете отключить парольную защиту с помощью нескольких простых приемов (рис. 4.1, на котором изображен внешний вид различных компонентов BIOS):

- **Элементы питания.** Память CMOS представляет собой энерго-зависимое ЗУ. Ее питание осуществляется от небольшой батарейки. Вам понадобится отключить питание компьютера, а затем найти и отключить батарейку на материнской плате (она выглядит как плоская, круглая монета). Некоторые производители материнских плат впаивают элемент питания в саму плату, что может осложнить вашу задачу в случае отсутствия паяльника и инженерных навыков. После отключения питания данные в памяти постепенно теряются. Однако разрядка

CMOS может занять от нескольких минут до нескольких дней, в зависимости от емкости схемы (один из способов быстро и безопасно разрядить CMOS – замкнуть резистором 10 кОм контакты элемента питания). Затем, при включении компьютера, программа в BIOS проверяет системные настройки и, ничего не обнаружив, использует настройки по умолчанию, записывая их в CMOS. Кроме того, обнуление настроек можно осуществить путем замыкания определенных контактов на материнской плате. Как это сделать, обычно описано в руководстве для пользователя по данной плате.

- **Перемычки.** Другой способ сброса CMOS подразумевает использование специальных перемычек на плате (которые позволяют менять аппаратные настройки). После помещения перемычек в положение, необходимое для очистки CMOS, при последующей загрузке компьютера будут использованы значения настроек по умолчанию (без пароля). Эти перемычки обычно маркируются на плате как «Clear RTC», «Clear CMOS» или PSWD. Конфигурации перемычек на компьютерах разных производителей отличаются – вот где вам на руку сыграет предварительная подготовка.



**Рис. 4.1.** Внешний вид микросхемы BIOS (BIOS chip), элемент питания (Battery) для хранения настроек в CMOS и перемычки для очистки CMOS (Jumpers)

Описанные аппаратные приемы сброса пароля в BIOS хороши для выключенной компьютерной техники. Если компьютер уже загружен и работает, для очистки CMOS вы можете прибегнуть к следующим программным методам решения проблемы:

- **Воспользоваться средствами очистки CMOS.** Утилиты вроде Cmospws, описываемые в параграфе «Средства проникновения в систему» данной главы, позволяют восстанавливать записанный в BIOS пароль либо полностью стирать данные, хранимые в CMOS.
- **Провести перезапись BIOS.** Большинство современных материнских плат позволяют перезаписывать содержимое BIOS (перепрограммировать его) с помощью соответствующих утилит. Утилиты для перезаписи BIOS обновляют и сам BIOS, и настройки, хранимые в CMOS. Применяйте этот метод с осторожностью, поскольку сбои в процессе перезаписи могут привести к повреждению и неработоспособности материнской платы и всего компьютера.

Главный недостаток очистки CMOS заключается в привлечении внимания пользователя к отсутствию пароля и изменению настроек. Вам следует прибегать к этому способу только в том случае, когда другие методы оказались неэффективны.



Следует с осторожностью отнестись к экспериментам с BIOS и CMOS, о чем мы особо хотим предупредить нетерпеливых или технически неграмотных шпионов, поскольку в результате ваших действий вы можете изменить системные настройки, вызвав неработоспособность системы (как правило, временную). По возможности выполняйте резервирование содержимого CMOS перед тем, как начать внесение изменений, благо для этого существует множество утилит, позволяющих сохранять и восстанавливать настройки CMOS в случае их непреднамеренной порчи.

**BIOS МОБИЛЬНЫХ ПК.** BIOS мобильных компьютеров требует отдельного рассмотрения. Дело в том, что получить доступ к защищенному при помощи пароля в BIOSциальному компьютеру намного сложнее, чем к его настольному родственнику. Ниже перечислены основные причины, по которым обойти защиту BIOS мобильного компьютера намного сложнее:

- **Конструктивное исполнение корпуса.** Даже если в ноутбуке предусмотрена функция обнуления настроек BIOS при помощи перемычек или удаления элемента питания, для среднестатистического шпиона вскрыть мобильный компьютер, чтобы добраться до аппаратного обеспечения, намного сложнее.
- **EEPROM.** Вместо CMOS в большинстве моделей современной мобильной техники для хранения настроек BIOS используется память EEPROM (электрически стираемое программируемое ПЗУ). Чтобы получить доступ к параметрам BIOS, необходимо

вначале выпаять микросхему EEPROM, а затем воспользоваться специальным устройством чтения ППЗУ. Такой способ атаки требует наличия специальных знаний и инструментов.

- **Элементы питания.** Удаление элемента питания (аккумулятора) позволяет сбросить настройки BIOS на некоторых мобильных компьютерах. Однако следует помнить о том, что в мобильных компьютерах может присутствовать два элемента питания: один для хранения настроек CMOS (его наличие необязательно) и другой для работы компьютера в режиме автономного питания.
- **Пароли на доступ к жесткому диску.** Некоторые производители включают в свои продукты возможность установки пароля на доступ к жесткому диску компьютера. В этом случае, подключив диск к другому компьютеру, вы все равно не сможете прочесть его содержимое.

Если вам необходимо взломать защиту мобильного ПК, следует потратить время на поиск и изучение информации по данному вопросу. Даже усовершенствованная система защиты ноутбуков не является непреодолимой. Доступность тех или иных способов обхода парольной защиты BIOS зависит от производителя модели мобильного компьютера. Приведем следующие примеры:

- **Аппаратные приспособления.** Поставщики ноутбуков нередко используют различные дополнительные устройства для сброса паролей в BIOS. К примеру, на некоторых моделях мобильных компьютеров производства Toshiba и Compaq пароли могут быть сброшены при помощи специальных приспособлений с обратной связью, представляющих собой простые 25-контактные разъемы, подключаемые к параллельному порту компьютера. На некоторых моделях Toshiba замыкание контактов 1-5-10, 2-11, 3-17, 4-12, 7-13, 8-14, 9-15, 18-25 разъема, обнаруживаемое BIOS во время загрузки, приводит к сбросу пароля.
- **Ключевые дискеты.** В старых моделях ноутбуков производства Toshiba для сброса пароля в BIOS использовались специальные ключевые дискеты. К помощи этих дискет прибегали в сервисных центрах. Вставив дискету в обычный дисковод, технический специалист включал компьютер, и когда при загрузке запрашивался пароль, нажимал Enter, затем Y и снова Enter при запросе задания пароля. После этого открывалось окно настроек BIOS, где можно было ввести новый пароль. Магический диск для сброса паролей на самом деле представлял собой обычную форматированную дискету, первые пять байт второго сектора которой имели значения 4B 45 59 00 00. Вы можете воспользоваться специальным hex-редактором, чтобы создать такую дискету, либо поискать в Интернете утилиту под названием KeyDisk, которая умеет делать это сама.

## Контрмеры: ноутбуки

Вторым по важности объектом пристального внимания со стороны шпионов являются ноутбуки или мобильные компьютеры. Хотя стоимость ноутбуков привлекает к себе и обычных воров, однако для шпионов, прежде всего, важна информация, хранимая на жестком диске ноутбука. Кража ноутбука у важного чиновника – наиболее быстрый и легкий способ получения доступа ко многим правительенным, военным и коммерческим секретам.

- По данным Института компьютерной безопасности и ФБР, только в США в течение 2001 года была украдена 591 тысяча мобильных компьютеров, причем 97% украденных ноутбуков больше никогда не увидели своих владельцев.
- В недавнем отчете главный инспектор Министерства юстиции заявил, что «пять агентств, включая ФБР и Администрацию по контролю над соблюдением законов о наркотиках, потеряли 400 мобильных компьютеров, больше половины из которых содержали секретную информацию, касающуюся вопросов национальной безопасности».
- Шестьсот мобильных компьютеров были украдены из Министерства обороны Великобритании с 1997 года, причем на некоторых из них также хранились секретные правительственные и военные данные.

Чтобы не допустить попадания вашего компьютера или хранимой на нем информации в чужие руки, советуем вам предпринять следующие меры безопасности:

- Не выпускать ваш мобильный компьютер из виду и не оставлять его без присмотра (при необходимости можете приковать его наручниками к своему запястью).
- Прятать ваш мобильный компьютер в безопасном месте, когда вы им не пользуетесь.
- Использовать устойчивые системы шифрования для защиты важной информации (некоторые из них описываются в параграфе «Контрмеры» пятой главы).
- Применять максимально возможное число опций безопасности в BIOS. Конечно, это не даст вам стопроцентной защиты против опытного шпиона, однако будет являться первой линией обороны на пути взломщика. (При этом не забывайте хранить пароли в безопасном месте. Интернет-форумы полны грустных рассказов о людях, забывших пароли к своим мобильным компьютерам.)

- **Комбинации клавиш.** Ряд производителей используют секретные комбинации клавиш для отключения пароля. К примеру, в некоторых ноутбуках производства Toshiba можно отключить действие пароля, если во время загрузки компьютера удерживать нажатой левую клавишу Shift.
- **Коммерческие службы по восстановлению паролей.** Многие производители ноутбуков и несколько легальных частных компаний предлагают услуги по восстановлению паролей владельцам мобильных компьютеров, у которых по той или иной причине он оказался заблокированным. Компания Password Crackers Inc. ([www.pwcrack.com](http://www.pwcrack.com)) занимается продажей «микросхем системы безопасности», которыми можно заменить соответствующие чипы во многих популярных моделях ноутбуков, чтобы разблокировать компьютер. Вам понадобится вынуть из своего ноутбука микросхему EEPROM, а компания вышлет вам аналогичную с настройками BIOS по умолчанию для вашего компьютера. Вы также можете выслать им оригиналную микросхему EEPROM, и компания восстановит ваш пароль. Корпорация Nortek Computers, Ltd. ([www.nortek.on.ca](http://www.nortek.on.ca)) специализируется на снятии паролей включения мобильных компьютеров ThinkPad и жестких дисков и полном восстановлении данных с жестких дисков. Однако эта канадская компания является чрезвычайно щепетильной и требует убедительных доказательств того, что ноутбук принадлежит именно вам, прежде чем заняться его разблокированием.

## WINDOWS 3.X/9X/ME

Если защиту при помощи пароля на загрузку компьютера в BIOS можно представить в виде самой внешней матрешки, то после ее преодоления следующей матрешкой для вас станет уровень безопасности операционной системы. Хотя Windows XP увидела свет еще осенью 2001 года, статистика утверждает, что к концу 2002-го Windows 98 продолжала удерживать лидерство как самая распространенная операционная система. А это хорошая новость для компьютерных шпионов, поскольку семейство операционных систем Windows 3.x/9x/Me не отличается надежной защитой в плане авторизации пользователей.

Полагаться на диалоговое окно входа в систему в предыдущих версиях Windows не более безопасно, чем покупать ювелирные изделия на уличной раскладке. Несмотря на явную экономию средств, и то и другое совершенно ненадежно. При появлении диалогового окна входа в систему Windows 3.x/9x/Me вы можете просто нажать Cancel. В результате вы получите полный доступ к системе и всем файлам на ней. Дело в том, что это диалоговое окно отвечает только за персонификацию внешнего вида Рабочего стола Windows и восстановление сетевых подключений на основе учетной записи и пароля пользователя. Все эти настройки хранятся в профиле пользователя (файл с расширением PWL).



Более подробно о профилях пользователя и способах извлечения из них паролей вы узнаете из главы 6.

Единственный более-менее серьезный способ защиты системы в старых версиях Windows сводился к включению «защиты паролем» в «хранителе экрана». Пользователь мог настроить систему, чтобы она требовала ввода пароля для возвращения к Рабочему столу. Если пароль был введен неправильно, «хранитель экрана» продолжал свою работу. Несмотря на кажущуюся надежность подобной защиты, пользователи испытывали ложное чувство безопасности, поскольку на самом деле обойти такую защиту достаточно просто. Перечисленные ниже методы обхода защиты «хранителя экрана» применимы только для Windows 3.x/9x/Ме, поскольку в Windows NT/2000/ХР используются более надежные методы аутентификации на уровне системы. Кроме того, более надежную защиту предлагают «хранители экрана» сторонних производителей для Windows 3.x/9x/Ме. Итак, существуют следующие способы преодоления защиты «хранителей экрана»:

- **Перезагрузка.** Простейший способ обойти защиту «хранителя экрана» – выключить, а затем заново включить питание компьютера. После загрузки системы вы получите полный доступ к файлам и приложениям. Сделав все, что вам нужно, просто активизируйте «хранитель экрана» заново. Недостаток такого способа в том, что наблюдательный пользователь может заинтересоваться, куда делись окна приложений на рабочем столе или открытые файлы, когда, возвратившись, он введет пароль для отключения «хранителя экрана». Кроме того, умный пользователь может поместить «хранитель экрана» в папку Автозагрузка, в результате чего «хранитель экрана» будет запускаться автоматически сразу после загрузки системы. В этом случае во время загрузки системы необходимо удерживать нажатой клавишу Shift – тогда автозагрузка программ будет отключена.
- **Autorun.inf.** Более хитрый способ обхода защиты «хранителя экрана» заключается в функции автозапуска CD-ROM. При вставке в CD-привод любого диска Windows проверяет наличие в его корневой папке файла с названием Autorun.inf и, обнаружив его, запускает заданные в нем приложения поверх активного «хранителя экрана». Поэтому вам достаточно создать текстовый файл с названием Autorun.inf, сохранив в нем единственную строчку с именем приложения, которое вы хотите запустить, а затем записать этот файл на компакт-диск. К примеру, если первой строчкой в этом файле будет являться Explorer.exe, при вставке данного компакт-диска в привод автоматически запустится стандартный файловый менеджер Windows, который будет выведен поверх работающего «хранителя экрана».

- **Взлом пароля.** В предыдущих версиях Windows использовались не слишком надежные системы шифрования паролей, в том числе и для «хранителя экрана». Для их расшифровки существует множество утилит (некоторые из которых упоминаются в параграфе «Средства проникновения в систему» этой главы). Вы можете сочетать использование этих утилит вместе с предыдущим приемом автозапуска CD-дисков, чтобы найти и расшифровать файл с паролем.

## WINDOWS NT/2000/XP

Если меры безопасности в операционных системах Windows 3.x/9x/Ме нельзя назвать надежными, то система безопасности в Windows NT/2000/XP сравнима с охраной комплекса зданий Лубянки, включавшего тюрьму и московскую штаб-квартиру КГБ. Однако то, что кажется неприступным снаружи, может оказаться уязвимым изнутри. (В ходе секретной операции под кодовым назначением СК-ТАW в начале 80-х ЦРУ смогла организовать прослушивание всех телефонных разговоров, перехват факсовых и телексных сообщений в тоннеле, соединявшем Лубянку, секретный узел связи в Троицке и штаб-квартиру Первого управления КГБ в Ясенево. В ходе операции была собрана масса ценной информации, пока перебежчики ЦРУ Эдвард Ховард Ли и Элдрик Эймс не сорвали ее проведение. Бывший генерал-майор КГБ Олег Калугин по этому поводу сказал так: «Лучший ход ЦРУ. Они слушали все наши разговоры. Все до единого!»)

Закончив исторический экскурс, вы рекомендуете вашим студентам заняться изучением слабых мест защиты Windows NT/2000/XP в ходе интерактивной загрузки (interactive logon – термин Microsoft, обозначающий несетевую загрузку системы), чтобы они могли провести собственную операцию «ТАW» против этих систем.

**УГАДЫВАНИЕ ПАРОЛЕЙ ВРУЧНЮЮ.** Простейший вариант атаки компьютера под управлением ОС Windows NT/2000/XP сводится к угадыванию пароля пользователя (вам может повезти, если пользователь отключил ради собственного удобства опцию «требовать ввод имени пользователя и пароля при входе в систему»). Кроме того, по умолчанию Windows выводит в поле «учетная запись» имя последнего пользователя, входившего в систему, поэтому вам останется только ввести правильный пароль.

Система Windows XP – еще более легкая цель для шпионской атаки. Пытаясь сделать систему более дружественной к пользователю, Microsoft включила функции подсказки паролей в процессе входа в систему. Пользователи, плохо знакомые с основными принципами соблюдения безопасности, могут задать легко угадываемую подсказку.

По умолчанию в Windows присутствуют, по крайней мере, две учетные записи: Администратор (Administrator) и Гость (Guest):

- Администратор либо другой пользователь с его привилегиями является основной целью злоумышленников (этот бюджет эквивалентен 'root' в операционных системах Unix). В качестве

Администратора вы получаете полный доступ ко всем файлам компьютера, за некоторыми исключениями в случае использования шифрованной файловой системы EPS. Полномочия Администратора просто необходимы для получения доступа к учетным записям и паролям пользователей в операционных системах Windows NT/2000/XP.

- Учетная запись Гостя используется для предоставления другим людям ограниченного доступа к компьютеру, если они не имеют собственного бюджета. По умолчанию учетная запись Гостя отключена.

Вы можете попытаться вручную отгадать пароли для одной из этих учетных записей. Чаще всего пароли выглядят как Admin и Guest или же для этих учетных записей пароль вообще не задается.



Более подробно об угадывании паролей вручную мы расскажем вам в главе 6.

**ЗАГРУЗКА ДРУГОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ.** Один из простейших и наиболее эффективных средств обхода защиты операционной системы – загрузка другой ОС, с помощью которой вы можете получить доступ к файлам на жестком диске. Если интересующий вас жесткий диск имеет файловую систему FAT или FAT32, вы можете воспользоваться простой загрузочной дискетой DOS для запуска компьютера и доступа к файлам. Однако чаще всего при использовании ОС Windows NT/2000/XP жесткий диск форматируется под систему NTFS, которая не распознается из-под DOS (NTFS обеспечивает улучшенную защиту файлов, благодаря хранению пользовательских разрешений). В этом случае вам понадобится воспользоваться специальными утилитами, такими как NTFSDOS, позволяющими получать доступ к разделу NTFS из-под DOS, либо загрузить версию Linux, поддерживающую файловую систему NTFS.

Некоторые программные средства для атак подобного типа будут перечислены в параграфе «Средства проникновения в систему».

**СИСТЕМНЫЕ ДИСКИ ДЛЯ СБРОСА ПАРОЛЯ.** В Windows XP существует опция создания дискеты для сброса пароля. Поскольку пользователи нередко забывают собственные пароли, Microsoft проявила заботу о таких пользователях, создав Мастер Забытых Паролей (Forgotten Password Wizard), записывающий на дискету специальную информацию. Если пользователь никак не может вспомнить собственный пароль для входа в систему, то, вставив эту дискету, он может сбросить старый пароль и ввести новый.

Хотя никто не гарантирует, что интересующий вас субъект действительно создал дискету для сброса пароля, не поленитесь поискать похожие дискеты в его кабинете. Если вы обнаружите на какой-то из них надпись Password, Windows Password или Windows XP, можете считать, что вам повезло.

## Тактика: онлайновые ресурсы разведчика

Хороший шпион знает сильные и слабые места своего оппонента (либо, по крайней мере, полагается на знания кого-то в своей организации). В данном случае вашим оппонентом является операционная система Windows, а именно ее средства защиты, не дающие вам возможность проникнуть в систему. Новые бреши обнаружаются буквально каждую неделю (а иногда и каждый день), поэтому вы должны всегда быть в курсе событий, чтобы суметь воспользоваться известными уязвимыми местами или же вовремя ликвидировать их, находясь по другую сторону баррикад.

Почему же компании по производству программного обеспечения допускают выход продуктов с таким множеством ошибок? Давайте для примера рассмотрим операционную систему Windows.

По приближенным оценкам, Windows NT состоит из 20 миллионов строк программного кода, Windows 2000 – из 35 миллионов строк, а Windows XP – из 40 миллионов строк. Для сравнения: в этой книге на одну страницу приходится в среднем 40 строк, таким образом, в бумажном виде программный код XP занял бы одну книгу в миллион страниц или 2500 книг такого же размера, как эта. Как, по-вашему: корректоры в состоянии справится с таким объемом работы?

Согласно статистике Института программного проектирования, на каждую тысячу строк программного кода приходится от 5 до 15 ошибок. Путем несложных расчетов получаем, что Windows XP потенциально может содержать от 200 до 600 тысяч ошибок. (Экономические причины играют не последнюю роль, поскольку намного дешевле выпустить последующие программные «заплаты», чем просматривать все эти миллионы строк кода.) Хотя не все программные ошибки имеют отношение к безопасности системы, все же с этим вопросом связан немалый процент из них. По этой причине в сложных и объемных приложениях или операционных системах так часто встречаются уязвимые места системы безопасности.

Ниже перечислены наиболее интересные онлайновые источники, которые мы рекомендуем вам регулярно посещать, чтобы оставаться в курсе событий по поводу постоянно обнаруживаемых новых уязвимых мест, которые могут быть использованы в шпионских целях:

- **NTBugTraq.** Данный сайт посвящен исключительно вопросам безопасности операционных систем Windows NT/2000/XP. Подписаться на рассылку и просмотреть архивы можно по адресу [www.ntbugtraq.com](http://www.ntbugtraq.com).

- **BugTraq.** Здесь размещен полный список обнаруженных ошибок, связанных с защищенностью различных операционных систем, который формируется на основе присланных по электронной почте отчетов. Данный список постоянно обновляется, но при этом нередко подвергается критике (в особенности со стороны производителей этих самых операционных систем, чьи ошибки здесь перечислены) за разглашение ненужных деталей. Узнать подробности вы сможете, посетив веб-страницу [www.securityfocus.com/popups/forums/bugtraq/intro.shtml](http://www.securityfocus.com/popups/forums/bugtraq/intro.shtml).
- **Microsoft.** Полный перечень бюллетеней по безопасности компании Microsoft (а также информацию о подписке на них) вы сможете найти по адресу: [www.microsoft.com/technet/security/current.asp](http://www.microsoft.com/technet/security/current.asp).
- **CERT.** Публикуемый псевдофедеральной Командой Быстрого Компьютерного Реагирования (Computer Emergency Response Team – CERT) университета Карнеги Меллона, этот список уязвимых мест системы безопасности и советов по их защите стал одним из первых источников подобной информации. Однако сейчас он уступает в плане подробности и своевременностидачи информации списку BugTraq. Тем не менее ознакомиться с ним вы можете по адресу [www.cert.org](http://www.cert.org).
- **NIPC.** Правительственный Центр защиты национальной инфраструктуры (National Infrastructure Protection Center – NIPC) занимается сбором и распространением информации по обнаруженным брешам в защите ОС. Сведения изложены в весьма сухом виде, без подробностей, но тем не менее эти данные могут послужить отправной точкой для формулировки запросов к поисковым серверам Интернета с целью поиска более детальной информации. Адрес веб-узла: [www.nipc.gov](http://www.nipc.gov).

**МЕНЕДЖЕР УЧЕТНЫХ ЗАПИСЕЙ В СИСТЕМЕ ЗАЩИТЫ.** Файл Менеджера учетных записей в системе защиты (Security Accounts Manager – SAM) – главная цель любого взломщика, пытающегося пробить брешь в защите операционной системы. Перед тем как обсудить способы атаки файла SAM, разберемся с алгоритмом процесса аутентификации Windows при входе в систему. Итак, после запуска компьютера и выполнения загрузочной программы BIOS начинается этап загрузки операционной системы, при завершении которого выполняются следующие операции:

1. Последним этапом загрузки ОС является запуск приложения Winlogon.exe.
2. Исполняемый файл Winlogon.exe обращается к библиотеке Msgrina.dll для вывода окна приветствия в Windows XP либо диалогового окна входа в систему в Windows NT/2000.

3. Winlogon.exe передает информацию об учетной записи пользователя и его пароле в подсистему локальных средств защиты (Local Security Authority – LSA), которая проверяет корректность введенной пользователем информации.
4. Если имя учетной записи и пароль являются правильными, Менеджер учетных записей возвращает идентификационный номер (Security Identifier – SID), а также идентификаторы всех групп, в состав которых включен данный пользователь.
5. При помощи подсистемы LSA на основе полученной информации создается маркер доступа. Этот маркер позволяет получать доступ к защищенным ресурсам, основываясь на привилегиях и полномочиях пользователя.
6. Затем Winlogon.exe загружает оболочку Windows в соответствии с маркером пользователя.

SAM-файл является величайшей ценностью системы защиты Windows, поскольку именно он содержит информацию обо всех учетных записях и паролях системы. Этот файл зашифрован при помощи односторонней функции хеширования, поэтому информация о паролях не может быть раскрыта непосредственно. В операционной системе Windows NT SAM-файл размещается в папке winnt\system32\config\sam, а для Windows XP – в папке windows\system32\config\sam. (На серверах Windows 2000, выступающих в роли контроллеров домена, сведения об учетных записях и паролях пользователей хранятся в службе Active Directory, а не в SAM-файле.)

Если шпиону удастся обойти защиту SAM-файла, то при помощи различных утилит он сможет получить полный доступ к системе. Существуют следующие способы обхода защиты с помощью файла Менеджера учетных записей:

- **Удаление либо переименование SAM-файла.** Если загрузить компьютер при помощи другой операционной системы, позволяющей получить полный доступ к жесткому диску, вы можете удалить или переименовать SAM-файл. После перезагрузки из системы будут удалены все учетные записи, в результате чего вы сможете загрузиться под бюджетом Администратора, оставив поле пароля пустым. (Каждый раз при изменении SAM-файла (путем его удаления или переименования), обязательно создавайте его резервную копию.)
- **Взлом SAM-файла в режиме реального времени.** Если целевой компьютер уже загружен, вы можете установить и запустить утилиту взлома SAM-файла (для этого вам понадобятся права администратора), чтобы расшифровать учетные записи и пароли пользователей системы.

- **Удаленный взлом SAM-файла.** Для атаки данного типа необходимо скопировать SAM-файл с целевого компьютера, а затем обработать его утилитой расшифровки на другой машине. В предыдущих версиях NT вам достаточно было загрузиться при помощи другой операционной системы, а затем скопировать SAM-файл себе на диск. В Windows 2000 или XP, благодаря наличию более сложной системы защиты, вам понадобятся права Администратора для запуска утилиты, позволяющей извлекать информацию из SAM-файла и затем сохранять ее на диск.
- **Изменение SAM-файла.** Существует несколько программ, с помощью которых вы можете менять пароли в SAM-файле. Для этого нужно загрузиться с дискеты с утилитой, выбрать учетную запись, для которой вы хотите задать пароль (например, Администратор), и ввести новый пароль.

С точки зрения надежности одностороннее хеширование в Windows NT являлось достаточно уязвимым, доказательством чего могут служить множество успешных атак хакеров, использовавших метод хеширования случайных паролей и последующее их сравнение с зашифрованными паролями, хранящимися в SAM-файле. Microsoft отреагировала на это замечание и включила в Service Pack 3 для Windows NT так называемый системный ключ (Syskey), который также используется в последующих версиях Windows – 2000 и XP.

Этот системный ключ представляет собой дополнительный уровень защиты для SAM-файла, выполняя его шифрование при помощи 128-битного ключа. Взломать SAM-файл, зашифрованный с помощью системного ключа, становится практически невозможно. Системный ключ должен быть включен вручную в Windows NT 4.0, тогда как в операционных системах Windows 2000 и XP он включается по умолчанию. (До недавних пор большинство хакерских утилит не умели различать обычные SAM-файлы и SAM-файлы, зашифрованные с помощью системного ключа. В результате шпионы просиживали дни и ночи, пытаясь взломать пароли обычными средствами, даже не ведая о дополнительном уровне защиты.)

Хотя системный ключ препятствует извлечению паролей непосредственно из SAM-файла, он не обеспечивает защиты хешированных паролей в памяти (если вы обладаете полномочиями Администратора) либо в сетевом трафике. В смешанных сетях, состоящих из компьютеров под управлением разных операционных систем (Windows 9x/Me и Windows NT/2000/XP), используется старый и менее безопасный менеджер сети и соответственно более низкий уровень защиты паролей. Хранимые в памяти либо передаваемые по сети хешированные пароли могут быть легко перехвачены и впоследствии расшифрованы при помощи обычных утилит взломщика.



Если в Windows XP Professional применяется шифрованная файловая система (EFS), то ваши попытки изменения пароля либо удаления SAM-файла для учетных записей, защищенных с помощью файловой системы EFS, могут привести к полной невозможности доступа к зашифрованным данным. Это не относится к защищенным при помощи EFS файлам и папкам в Windows 2000, поскольку человек с привилегиями администратора может получить доступ к зашифрованным файлам, изменив пароль для учетной записи пользователя. Windows XP Home не поддерживает файловую систему EFS.

**ЭСКАЛАЦИЯ ПРИВИЛЕГИЙ.** Предположим, что вы вошли в систему под учетной записью Гостя. В этом случае ваши возможности будут весьма ограничены, поскольку файловая система NTFS не предоставит вам доступа к файлам других пользователей, а для использования утилит расшифровки паролей в SAM-файле вам также понадобятся привилегии администратора.

Тем не менее, получив доступ в систему даже под непривилегированной учетной записью, вы можете попытаться расширить свои права. В атаках подобного рода используются известные системные ошибки, позволяющие пользователю выполнять действия, на которые он на самом деле не имеет права, хотя система полагает, что с вашими полномочиями все в порядке. Благодаря эскалации привилегий вы можете добавлять, удалять или изменять данные в системе, создавать либо удалять пользовательские бюджеты или же добавлять пользователей в группу администраторов.

К примеру, популярная брешь Windows 2000 связана с использованием службы NetDDE. Было обнаружено, что если данная служба является активной, то вы можете выполнять команды с системными полномочиями. (Имеются в виду полномочия процессов, запущенных на уровне операционной системы; их можно представить как суперполномочия Администратора.) Например, набрав следующую команду в командной строке, любой пользователь, интерактивно вошедший в систему, независимо от своих начальных полномочий может запустить cmd.exe и получить доступ ко всем файлам жесткого диска:

```
C:\netdmsg -s Chat$ cmd.exe
```

После того как данный способ атаки путем эскалации привилегий стал известен широкой публике, корпорация Microsoft выпустила «заплатки» для решения этой проблемы. (Оперативность выпуска «пакетов исправлений» с момента обнаружения новых уязвимых мест может варьироваться в широких пределах. К примеру, возможность эскалации привилегий при помощи события WM\_TIMER, ставшая известной в августе 2002 года, которая позволяла любому вошедшему в систему пользователю получать над ней полный контроль, была окончательно решена Microsoft только в декабре 2002.) Учтем также тот факт, что среднестатистические пользователи не всегда знают о существовании «заплат», а даже если и знают, то не всегда их устанавливают. Очевидно, что в данном случае все зависит от вашего везения.

## Средства проникновения в систему

Вы рассказываете вашим студентам о том, что нет смысла пытаться открыть матрешку вручную, когда на рынке представлено множество бесплатных и коммерческих утилит, призванных облегчить вашу задачу. Вы пускаете по рядам список наиболее популярных утилит, предназначенных для проникновения в систему, и вкратце обсуждаете каждую из них.

### СРЕДСТВА ВЗЛОМА ПАРОЛЕЙ BIOS

Существует великое множество программ, предназначенных для расшифровки пароля BIOS. Однако помните, что все они применимы только в случае, если компьютер уже загружен и работает. Если вам не удается загрузить компьютер из-за заданного в BIOS пароля, необходимо прибегнуть к другим способам доступа к компьютеру и жесткому диску, описанным в разделе «Использование слабых мест» данной главы.

**CMOSPWD.** Одна из наиболее распространенных и часто используемых программ расшифровки паролей BIOS, запускаемая из командной строки, носит название cmospwd; ее автором является Кристоф Гренье. Эта утилита позволяет расшифровывать пароли следующих версий BIOS:

Acer/IBM	семейство ноутбуков фирмы IBM
AMI BIOS	Packard Bell Supervisor/User
AMI WinBIOS (12/15/93)	Phoenix 1.00.09.AC0 (1994)
AMI WinBIOS 2.5	Phoenix 1.04
Award 4.5x	Phoenix 1.10 A03/Dell GXi
Award Medallion 6	Phoenix 4 release 6 (User)
Compaq	Phoenix 4.05 rev 1.02.943
Compaq (1992)	Phoenix 4.06 rev 1.13.1107
Gateway Solo – Phoenix 4.0 r6	Phoenix A08, 1993
IBM (PS/2, Activa)	Toshiba
IBM 300 GL	Zenith AMI

На тот случай если программе не удается расшифровать пароль, в ней предусмотрена опция “kill” для его удаления. Программа cmospwd проста в использовании, эффективна и хорошо документирована: файл ReadMe содержит массу полезной информации, касающейся атак на компьютеры, защищенные при помощи пароля BIOS. Загрузить эту программу можно по адресу:

[www.cgsecurity.org/index.html?cmospwd.html](http://www.cgsecurity.org/index.html?cmospwd.html).

**ДРУГИЕ УТИЛИТЫ.** Существуют и другие утилиты, предназначенные для работы со специфическими версиями BIOS, и мы советуем вам обзавестись набором подобных утилит, поскольку в ряде случаев одни средства являются более эффективными, чем другие. А начать формирование вашей коллекции рабочих утилит можно с посещения веб-сайта [www.packetstormsecurity.org/Crackers/bios/](http://www.packetstormsecurity.org/Crackers/bios/), на котором размещен список программ, предназначенных для взлома паролей BIOS.

## ИНСТРУМЕНТЫ АТАКИ ДЛЯ WINDOWS 3.X/9X/ME

Поскольку в семействе операционных систем Windows 3.x/9x/Me не предусмотрена защита от проникновения в систему неавторизованных пользователей, единственный вид атаки работающей системы связан с преодолением защиты «хранителя экрана» с заданным паролем. (Другие виды атак, направленные на взлом систем шифрования отдельных приложений и сетевой защиты в разных версиях Windows, описываются в главах 6 и 10 книги.) Обход защиты «хранителя экрана» возможен при помощи следующих инструментальных средств:

- **Ratware Win9x Screen Saver Buster.** Записав эту свободно распространяемую утилиту на CD-ROM и дописав ее автозапуск в файл autorun.inf, вы добьетесь отключения работающего «хранителя экрана». Найти данную утилиту можно по адресу: <http://packetstormsecurity.org/Win/RWSaverBust.zip>.
- **Scrsavpw.** Данная свободно распространяемая утилита, написанная Матиасом Бокэлкэмпом, предназначена для взлома паролей «хранителя экрана». Загрузить ее можно с веб-страницы [www.geocities.com/mbockelkamp/](http://www.geocities.com/mbockelkamp/).

## ИНСТРУМЕНТЫ АТАКИ ДЛЯ WINDOWS NT/2000/XP

С ростом популярности последних версий операционных систем Windows в корпоративном окружении у администраторов возникла необходимость в проведении более серьезного мониторинга системы безопасности, а иногда и в восстановлении информации с заблокированных систем. Им на встречу пошли производители ПО, выпустившие на рынок множество коммерческих и бесплатных инструментальных средств, необходимых для выполнения функций администратора, которые могут с тем же успехом использоваться в целях шпионажа. Далее мы обсудим ряд программных утилит для Windows NT/2000/XP, пользующихся одинаковой популярностью как у системных администраторов, так и среди профессиональных шпионов.

**LC (LOPHTCRACK).** Утилита LOptCrack (названная так в честь хакерской группы LOpt Heavey Industries, которая впоследствии стала частью консалтинговой компании по обеспечению корпоративной безопасности @Stake) на сегодняшний день является наиболее популярным средством взлома паролей для Windows NT/2000/XP. Ее последняя (на

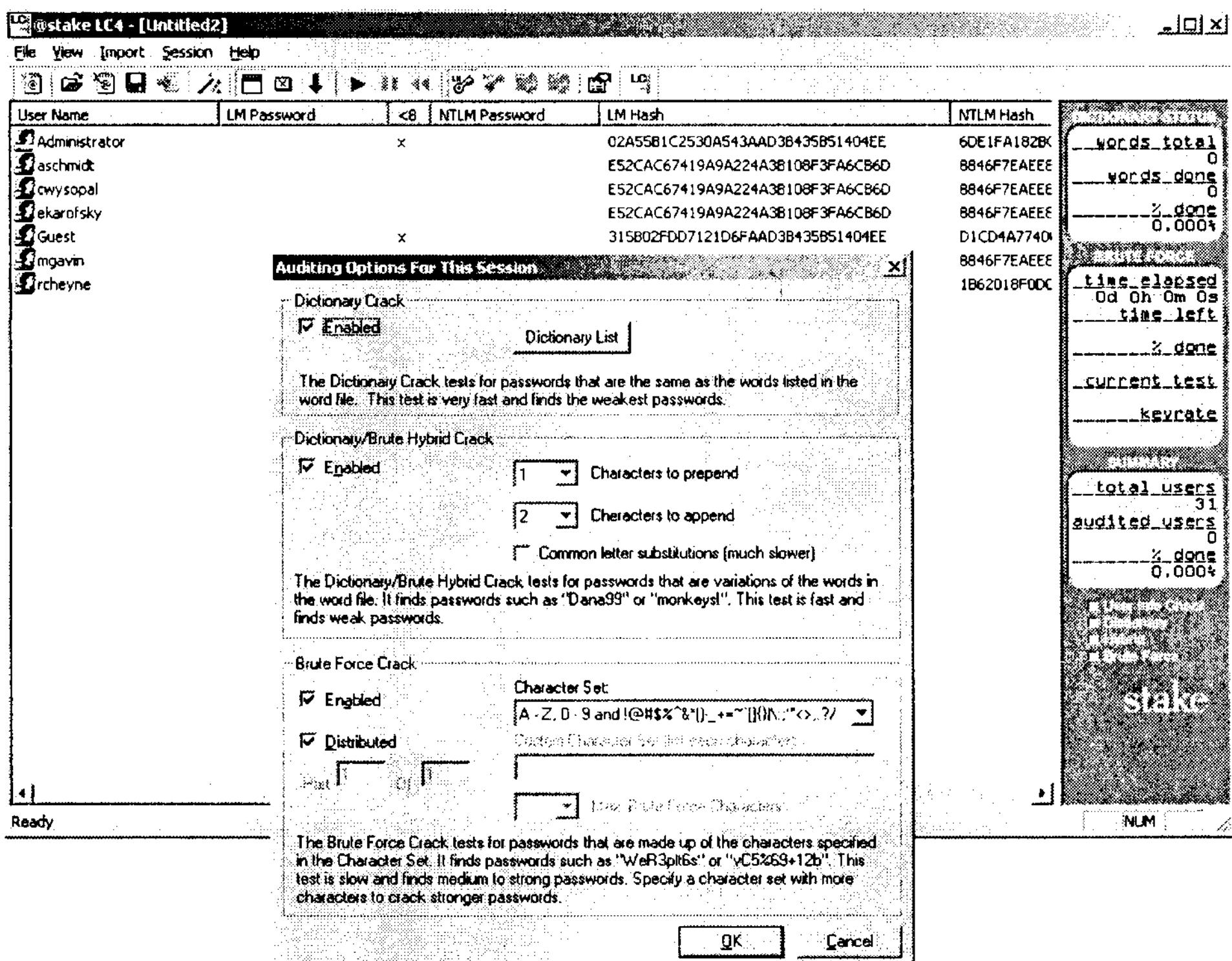
момент написания книги) версия 4.0 была названа политически более корректно – LC4, для того чтобы дистанцироваться от своих хакерских корней.

История программы LC, автором первых версий которой выступал Питер Затко (известный также под псевдонимом Mudge), началась в 1997 году с простой программки для взлома паролей методом перебора. С тех пор она превратилась в сложное инструментальное средство с простым и удобным интерфейсом (рис. 4.2), с возможностью распределения вычислительных ресурсов для «лобовой атаки» между несколькими компьютерами и поддержкой нескольких способов извлечения хешированных паролей:

- **Импорт с локальной машины.** LC позволяет извлекать всю хешированную информацию об учетных записях и паролях с локального компьютера, для чего требуются привилегии администратора.
- **Удаленный импорт из системного реестра.** Если в системе разрешен удаленный доступ к реестру, вы можете импортировать из него хешированные данные (при условии отсутствия Syskey).
- **SAM-файлы.** LC может напрямую считывать хешированные пароли из скопированных SAM-файлов, если они не защищены дополнительно при помощи системного ключа Syskey.
- **Перехват.** LC может перехватывать пароли в процессе обмена информацией, когда один компьютер подключается к другому в сети Ethernet.
- **Совместное использование с утилитой Pwdump.** LC позволяет импортировать хешированные пароли, собранные при помощи утилиты Pwdump. Эта утилита будет описана далее.
- **Импорт файлов из предыдущих версий LC.** Текущая версия LC обладает совместимостью сверху вниз, поддерживая предыдущие версии, в которых для хранения учетных записей и паролей использовались отдельные файлы разных форматов.

После загрузки хешированных паролей в LC утилита позволяет выполнять подбор паролей при помощи словаря, проводить гибридные словарные атаки, учитывающие добавление, подстановку или общепринятую замену буквенных сочетаний в словах, а также атаку «в лоб» (скорость лобовой атаки составляет 2 800 000 паролей в секунду на процессоре mobile Pentium III с тактовой частотой 1 ГГц).

Использование этой утилиты обойдется вам в каких-то \$350, но при этом она заслуженно считается одним из лучших средств для несанкционированного проникновения в систему (либо для законного аудита паролей). Если вы хотите получить более подробную информацию либо загрузить демонстрационную версию программы, посетите веб-сайт [www.atstake.com](http://www.atstake.com).



**Рис. 4.2.** Утилита для взлома паролей LC4 (LOphtCrack) выполняет расшифровку хешированных паролей. Пароли учетных записей могут быть расшифрованы при помощи словаря (Dictionary Crack), методом «лобовой» атаки (Brute Force Crack) и комбинированным методом

**ADVANCED NT SECURITY EXPLORER.** Эта коммерческая утилита позволяет выполнять подбор паролей при помощи словаря, масок символов (вы можете ввести известные вам символы пароля, и программа сосредоточится на отгадывании остальных) и «лобовой» атаки. Возможно извлечение хешированных паролей из памяти, системного реестра либо импорт из других утилит взлома паролей, таких как Pwdump. Скорость выполнения лобовой атаки исчисляется 2 000 000 проверяемых вариантов пароля в секунду на процессоре Intel mobile Pentium III с тактовой частотой 1 ГГц. Стоит Advanced NT Security Explorer \$49 за однопользовательскую лицензию, а демонстрационная версия доступна на веб-сайте [www.elcomsoft.com/antexp.html](http://www.elcomsoft.com/antexp.html).

## Тактика: FakeGINA

Аббревиатура GINA расшифровывается как Graphical Identification and Authorization mechanism (графический механизм идентификации и авторизации) для Windows NT/2000/XP. Динамическая библиотека GINA является промежуточным звеном между пользователем и службой аутентификации операционной системы, отвечающей за вывод диалогового окна входа в систему.

Один из способов несанкционированного проникновения в операционную систему заключается в выводе фальшивого окна аутентификации. Ничего не подозревающий пользователь, как всегда, вводит в соответствующих полях свое имя и пароль, однако на самом деле хакерское приложение («тロjanский конь», занесенный в систему взломщиком) осуществляет перехват и запись введенного пароля перед входом в систему. Именно в целях защиты от подобных приложений компания Microsoft задумала использование сочетания клавиш Ctrl+Alt+Del для вызова диалогового окна входа в систему, поскольку это сочетание клавиш распознается в первую очередь Windows и применяется для программной перезагрузки.

К сожалению, программисты Microsoft не приняли в расчет способностей других талантливых программистов, как, например, Арни Видстрома, который написал дополнительную библиотеку под названием FakeGINA, то есть «фальшивая GINA». Созданная им библиотека осуществляет перехват интерактивного обмена информацией между процессом winlogon.exe и GINA.dll – в результате имя домена, пользователя и пароль в случае успешной загрузки системы записываются в текстовый файл. А именно этого компания Microsoft пыталась избежать в первую очередь. FakeGINA работает благодаря копированию небольшого DLL-файла в системную папку \system32 и модификации ключей реестра, так что ключ библиотеки GINA.dll указывает на файл FakeGINA.dll. При входе пользователя в систему Windows 2000 или Windows NT 4.0 учетная запись пользователя и его пароль сохраняются в файл под названием passlist.txt. Познакомиться со столь забавной утилитой вы можете по адресу [www.ntsecurity.nu/toolbox/fakegina/](http://www.ntsecurity.nu/toolbox/fakegina/).

**PWDUMP.** Pwdump представляет собой утилиту командной строки, предназначенную для сохранения дампа хешированных паролей в Windows NT/2000/XP. Эта программа, первая версия которой была написана Джереми Элисон, предназначалась для извлечения информации о бюджетах пользователей и паролей из SAM-файлов с помощью технологии «инжекции динамической библиотеки». Не углубляясь в технические подробности, поясним, что Pwdump заставляет службу локальных средств защиты (LSA) выполнять в адресном пространстве процесса программный код, по-

зволяющий получать доступ к хешированным паролям. С появлением дополнительного системного ключа, предназначенного для 128-битного шифрования SAM-файла, Microsoft на время победила эту программу. Однако очень скоро, в ответ на действия Microsoft, Тод Сабин занялся развитием вышеупомянутой идеи и выпустил новую версию программы – Pwdump2, позволяющую извлекать хешированные пароли, невзирая на защиту с помощью системного ключа. Существует также версия Pwdump3, написанная Филом Стаубсом и Эриком Хелмстадом, которая основана на коде Pwdump2, но кроме всего прочего умеет извлекать хешированные пароли с удаленных компьютеров по сети. После извлечения хешированных паролей, их можно экспортить в такие утилиты, как LC или Advanced NT Security Explorer, для дальнейшей расшифровки. Для успешного запуска любой из версий Pwdump вам необходимо обладать полномочиями администратора данной системы.

Все версии Pwdump являются свободно распространяемыми, а загрузить их можно по следующим адресам в сети Интернет:

- Pwdump2 (<http://razor.bindview.com/tools/index.shtml>)
- Pwdump3 ([www.polivec.com/pwdump3.html](http://www.polivec.com/pwdump3.html)) \*

**ERD COMMANDER.** ERD Commander является многофункциональным программным продуктом для Windows NT/2000/XP, поставляемым в виде загрузочного CD-диска. Данный продукт был разработан в первую очередь для системных администраторов и предназначался для восстановления и диагностики поврежденных систем, но в то же время он обладает рядом возможностей, которые идеально подходят для шпиона, включая функции сброса паролей, редактирования реестра, копирования, перемещения и удаления файлов и выполнения системных команд. ERD Commander – отличное средство для среднестатистического пользователя, поскольку он имеет интуитивно понятный интерфейс обычного Рабочего стола Windows. Текущая версия программы, ERD Commander 2002, доступна по цене в \$399, а более подробную информацию о программе вы можете прочесть на официальном сайте производителя [www.winternals.com](http://www.winternals.com).

**CIA COMMANDER.** Утилита CIA Commander, разработанная немецкой компанией Datapol, полностью оправдывает свое шпионское название. Утилита позволяет менять пароли учетных записей, хранимых в SAM-файле, сохранять пароли учетных записей перед их изменением для последующего восстановления, модифицировать динамически подключаемую библиотеку GINA для отключения альтернативных способов аутентификации, например при помощи устройств считывания карт, и включает в себя файловый менеджер, позволяющий легко копировать и удалять файлы на жестком диске. CIA Commander обладает небольшим

\* Утилита доступна также по адресу <http://securitylab.ru/tools/22142.html>. – Прим. ред.

размером, что позволяет легко умещать ее на одну дискету, и простым интерфейсом. Стоимость программы составляет \$249, причем пробную версию вы можете загрузить с веб-узла [www.ciacommander.com](http://www.ciacommander.com).

## Тактика: *Wall Street Journal* против Аль-Кайды

В январе 2002 года популярное издание *Wall Street Journal* сообщило об успешном взломе файлов с управляемого системой Windows 2000 компьютера, доставленного из штаб-квартиры Аль-Кайды в Кабуле. На компьютерах террористов применялась файловая система EFS, однако ими использовалась более старая экспортная версия Windows с поддержкой 40-битного шифрования, в отличие от 128-битного шифрования в ОС Windows 2000, продаваемой на территории Соединенных Штатов. В соответствии с предоставленным для прессы отчетом, пароли были взломаны за пять дней при помощи группы компьютеров, объединенных в «клuster».

В Windows 2000 файловая система EFS обладает рядом уязвимых мест. По умолчанию бюджет Администратора имеет доступ к любым зашифрованным файлам и папкам, независимо от того, кем они были созданы. Поэтому, узнав пароль администратора, шпион получает неограниченный доступ к системе. Вдобавок при изменении при помощи утилиты Chntpw пароля пользователя для зашифрованных файлов шпион также может работать с файлами этого пользователя.

Любопытно, что работники *Wall Street Journal* заявили, что не применяли подобный тип атаки, но, поскольку подробности дела не были раскрыты, осмелимся подвергнуть это утверждение сомнению. Возможно, однако, что сам пароль интересовал журналистов не меньше, чем факт получения доступа к файлам, защищенным при помощи файловой системы EFS.

**ПРОГРАММЫ ОЧИСТКИ ЖУРНАЛОВ.** В операционных системах Windows NT/2000/XP существует возможность записи системных событий в журнал (хотя по умолчанию протоколирование событий системы безопасности не включено). Разумеется, при загрузке альтернативной операционной системы и выполнении манипуляций с файлами из нее эти события не будут отражены в журнале. Однако атака в рамках работающей системы может привести к обнаружению ваших действий. Если вы хотите действовать осторожно, вам необходимо удалить за собой любые следы ваших действий.

Советуем вам посетить веб-сайт Арни Видстрома, шведского эксперта по безопасности и плодовитого автора программных средств защиты Windows. На его веб-сайте [www.ntsecurity.net](http://www.ntsecurity.net) размещен целый ряд полезных программных утилит, пригодных для шпионажа (либо выполнения

задач системного администратора). В качестве инструментов очистки журналов событий Видстром предлагает две утилиты:

- **ClearLogs** – утилита, запускаемая из командной строки и позволяющая удалять журнал событий системы безопасности и приложений.
- **WinZapper** – средство, позволяющее проводить выборочное удаление событий из журнала безопасности систем Windows NT 4.0 и 2000.

Помните, что пустой журнал событий может вызвать подозрение у системного администратора или пользователя, имеющего опыт в вопросах безопасности. Иногда лучше вызвать преднамеренную порчу файла журнала, чтобы убедить пользователя в системной ошибке. Конечно, лучше всего, по возможности, провести избирательное удаление записей, касающихся выполненных вами действий.

**СРЕДСТВА АЛЬТЕРНАТИВЫ ОПЕРАЦИОННЫХ СИСТЕМ.** Для получения доступа к жесткому диску компьютера под управлением Windows NT/2000/XP также могут использоваться другие операционные системы, такие как DOS или Linux. Для этого вам понадобится создать загрузочный диск с соответствующими драйверами и утилитами, предназначенными для поддержки файловой системы NTFS, а затем атаковать систему путем просмотра, модификации либо копирования файлов с жесткого диска. (Операционные системы Windows NT/2000/XP поддерживают следующие файловые системы: FAT, FAT32 и NTFS. Если целевой диск отформатирован под FAT или FAT32, доступ к нему можно получить при помощи обычной загрузочной дискеты DOS.)

Более новые компьютеры, с предустановленной операционной системой Windows 2000/XP, обычно имеют жесткие диски, отформатированные под NTFS, поэтому вы не сможете получить к ним доступ с загрузочной дискеты DOS без помощи утилит сторонних разработчиков, таких как NTFSDOS. После запуска NTFSDOS вы получаете возможность работы с разделами NTFS в рамках DOS. Существует две версии NTFSDOS: одна, бесплатно распространяемая, позволяет получать доступ только для чтения; другая, коммерческая версия, позволяет как читать, так и изменять информацию в разделе NTFS. Бесплатная версия может пригодиться вам для просмотра содержимого жесткого диска и копирования нужных файлов. (Если файлы или папки защищены при помощи EFS, вы не сможете получить к ним доступ ни из бесплатной, ни из коммерческой версии программы.)

- Бесплатная версия утилиты NTFSDOS доступна на веб-сайте [www.sysinternals.com](http://www.sysinternals.com).
- Полную коммерческую версию NTFS DOS Professional по цене \$299 можно заказать на сайте [www.winternals.com](http://www.winternals.com).

Существует также две утилиты под Linux, которыми вы можете воспользоваться для атаки на компьютеры под управлением Windows NT/2000/XP:

- **Chntpw (Change NT password).** Эта утилита под Linux, запускаемая из командной строки, разработанная Питером Нордал-Хагеном, позволяет изменять пароли бюджетов пользователей в SAM-файле. Хаген сделал ее использование понятным даже для тех пользователей, которые незнакомы с ОС Linux, включив в состав программы образ загрузочного диска Linux с поддержкой NTFS, который легко может быть скопирован на дискету либо записан на CD-ROM. Вам останется только загрузиться при помощи этого диска и запустить утилиту. Программа Chntpw распространяется бесплатно: вы можете загрузить ее по адресу <http://home.eunet.no/~pnordahl/ntpasswd/>.

### Тактика: «хранитель экрана» или источник разочарований?

Если вы обладаете полным доступом к целевому жесткому диску, еще один способ атаки на систему заключается в использовании файла Logon.scr. После появления диалогового окна входа в систему в Windows NT/2000/XP и в случае отсутствия активности со стороны пользователя в течение некоторого времени, происходит запуск файла Logon.scr, осуществляющего вывод используемого по умолчанию «хранителя экрана».

Вам понадобится загрузить компьютер при помощи другой операционной системы и переименовать файл Logon.scr, находящийся в папке \winnt\system32 (Windows NT/2000) либо \windows\system32 (для Windows XP). Затем необходимо сделать копию файла cmd.exe, переименовав ее в Logon.scr.

После этого перезапустите компьютер и подождите, пока загрузится Windows. После появления диалогового окна входа в систему ничего не вводите и не трогайте мышь. Приблизительно через пятнадцать минут бездействия автоматически запустится файл Logon.scr. Но на этот раз вместо «хранителя экрана» появится оболочка cmd.exe, запущенная с привилегиями системного процесса. С этого момента вы сможете делать из командной строки все, что угодно, включая создание новых учетных записей с полномочиями администратора.

- **John the Ripper.** Это популярная утилита для взлома паролей под UNIX, которая тем не менее запускается под множеством других операционных систем и обладает широкими возможностями. Вместе с программой распространяется ее исходный код, так что при желании вы сможете скомпилировать собственную версию утилиты для взлома SAM-файла. Загрузить программу можно с веб-страницы [www.openwall.com/john/](http://www.openwall.com/john/).

# Контрмеры

В данном разделе мы расскажем вам о контрмерах, позволяющих держать на расстоянии коварных агентов КГБ и других лиц, заинтересованных в имеющейся у вас информации. В первую очередь вам, разумеется, необходимо заняться ужесточением физических мер защиты вашего компьютера, о которых шла речь в третьей главе. Защитив ваш компьютер от физического проникновения извне, вы уже сделаете половину дела. Но даже если вы не в состоянии обеспечить должные меры физической защиты компьютера, существуют способы, которые могут сделать доступ к вашим данным задачей далеко не тривиальной.

## Настройки безопасности

Сейчас мы поговорим о настройках BIOS и операционной системы, позволяющих снизить шансы на успех у людей, стремящихся завладеть вашей конфиденциальной информацией. Но перед тем как изменять какие-либо настройки операционной системы, убедитесь в том, что для вашей версии Windows установлены все текущие пакеты обновления, включая свежие «заплаты» системы безопасности. Квалифицированный компьютерный шпион, как правило, постоянно находится в курсе событий и знает обо всех последних обнаруженных уязвимых местах, которые могут быть использованы для проникновения в систему. Поэтому своевременное обновление системы уменьшает шансы злоумышленников на успешное проведение локальных или удаленных атак.

Корпорация Microsoft предлагает множество свободно распространяемых утилит и источников информации, чтобы обеспечить защиту своих программных продуктов от обнаруженных брешей:

- **Бюллетени по безопасности Microsoft (Microsoft Security Bulletins).** Компания Microsoft регулярно выпускает бюллетени безопасности с описаниями обнаруженных ошибок в защите системы и «горячими заплатами» для них. Эти бюллетени и другие ресурсы доступны по адресу [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security). Вы будете находиться в курсе всех последних событий, если подпишетесь на службу уведомлений безопасности компании Microsoft (Microsoft's Security Notification Service), отослав пустое письмо по адресу [securbas@microsoft.com](mailto:securbas@microsoft.com).
- **Служба автоматического обновления Windows.** В Windows 2000 и Windows XP встроена служба автоматического обновления компонентов Windows, осуществляющая поиск и загрузку последних обновлений для вашей операционной системы. Включив эту опцию, вы разрешите вашему компьютеру периодически подключаться через Интернет к домашней странице компании Microsoft, чтобы проверять наличие обновлений.

(Раньше между публикацией бюллетеня по безопасности Microsoft и появлением соответствующих заплат на узле Windows Update проходили дни и даже недели. Поэтому, если вы всерьез обеспокоены защищенностью вашей системы, не полагайтесь исключительно на службу автоматического обновления.)

- **«Горячие обновления» средств сетевой безопасности Microsoft (hfnetchk.exe).** Утилита Hotfix Checker, запускаемая из командной строки, проверяет наличие «заплат» для системы безопасности (с декабря 2002 года функциональность данной утилиты интегрирована в Microsoft's Baseline Security Advisor). Загрузить программу и получить подробные рекомендации по ее использованию вы можете по адресу <http://support.microsoft.com/default.aspx?scid=KB;en-us;q303215>.

Удовствовившись, что ваша операционная система и потенциально уязвимые приложения являются максимально защищенными на данный момент времени, можете смело переходить к рассмотрению рекомендуемых настроек безопасности.

## BIOS

Несмотря на множество способов обхода парольной защиты BIOS, не отказывайтесь от их использования, если вы заинтересованы в надежной защите вашей системы. Заданный в BIOS пароль отпугнет рядового същика либо неопытного шпиона и, по крайней мере, замедлит работу профессионала. Причем обязательно следует задавать оба пароля: как на загрузку компьютера, так и на изменение настроек в BIOS.

В качестве дополнительной меры предосторожности можно отключить в BIOS опции альтернативной загрузки с дискеты, CD-ROM или других устройств USB. Вы всегда сможете включить опции альтернативной загрузки обратно, если с системой или жестким диском случится какая-то неприятность.

## WINDOWS 3.X/9X/ME

Не надейтесь на надежную защиту системы, если вы используете операционную систему Windows 3.X/9X/Me. (Вы только сможете защитить себя от автозапуска CD, выбрав пункт Свойства в контекстном меню значка Мой компьютер, а затем сбросив флажок «автоматическое распознавание диска» для вкладки CD-ROM в Диспетчере устройств).

Если шпион получил физический доступ к вашему компьютеру, работающему под управлением более старых версий Windows, вы не сможете защитить ваши данные от просмотра. Лучшее, что вы можете сделать в этом случае, – воспользоваться описываемыми в данной книге мерами безопасности, не связанными с конкретной операционной системой. Однако, если вы серьезно обеспокоены вопросами безопасности, подумайте об обновлении операционной системы до уровня Windows 2000/XP или попробуйте Linux.

## WINDOWS NT/2000/XP

В отличие от предыдущих версий Windows, делающих акцент на удобстве использования, операционные системы семейства Windows NT/2000/XP предоставляют большие возможности в плане безопасности. Однако учите, что многие настройки безопасности, позволяющие повысить защищенность системы, не включены по умолчанию. Поэтому, вам придется потратить некоторое время на конфигурирование системы, чтобы обезопасить себя от плохих парней.



Microsoft Baseline Security Analyzer представляет собой бесплатно распространяемую утилиту, которая выполняет анализ конфигурации вашей системы (Windows 2000/XP) и предлагает меры по увеличению надежности защиты системы. Вы можете загрузить программу с веб-узла [www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp](http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp).

Чтобы повысить надежность и защищенность системы, необходимо прибегнуть к следующим мерам безопасности (многие из перечисленных ниже опций можно менять в настройках локальной безопасности, набрав в командной строке `secpol.msc`):

- **Используйте файловую систему NTFS.** Файловые системы FAT и FAT32 не предоставляют защиты на уровне файлов и папок, поэтому доступ к жесткому диску возможен при помощи обычной загрузочной дискеты DOS.
- **Отключите учетную запись Гостя.** Не предоставайте шпиону отправной точки, с помощью которой он может попытаться расширить свои привилегии.
- **Переименовывайте учетную запись Администратора.** Любой мало-мальски грамотный шпион знает имя учетной записи по умолчанию и может сразу направить свои попытки на подбор пароля к ней. Воспользуйтесь другим именем учетной записи для настоящего администратора компьютера (которая бы вообще не напоминала о принадлежности данного пользователя к категории администраторов), а затем создайте фальшивую учетную запись с именем Администратор и сложным паролем, не обладающую на самом деле никакими привилегиями. Так вы сбьете злоумышленника с толку, заставив его направить свои усилия в ложном направлении.
- **Отключите вывод имени последнего входившего в систему пользователя.** Это можно сделать в настройках локальной политики безопасности (Local Policies), и тогда в диалоговом окне входа в систему не будет отображаться имя последнего пользователя. Это усложнит задачу взломщика, поскольку ему понадобится угадывать не только пароль, но и имя учетной записи пользователя.

- **Соблюдайте строгую политику паролей.** В разделе политики паролей (Password Policy) настроек локальной безопасности надо задать минимально необходимую длину пароля, его сложность и время действия. Вообще-то, пароль должен иметь в длину не менее 8 символов, состоять из сочетания букв, цифр и символов и меняться не реже, чем раз в 3 месяца.
- **Разрешите блокирование учетных записей пользователей.** Там же, в настройках локальной безопасности, в разделе блокировки бюджетов (Account Lockout Policy), необходимо задать блокирование учетной записи пользователя после определенного количества неудачных попыток входа в систему (хотя заблокировать таким образом встроенную учетную запись Администратора нельзя). Опция длительности блокирования учетной записи позволяет задать время, в течение которого пользователь не сможет совершать повторные попытки входа в систему. К примеру, если количество неудачных попыток сделать равным трем, а продолжительность установить равной 15 минутам, шпион, испробовав три варианта пароля, сможет совершить четвертую попытку не ранее, чем через 15 минут.
- **Включите запись событий в журнал.** По умолчанию часть событий, связанных с системой безопасности, в журнал не заносятся. Вы должны сами включить их регистрацию и периодически проверять журнал, чтобы вовремя обнаружить попытки несанкционированного проникновения в систему. Необходимо включить запись в журнал следующих событий:
  - события учетных записей (успехи, неудачи);
  - управление учетными записями (успехи, неудачи);
  - события входа в систему (успехи, неудачи);
  - доступ к объектам (успехи);
  - изменения политик (успехи, неудачи);
  - использование полномочий (успехи, неудачи);
  - события системы (успехи, неудачи).
- **Подумайте об использовании дополнительных мер безопасности помимо системного ключа.** Хотя включение шифрования при помощи системного ключа Syskey увеличивает защищенность хешированных паролей, обдумайте также возможность использования загрузочной ключевой дискеты. Обычно загрузочный системный ключ хранится на жестком диске, но вы можете настроить систему таким образом, что она будет требовать ввода пароля либо вставки ключевого диска для входа в систему. Однако отнеситесь к этому способу с осторожностью, поскольку в случае утери этой дискеты вы не сможете загрузить Windows, и вам останется только переустанавливать ее.

- **Будьте осторожны с подсказками для паролей в Windows XP.** Учтите, что легко угадываемая подсказка для пароля и известное имя пользователя значительно облегчат задачу проникновению в вашу систему для взломщика.
- **Защищайте «хранители экрана» при помощи пароля.** Не забывайте защищать паролями работающие «хранители экрана», чтобы не допустить кого-либо к вашему компьютеру, когда он находится без присмотра.

Более подробно о реализации этих и других настроек безопасности можно прочесть на веб-сайте <http://labmice.net> – отличном веб-ресурсе, предназначенном для администраторов и пользователей Windows NT/2000/XP.

### **Контрмеры: чем больше, тем лучше**

Как вы уже знаете, для надежной защиты системы необходимо использовать пароли длиной не менее 8 символов, мы же рекомендуем применять пароли длиной в 15 и более символов для Windows 2000 или XP, причем не только потому, что чем длиннее пароль, тем сложнее его отгадать. В данном случае пароли такой длины обеспечивают дополнительный уровень защиты в смешанном сетевом окружении.

Дело в том, что в сети, где присутствуют компьютеры под управлением Windows 3.x/9x/Me, для хеширования паролей на всех компьютерах операционная система использует Диспетчер сети (LAN Manager). Хешированные с его помощью пароли взломать намного легче, чем при использовании более безопасных методов аутентификации NTML или Kerberos, и даже если пароль имеет в длину более 8 символов, его несложно раскрыть из-за ненадежной схемы хеширования, используемой Диспетчером сети.

Однако в случае применения пароля длиной в 15 и более символов в процессе аутентификации Windows 2000 и XP возникает одна ошибка: вне зависимости от самого пароля, Диспетчер сети выполняет хеширование с помощью одного и того же значения. Благодаря этому разгадать пароль при помощи утилит вроде LC становится чрезвычайно сложно (в LC4 хешированный пароль, имеющий 15 и более символов в длину, отображается как «пустой»). Скорее всего, это связано с тем, что в Windows NT максимальная длина пароля составляла 14 символов (для Windows 2000 и XP она может достигать 127 символов).



Помимо шпионажа, Управление национальной безопасности также отвечает за поддержание безопасности правительственные компьютерных систем. Управлением была опубликована серия Рекомендаций по безопасности для Windows NT/2000/XP, которые включали .inf-файлы с предлагаемыми политиками безопасности. Текст рекомендаций и файлы политик вы можете загрузить с веб-узла [www.nsa.gov/snac/index.html](http://www.nsa.gov/snac/index.html).

## Надежные пароли

Когда речь заходит о паролях, используемых для аутентификации пользователей (либо для других целей, требующих поддержания высокого уровня безопасности), никогда не используйте простые пароли! Ваш компьютер становится легкой мишенью для шпиона, когда вы начинаете использовать слишком короткие или простые пароли. О том, чем грозит для вас использование простых паролей и как выбрать надежный пароль, вы сможете прочесть в разделе «Контрмеры» шестой главы книги.

## Шифрование

Любые конфиденциальные данные на вашем жестком диске должны быть зашифрованы. Даже если злоумышленник преодолеет уровни защиты BIOS и операционной системы, при использовании устойчивых систем шифрования критичная для вас информация не пострадает. Шифрованная файловая система Microsoft (EFS) обеспечивает приемлемый уровень защиты под Windows XP Professional – хотя использование EFS в Windows 2000 не так надежно и подвержено атакам различных типов. Более подробно об устойчивых системах и надежных утилитах шифрования вы узнаете из раздела «Контрмеры» шестой главы книги.

## Заключение

Итак, мы выяснили, что первыми линиями обороны на пути шпиона, получившего физический доступ к вашему компьютеру, являются защита при помощи пароля BIOS и авторизация пользователя при входе в систему. Хотя для обеспечения безопасности системы существует также масса других средств, не пренебрегайте возможностями настроек безопасности BIOS и операционной системы Windows. Эти защитные меры обезопасят вас от рядового шпиона и даже могут отпугнуть профессионала, заставив его заняться поиском более легкой цели. Кроме того, не зацикливайтесь только на сетевых видах атак: не меньшую важность представляет физическая защита компьютера и соблюдение локальной политики безопасности.

## Глава 5

# В поиске доказательств

«Это – как смотреть детективы. От этого вы не сделаетесь сообразительнее!»

Элвис Костелло, сингл «Watching the Detectives» из альбома *My Aim is True*

## Законное наблюдение

Некоторым людям платят за то, чтобы они легально шпионили за компьютерами других людей. Компьютерные специалисты – полицейские и судебные эксперты бывают за байтом анализируя информацию, хранимую на жестких дисках и других электронных носителях, ищут информацию и доказательства, которые бы могли послужить подтверждением или опровержением возникших подозрений.

Компьютерные полицейские работают на правоохранительные органы. В этой роли могут выступать принявшие присягу полицейские либо гражданские консультанты. Аналогичные функции в частном секторе выполняют компьютерные судебные эксперты, делающие ту же самую работу, только по заказу корпораций или юристов. Судебных экспертов не заботит наличие соответствующего значка и пистолета, поскольку это компенсируется более высоким уровнем оплаты труда.

Забудьте об опасностях, на каждом шагу подстерегавших Джеймса Бонда, интригах и романах с его активным участием. Все это не имеет никакого отношения к компьютерному шпионажу. В судебных расследованиях все сводится к нудному и кропотливому труду, связанному с изучением мельчайших подробностей. Вам придется просматривать миллионы байтов в шестнадцатеричной системе с секторов жесткого диска в поисках доказательств, которых здесь может и не быть. Компьютерные полицейские вынуждены сталкиваться с самыми темными сторонами человеческой природы, например, при расследовании дел, связанных с распространением детской порнографии.

В данной главе мы расскажем вам о кропотливом труде компьютерных полицейских и судебных экспертов, а также об используемой ими технике и средствах для поиска информации и улик. Затем, познакомив вас со шпионским инструментарием, мы поговорим о контрмерах, которые помогут вам защититься от вышеперечисленных способов атаки.

## Как работают компьютерные полицейские

И компьютерные полицейские, и судебные эксперты выполняют одну и ту же работу: ищут компьютерные доказательства причастности подозреваемых к противозаконной деятельности, включая даже те крупицы информации, которые могут когда-нибудь вывести их на преступника. Для полицейского это может означать просмотр записей о принятых ставках на конфискованном у букмекерской конторы компьютере, для частного эксперта – восстановление удаленных файлов, связанных со скандалом в коррумпированной бухгалтерской фирме.

Расследования обеих разновидностей подразумевают применение схожих методов и процедур. Главная разница состоит в том, что полицейские вынуждены придерживаться более строгих правил при обращении с компьютером, который может содержать важные свидетельства. К примеру, если полицейскому для проникновения в офис с целью сбора компьютерных улик необходим официальный судебный ордер, то эксперту, работающему в этой корпорации, достаточно получить разрешение от руководства компании на осмотр компьютера одного из сотрудников.

Данный параграф мы посвятим, главным образом, полицейским, занимающимся расследованиями компьютерных преступлений. Тем не менее, поскольку многие технологии и навыки, используемые обеими категориями легальных шпионов, нередко совпадают, большинство из того, что мы расскажем о полицейских, справедливо и для других компьютерных экспертов.

Начнем с того, что уровень знаний и навыков отдельных индивидуумов как среди полицейских, так и среди технических экспертов варьируются в широких пределах. Немногие компьютерные полицейские сумеют дизассемблировать утилиту шифрования, подавляющее большинство пользуется готовыми к использованию программными утилитами для выполнения своей работы. Практика показывает, что на сегодняшний день большинство полицейских, занимающихся расследованием компьютерных преступлений, прежде всего являются полицейскими, а не техническими специалистами, решившими поступить на службу в полицию. (Правоохранительные органы иногда нанимают на работу технических специалистов с компьютерным образованием и соответствующим опытом работы в данной области, а также частных экспертов, которые обычно обладают более глубокими техническими познаниями, чем их коллеги из полиции. Кроме того, из-за своей чрезмерной загруженности некоторые правительственные организации обращаются за помощью по сбору и обработке компьютерных улик в частные консалтинговые фирмы.)

Поскольку мало кто из компьютерных полицейских начинал свою карьеру с хакерства в подростковом возрасте, для таких работников существует множество частных и государственных организаций, предлагающих обучение на компьютерного эксперта, с выдачей в конце обучения соответствующего сертификата. Сертификация работников полиции вызвана частой необходимостью дачи показаний в суде, чтобы их можно было рассматривать как показания специалиста.

## Разоблачения: региональные компьютерные экспертные лаборатории

В ноябре 2000 года ФБР открыла первую региональную компьютерную экспертную лабораторию (RCFL) в Сан-Диего, Калифорния. Эта лаборатория начала сотрудничать со многими управлениями и множеством юрисдикций. В ее штате работают 18 компьютерных специалистов – полицейских, занимающихся расследованием компьютерных преступлений в округе Сан-Диего. За первый год своего существования лаборатория расследовала более 400 дел, став образцом для других региональных экспертных лабораторий, которые начали открываться по всей стране.

Перечислим нашумевшие дела, по которым в сборе улик помогала региональная экспертная компьютерная лаборатория Сан-Диего:

- Дело Майкла Крэга Дикмана, по прозвищу «Редкозубый Бандит», приговоренного к девяти годам тюремного заключения за ограбление 12 местных банков. Компьютерные эксперты нашли копии записок бывшего биотехника, которые он передавал служащим банка во время ограбления. Причем файлы с текстом записок были восстановлены с ноутбука, который он попросил сестру забрать из его дома.
- Дело Артура Жерардо и Валерии Бейблер, осужденных за издевательства и убийство своей сожительницы, помогшей им сфальсифицировать чеки и документы. На изъятом в ходе расследования компьютере были обнаружены отсканированные изображения чеков и водительских прав, предназначавшихся для дальнейшего цифрового редактирования.
- Дело Чарльза «Энди» Уильямса, подростка, признанного виновным по обвинениям в убийстве двух своих одноклассников и нанесении телесных повреждений тринадцати школьникам в колледже Сантаны в марте 2001 года. В ходе расследования было также изучено содержимое компьютера Уильямса.
- Дело Дэвида Уэстерафилда, признанного в августе 2002 года виновным в похищении и убийстве семилетнего ребенка соседей Даниэля Ван Дама. На компьютере Уэстерафилда было обнаружено около 64 000 фотографий и 2200 видеоклипов (85 восстановленных фотографий содержали изображения насилиемых подростков и несовершеннолетних).



В июле 2001 года Министерство юстиции выпустило великолепный справочник под названием «Расследование электронных преступлений: руководство для начинающих». Это небольшое пособие, написанное простым и доступным языком, предназначено в первую очередь для представителей правоохранительных органов, не владеющих глубокими техническими познаниями, тем не менее даже технические специалисты найдут в нем для себя массу ценной информации. Найти его электронную версию можно по адресу [www.ncjrs.org/pdffiles1/nij/187736.pdf](http://www.ncjrs.org/pdffiles1/nij/187736.pdf).

Обычно компьютерные полицейские работают в офисах и лабораториях со специальным программным и аппаратным обеспечением, предназначенным для обработки улик. Не так давно только федеральные и крупные муниципальные учреждения могли позволить себе нанимать специалистов и обеспечивать их нужным оборудованием, но сейчас, когда компьютеры прочно вошли в нашу повседневную жизнь, даже небольшие отделы включают в бюджет оплату труда компьютерных экспертов на полный или частичный рабочий день.

В отличие от шпионов, полицейские в большинстве случаев не стремятся скрыть следы своей деятельности, если только они не привлечены для участия в тайных проникновениях (мероприятиях по незаметному вторжению в частную собственность для сбора информации или улик). Полицейские обычно и так имеют доступ к аппаратному и программному обеспечению принадлежащего злоумышленнику компьютера и в первую очередь заинтересованы в поиске доказательств, подтверждающих связь подозреваемого с совершенным преступлением.

В настоящее время необходимость в услугах компьютерных полицейских (и частных экспертов также) огромна, поэтому вызывает сомнение тот факт, что существующее предложение специалистов сможет удовлетворить растущий на них спрос. Несмотря на то, что правоохранительные органы понимают важность наличия квалифицированных кадров, которые могли бы «по байтам» вычислить улики, полиция сталкивается все с новыми препятствиями на пути борьбы с преступностью:

- **Увеличение объема жестких дисков.** Чем больше объем информации, тем тяжелее ее обработать, и тем больше времени это занимает. Сейчас, когда общедоступными стали винчестеры объемом 100...200 Гбайт, копирование данных с них с последующим поиском улик требует все больше времени и большего количества электронных носителей для создания резервных копий. Что, в свою очередь, приводит к росту бюджетных расходов.
- **Повышение технической образованности преступников.** Поскольку правонарушители составляют определенный процент от общего числа населения, а новое поколение учится компьютерной грамотности с пеленок, те представители нового поколения, которые ступают на преступную стезю, часто могут бросить вызов даже опытным полицейским, когда дело касается компьютерных технологий.

## Контрмеры: сертификация

К наиболее известным организациям, предлагающим услуги по обучению навыкам расследования компьютерных преступлений, включая вашу сертификацию как специалиста, относятся:

- **Международная ассоциация специалистов по компьютерным расследованиям (International Association of Computer Investigative Specialists – IACIS).** IACIS является бесприбыльной организацией, помогающей готовить компьютерных специалистов для работы в правоохранительных органах. Ее программы подготовки и сертификации признаются многими учреждениями. Более подробно об этой ассоциации вы сможете прочесть по адресу [www.cops.org](http://www.cops.org).
- **Ассоциация расследования преступлений, связанных с применением высоких технологий (High Technology Crime Investigative Association – HTcia).** Эта профессиональная организация включает в себя как представителей правоохранительных органов, так и частных лиц, занимающихся расследованием преступлений. Ассоциация имеет региональные представительства и довольно регулярно проводит конференции и обучающие тренинги. Получить дополнительную информацию о деятельности HTcia можно на веб-странице [www.htcia.org](http://www.htcia.org).
- **Национальный Центр административных преступлений (National White Collar Crime Center – NWCC).** Этот центр предлагает услуги по бесплатной компьютерной подготовке работников правоохранительных органов. Центр проводит обучающие курсы по всей стране. Его адрес в Интернете: [www.cybercrime.org](http://www.cybercrime.org).
- **New Technologies Inc (NTI).** Эта коммерческая компания из Орегона занимается производством программного обеспечения и обучением компьютерных экспертов среди полицейских и гражданских лиц. Узнать о ней поподробнее вы сможете, посетив ее официальный сайт: [www.forensics-intl.com](http://www.forensics-intl.com).

- **Увеличение количества дел, связанных с компьютерными преступлениями.** Применение компьютерной техники в различных видах преступлений постоянно расширяется. Десять лет назад компьютерные полицейские были заняты расследованием административных правонарушений и нечастых случаев хакерства. Теперь же они вынуждены изучать компьютерные доказательства по делам, связанным с наркотиками, самоубийствами и

убийствами, мошенничеством и многими другими преступлениями, в которых, так или иначе, фигурирует компьютерная техника.

Хотя работа компьютерного полицейского включает в себя множество элементов, ее можно разделить на три основных этапа: конфискацию носителя информации, копирование данных и их изучение. Давайте рассмотрим каждый этап по порядку.

## Конфискация

Перед тем как вы сможете начать поиск компьютерных доказательств совершенных преступлений, вам, разумеется, необходимо получить доступ к самому компьютеру, что, как правило, означает конфискацию системного блока и электронных (или неэлектронных) носителей информации, которые могут иметь отношение к расследованию. (В некоторых случаях для проведения конфискации имущества могут привлекаться и частные судебные эксперты.)

Конституция запрещает полиции просто так врываться в дома граждан и арестовывать технику, если возникло подозрение в совершении преступления. Перед тем как произвести конфискацию, представители правоохранительных органов обязаны получить судебный ордер. Когда дело касается компьютеров, компьютерные полицейские помогают в составлении формулировки заявки на ордер. Ордер на обыск должен быть точно сформулирован, чтобы его можно было предъявить в суде во время рассмотрения дела подозреваемого. Поэтому в ордере должно быть четко оговорено, какие компьютеры и связанное с ними аппаратное обеспечение должны быть изъяты для дальнейшего изучения.

После предоставления ордера на обыск он приводится в исполнение. В зависимости от того, кто является вашим подозреваемым – простой клерк или знаменитый террорист, и от того, какое преступление он совершил, обыск может начаться с деликатного стука в дверь или же с грохота стенобитного орудия вместе с десятком нацеленных на дом стволов.

Поскольку изучение улик редко можно провести непосредственно на месте их изъятия, в ходе конфискации компьютерной техники и электронных доказательств представители полиции должны выполнить следующие действия:

- **Обеспечить защиту места преступления.** Вам необходимо удалить из помещения всех людей для сбора доказательств. Если компьютер включен, не трогайте его. Если он выключен, не включайте его. (Если компьютер включен, необходимо записать содержимое экрана, а затем вытащить тот конец шнура питания, который подключается к системному блоку компьютера, а не к настенной розетке.)

- **Защитить неустойчивые данные.** Любые устройства, хранящие данные в энергозависимой памяти (пейджеры, сотовые телефоны, КПК и т. д.), должны быть задокументированы и подключены к источнику питания.
- **Идентифицировать телефонные линии и сетевые кабели, подключенные к компьютеру.** Необходимо отключить все телефонные и кабельные линии от компьютера и пометить каждый шнур.
- **Провести предварительный опрос.** После установления личности всех присутствующих на месте обыска (свидетелей, подозреваемых и других людей), необходимо выяснить, кто является хозяином компьютера, узнать пароли и дополнительные, используемые владельцем меры безопасности; уточнить, существуют ли где-то резервные копии данных. (Иногда просто удивляет, сколько информации люди готовы сообщить полиции добровольно.)
- **Задокументировать состояние помещения, в котором проводится обыск.** Перед началом изучения либо перемещения каких-либо предметов необходимо сфотографировать или целиком записать на видеопленку место обыска, а также сделать снимки компьютера, монитора и периферии крупным планом. Не забывайте делать письменные заметки помимо визуальной документации.
- **Заняться непосредственно сбором доказательств.** Улики могут быть представлены в электронной и неэлектронной форме. Любые бумажные записки, пароли, руководства или документы, имеющие отношение к преступлению, должны быть собраны. Для конфискации включенного компьютера вначале выдерните шнур питания из системного блока, а в случае с ноутбуком удалите батарею, чтобы не допустить удаления данных какими-либо программными средствами в случае использования стандартной процедуры выключения питания. Заклейте лентой все слоты для приводов и разъем пит器ия. Запишите производителя, модель и серийный номер компьютера.
- **Упаковать и перевезти доказательства.** Все собранные вами улики должны быть тщательным образом инвентаризованы и классифицированы. Нужно пометить все шнуры и соответствующие им разъемы (например, отметьте буквой М разъем для подключения мыши и поставьте букву М на самом шнуре от мыши). Если во время обыска изымается сразу несколько компьютеров, необходимо так пронумеровать периферию и компьютеры, чтобы впоследствии знать, какое устройство к какому компьютеру следует подключить. Любые магнитные носители информации должны быть помещены в бумагу или антистатические пластиковые пакеты. Во время транспортировки компьютерной техники необходимо защитить ее от ударов и

сильных вибраций. Избегайте попадания электронных носителей информации в магнитные поля (от радио, наушников/колонок, сидений с подогревом), предохраняйте их от сильного перегрева, переохлаждения либо повышенной влажности.

- **Обеспечить хранение доказательств.** В соответствии с политикой полицейского отдела оговаривается способ хранения улик, однако при этом необходимо учитывать, что компьютерная техника должна быть защищена от перегрева, переохлаждения, повышенной влажности и прямого попадания воды, пыли и источников электромагнитного излучения. В ходе одного из расследований по делу о распространении детской порнографии доказательства хранились в подвале почтового отделения. Преступники вышли сухими из воды, поскольку в результате нескольких наводнений улики, в роли которых выступали компьютеры, покрылись ржавчиной, а дискеты – слоем плесени.

После сбора улик, их транспортировки и отправки на хранение компьютерные полицейские должны скопировать содержимое всех носителей информации, связанных с данным расследованием, для последующего анализа.



Выпущенное Министерством юстиции руководство «Поиск и изъятие компьютеров и прочих электронных доказательств в ходе уголовных расследований» вы можете найти в сети Интернет по адресу [www.cybercrime.gov/s&smanual2002.htm](http://www.cybercrime.gov/s&smanual2002.htm).

### Тактика: цепочка владельцев

Понимание концепции «цепочки владельцев» важно для успешного ведения уголовных и гражданских расследований. Под нею подразумевается обязательное фиксирование информации обо всех, кто прикасался к данной улике с момента ее изъятия и до момента помещения в хранилище доказательств. Это необходимо для того, чтобы не допустить фальсификации доказательств, что особенно важно, когда в деле фигурируют компьютерные доказательства, которые слишком легко изменить.

Документы по «цепочке владельцев» обычно оформляются в виде журнала, в котором хранятся сведения обо всех лицах, имевших доступ к данной улике, присвоенный ей уникальный номер и ее место в хранилище доказательств.

## Дублирование информации

Перед тем как начать анализ содержимого компьютера, необходимо создать дубликат жесткого диска либо других электронных носителей информации, изъятых в качестве улик. Главное правило любого компьютерного эксперта заключается в том, чтобы никогда не заниматься изучением оригинального носителя, а использовать его точную копию. Это важно по двум причинам:

- Если анализировать содержимое жесткого диска, запустив установленную на нем систему, то открытие каких-либо файлов может привести к непреднамеренному изменению доказательств. Даже процесс загрузки операционной системы может привести к изменению файлов.
- Поскольку данные, хранимые в цифровой форме, очень легко изменить, у обвинителей либо адвокатов может возникнуть вопрос о подлинности данных и возможности их фальсификации, если эксперты изучали оригиналный носитель, выступающий в роли единственного доказательства.

Создание дубликатов оригинальных носителей может выполняться как непосредственно на месте сбора улик, так и в полицейском офисе или лаборатории. Большинство полицейских предпочитают делать это в офисе, поскольку там в их распоряжении находятся все необходимые средства и оборудование. Однако в некоторых случаях, например в ходе тайного проникновения, может потребоваться копирование информации на месте.

Чтобы гарантировать подлинность свидетельств для представления их в суде, выполняются следующие процедуры:

1. Компьютер загружается с помощью другой операционной системы, например DOS или Linux. Затем путем подсчета контрольной суммы или безопасным хешированием (например, с помощью алгоритмов SHA-1 или MD-5) создаются цифровые подписи для файлов и папок. (Использование альтернативной операционной системы предотвращает внесение изменений в файлы во время загрузки системы.)
2. При помощи утилит DOS или Linux создается точная копия (образ) жесткого диска (некоторые из таких средств перечислены в параграфе «Средства сбора доказательств» данной главы). Копия должна создаваться на абсолютно пустом носителе (на новом жестком диске или ленте) либо на очищенном электронном носителе, не содержащем остаточных данных.
3. После окончания копирования применяется программа проверки контрольной суммы либо утилита хеширования для проверки идентичности дубликата оригиналу.

4. Проводится обязательное документирование всего процесса, после чего оригиналный носитель помещается в безопасное место.

Следующий этап заключается в поиске доказательств на созданной вами копии жесткого диска. Если вы подозреваете, что доказательства могут содержаться на других носителях информации, например дисках, CD-R, лентах и т. п., с них также снимаются точные копии для последующего изучения.



Существует несколько компаний, которые занимаются производством рабочих станций, специально предназначенных для дублирования содержимого жестких дисков и других электронных носителей с целью их последующего анализа и обработки. Такие рабочие станции позволяют подключать массивы жестких дисков и другое оборудование для хранения информации, а также устанавливать стандартное экспертное ПО. Среди основных производителей можно назвать: Digital Intelligence ([www.digitalintel.com](http://www.digitalintel.com)), DIBS USA ([www.dibusa.com](http://www.dibusa.com)) и Forensic Computers ([www.forensic-computers.com](http://www.forensic-computers.com)).

## Экспертиза

После создания дубликата электронного носителя информации компьютерные полицейские начинают его изучение, подключая скопированный жесткий диск к экспертной рабочей станции, а другие типы носителей – вставляя в соответствующие приводы для их чтения. (Изъятый компьютер вначале загружается при помощи специальной дискеты, предназначенней для сбора данных из CMOS, которые необходимы для определения дат создания и модификации файлов. Загрузка с оригинального жесткого диска в любом случае недопустима, поскольку при этом происходит изменение данных на диске.) Экспертные рабочие станции содержат аппаратное и программное обеспечение, оптимизированное для выполнения функций анализа электронных доказательств, – на них вы не поиграете в Doom и не сможете обмениваться мгновенными сообщениями.

В ходе судебной экспертизы электронных материалов, независимо от вида носителя, выполняются следующие операции:

- **Экспертное изучение системы.** Выполняется анализ загрузочного сектора и файлов системной конфигурации (таких как, например, config.sys, autoexec.bat и файлов реестра).
- **Восстановление удаленных файлов.** По возможности производится восстановление всех удаленных файлов. (При этом первый символ имени восстанавливаемого файла вам придется задавать вручную, чтобы гарантировать непротиворечивость информации; более подробно мы обсудим это чуть позже.)

- **Составление списка всех имеющихся на жестком диске файлов.** Эксперты обязаны составить список всех файлов на электронном носителе, независимо от того, могут ли содержаться в них какие-то доказательства.
- **Анализ свободного дискового пространства.** Выполняется анализ свободного пространства на жестком диске или другом электронном носителе на предмет наличия доказательств, связанных с текущим расследованием.
- **Анализ неиспользуемого дискового пространства (остатков кластеров).** Также необходимо выполнить побайтовый анализ остатков кластеров, в которых могут находиться релевантные доказательства.
- **Изучение файлов.** Открываются и просматриваются все файлы документов.
- **Расшифровка файлов.** Осуществляются попытки расшифровать все защищенные документы. В случае благоприятного исхода содержимое файлов просматривается и анализируется.
- **Документирование всех доказательств.** Создается твердая копия со списком всех обнаруженных доказательств. Кроме того, сам процесс экспертизы также должен быть самым тщательным образом задокументирован.

Экспертиза доказательств может выполняться двумя способами: вручную, когда каждый этап осуществляется при помощи отдельных программных утилит, и в автоматическом режиме с помощью специального ПО, предназначенного для поиска, сбора и анализа улик, облегчающего и ускоряющего работу эксперта. В разделе «Средства сбора доказательств» данной главы перечислены приложения, чаще всего используемые в ходе экспертного анализа компьютерных улик. А применение одной и той же последовательности действий в ходе экспертизы различных электронных улик гарантирует слаженность действий во время расследования.

Важно отметить, что этап экспертизы обычно связан с поиском определенных доказательств в контексте конкретного преступления. Естественно, доказательства причастности к другой незаконной деятельности ни в коем случае не игнорируются, однако основной акцент делается на анализе улик по данному расследованию.

По окончании этапа экспертизы полицейские обязаны отчитаться об обнаруженных находках. Длительность этого этапа зависит от сложности и серьезности преступления, а также от количества накопившихся перед этим других неизученных электронных улик. Нередко бывает, что экспертиза затягивается на несколько месяцев, поскольку криминальные лаборатории не в состоянии справиться с накопившимся ворохом дел, а провести квалифицированную обработку доказательств в условиях небольших полицейских управлений не всегда представляется возможным.

Когда дело выносится на судебное слушание, полицейским, занимающимся расследованием компьютерных преступлений, часто приходится выступать свидетелями обвинения. В этом случае умение объяснять жюри присяжных сложные технические термины простым и понятным языком не менее важно для их работы, чем навыки восстановления улик с электронных носителей информации. В ходе подобных разбирательств бывают случаи, когда компьютерному полицейскому приходится сталкиваться со своим коллегой – частным компьютерным экспертом, выступающим на стороне защиты, в задачи которого входит посеять сомнение в достоверности доказательств и корректности процедуры их сбора и анализа.

## Шпионская тактика

Итак, пришло время опять поиграть в шпионов, только на этот раз вы будете выступать на стороне закона. Для этого вам придется примерить на себя маску детектива полиции, участника в расследовании серьезного преступления. Дело пахнет похищением несовершеннолетних и возможным убийством. Для поиска доказательств у подозреваемого был изъят компьютер, и сейчас ваша задача заключается в том, чтобы найти на нем улики, которые помогли бы разобраться в деле. (На этом этапе сконцентрируйтесь на изучении содержимого данного компьютера, не отвлекаясь пока на исследование сетевой активности пользователя. Вопрос сетевого шпионажа мы обсудим подробнее в главе 10 книги.)

Предположим, что вы уже сделали дубликат жесткого диска и теперь приступаете к проведению экспертизы, вручную выполняя анализ тех областей жесткого диска, где чаще всего можно найти улики.

Учтите, что, хотя сейчас мы будем описывать процедуру изучения электронных носителей полицейскими, в роли одного из которых в данный момент выступаете вы, эта же тактика применима для работы любых лиц, заинтересованных в извлечении информации с жестких дисков и других электронных носителей.

## Использование слабых мест

Когда речь заходит о хранении цифровой информации и улик (в соответствии с определением пункта 1001 Федеральных Правил о доказательствах, электронными данными называют информацию, записанную в виде магнитного импульса либо электронным способом), перед вами встает необходимость обработки огромного объема информации. Ведь данные, являющиеся доказательствами расследуемого преступления, могут находиться практически в любом месте. Поэтому в идеале следует перевезти компьютер в ваш офис или лабораторию, где вы сможете сделать дубликат жесткого диска, а затем провести экспертизу. В первую очередь доказательства следует искать в следующих местах.

## ФАЙЛЫ

Не нужно быть специалистом в области компьютерных наук, чтобы догадаться, содержимое каких документов следует изучить в первую очередь. К примеру, файлы с такими названиями, как НаркоСделки2002.doc, Лолита.jpg или ПланыФинТранзакций.xls, наверняка привлекут ваше внимание, и вы захотите начать с них.

Однако когда речь заходит об уликах, недостаточно изучить только содержимое файлов. Другими, не менее ценными, доказательствами могут послужить:

**ВРЕМЯ СОЗДАНИЯ, ИЗМЕНЕНИЯ И ОБРАЩЕНИЯ К ФАЙЛУ.** В Windows для каждого файла хранятся сведения о времени создания, последней модификации и последнего открытия файла. Их можно просмотреть из стандартного Проводника Windows, выбрав имя файла, а затем его свойства. Эти данные бывают важны для сбора доказательств, поскольку с их помощью можно выяснить историю файла. К примеру, если подозреваемый в корпоративном шпионаже утверждает, что он совершенно случайно загрузил таблицы бюджетных прогнозов в определенный день, но никогда их не просматривал, сведения о времени/дате последнего изменения или обращения к этим файлам позволяют проверить правдивость его слов.

**ЯРЛЫКИ.** Ярлыки могут ссылаться на приложения, отдельные файлы или устройства (принтеры, внешние устройства хранения информации и узлы сети). Ярлыки представляют собой файлы с расширением LNK, которое не отображается в Проводнике, так что пользователь видит только название ярлыка на Рабочем столе, в меню или папках Проводника. Предназначение ярлыков – экономия вашего времени. К примеру, менеджер по продажам может создать ярлык для файла списка клиентов, который часто бывает ему нужен. В дальнейшем для вызова списка ему достаточно будет сделать двойной щелчок по ярлыку, а не искать сам файл по всему дереву каталогов.

Помимо пользовательских ярлыков Windows любит создавать собственные ярлыки в различных местах, например, на Рабочем столе, в папке Recent, меню Пуск и папке SendTo.

- **Рабочий стол.** В этой папке хранятся все ярлыки, представленные на Рабочем столе Windows.
- **Recent.** Эта папка содержит ссылки на недавно открывавшиеся файлы, причем содержимое отображается в пункте Документы, доступ к которому возможен из меню Пуск.
- **Меню Пуск.** В этой папке хранятся ссылки на все установленные в системе приложения, доступные в меню Программы.
- **SendTo.** Папка SendTo содержит ссылки на приложения и устройства, в которые пользователь может передавать данные, например, флоппи-диски или приложения электронной почты.

В Windows 9x/Ме эти папки размещаются внутри папки Windows; в Windows NT/2000/ХР эти папки размещаются в Documents and Settings/ИмяПользователя. Ярлыки бывают чрезвычайно важны во время сбора доказательств по следующим причинам:

- Ярлык, ссылающийся на внешнее устройство хранения либо узел сети, указывает на возможные дополнительные места поиска доказательств, помимо жесткого диска компьютера.
- Ярлыки в меню Пуск могут служить доказательством установки на компьютере определенных приложений.
- Ярлыки в папке Recent содержат информацию о недавно открывавшихся документах, даже если теперь они удалены.
- В файле ярлыка, в байтах со смещением 28, 36 и 44 также содержится информация о времени открытия, модификации и создания файла.

**СКРЫТЫЕ ПАПКИ И ФАЙЛЫ.** Некоторые пользователи компьютеров, считающие себя достаточно умными, пытаются скрыть доказательства, задавая для папок или файлов атрибут hidden. Изначально этот атрибут предназначался для сокрытия от пользователя системных папок и файлов, однако пользователь имеет возможность задавать этот атрибут для своих файлов и папок.

Щелкните в Проводнике Windows правой кнопкой мыши на файле или папке, затем в контекстном меню выберите пункт Свойства и найдите атрибуты файла. Если флажок Скрытый (hidden) установлен, этот файл или папка по умолчанию не будут отображаться в Проводнике Windows или диалоговых окнах открытия файла.

Неопытные компьютерные пользователи, не разбирающиеся в принципах работы файловой системы, полагают, что смогут таким образом защищить свои документы от чужих глаз. К сожалению, эта мера не способна остановить прошедших школу криминального мастерства шпионов. Просмотреть скрытые файлы и папки можно несколькими способами:

- **Через Проводник Windows.** По умолчанию в Проводнике Windows не отображаются скрытые файлы и папки, однако вы легко можете изменить эту настройку в пункте Свойства Папки меню Сервис.
- **Через командную строку.** Стандартная утилита командной строки dir без параметров не выводит список скрытых файлов; для просмотра скрытых файлов и папок необходимо использовать ее с параметром: dir /a.
- **При помощи специальных приложений.** Скрытые файлы и папки легко можно просмотреть при помощи специальных экспертиз приложений, позволяющих выполнять каталогизацию всех обнаруженных на жестком диске файлов и папок, независимо от их атрибутов.

Таким образом, применение скрытых файлов и папок сможет ввести в заблуждение разве что рядового шпиона, просматривающего содержимое файлов и папок из простого любопытства, и ни в коем случае не остановит кого-либо, серьезно настроенного на поиск информации.

**ВРЕМЕННЫЕ ФАЙЛЫ.** Операционная система и многие приложения часто используют так называемые временные файлы, автоматически создаваемые и удаляемые без ведома пользователя. Временные файлы, как правило, предназначены для кратковременного хранения информации, и в них иногда можно обнаружить весьма интересные данные, которые могут быть использованы в качестве доказательств. К примеру, временные файлы, создаваемые Microsoft Word, имеют названия ~WRLxxxxxx.tmp, присвоив им расширение .doc, вы сможете открывать их непосредственно из текстового редактора Word.

Временные файлы обычно размещаются в следующих местах:

- в папке Temp системной папки Windows;
- в папке, в которую было установлено приложение, либо в папке, содержащей документы, обрабатываемые данным приложением.

Многие приложения не достаточно тщательно заботятся об удалении за собой временных файлов, поэтому нередко эти файлы с расширением .TMP можно увидеть прямо из Проводника Windows. Даже если временные файлы были благополучно удалены, вы можете попытаться восстановить их при помощи специальных утилит.

Если поиск файлов .TMP не дал результатов, существует вероятность, что пользователь использует специальное программное обеспечение, мешающее обнаружению доказательств (этот вид ПО будет рассмотрен немного позже). Другая причина может состоять в том, что переменные окружения Windows TMP и TEMP указывают на виртуальный диск, создаваемый в оперативной памяти (содержимое которого теряется в случае выключения питания), либо на зашифрованную папку. В этом случае временные файлы уничтожаются сразу после выключения компьютера либо сохраняются на томе, защищенном паролем, для получения доступа к которому его необходимо вначале загрузить.

**ИЗМЕНЕНИЕ РАСШИРЕНИЙ ФАЙЛОВ.** Тип файла определяется исходя из его расширения (нескольких символов после последней точки в имени файла). Например, расширение .DOC означает, что вы имеете дело с документом Microsoft Word, в файлах с расширением .XLS хранятся таблицы Microsoft Excel, а .BMP говорит о том, что перед вами графический файл Windows.

Иногда, пытаясь скрыть доказательства, некоторые ошибочно полагают, что простое присвоение файлу другого расширения поможет завуалировать истинный формат файла. Подобная тактика нередко применяется коллекционерами детской порнографии, пытающимися спрятать графические файлы .JPG и .GIF.

Чтобы убедиться в ненадежности подобной практики, откройте графический редактор Paint, создайте в нем рисунок, а затем сохраните его под именем SPY.BMP. Затем воспользуйтесь Проводником Windows и переименуйте файл в SPY.INI. Теперь по расширению файла и используемому для него значку никто не догадается об его истинном содержимом. А может, все-таки, догадается?

Снова запустите Paint и попытайтесь открыть файл SPY.INI. Несмотря на то, что этот файл имеет расширение INI, графический редактор Paint все равно вначале проверит, какой реальный формат данных имеет этот файл, и если в нем содержится графическая информация, то успешно откроет его.

За исключением простых текстовых файлов, все типы документов имеют свой уникальный формат. Формат файла указан в его заголовочной части, по которой приложение решает, сможет ли оно прочесть данный формат, и в противном случае выдает сообщение о том, что данный формат не поддерживается. Достаточно легко написать программу, которая бы выполняла анализ файлов на жестком диске и составляла списки файлов по типам в соответствии с информацией в их заголовках, независимо от присвоенного им расширения. Эта функция встроена в ряд коммерческих приложений, предназначенных для компьютерных экспертов.

Если вы считаете, что подозреваемый обладает более чем средними познаниями в области компьютерной техники, вы обязательно должны проверить, не были ли изменены расширения у некоторых файлов.



Если вы хотите подробнее узнать о различных файловых форматах, посетите веб-сайт [www.wotsit.org](http://www.wotsit.org). А определить, какие расширения файлов к каким приложениям относятся, можно по адресу <http://fileext.com>.

**УДАЛЕННЫЕ ФАЙЛЫ.** На первый взгляд, удаление файлов в Windows состоит из двух этапов. Вначале вы помещаете файлы в Корзину, а затем со временем очищаете ее. Перед тем как Корзина будет очищена, вы еще можете восстановить файл в оригиналную папку, выбрав имя файла в Корзине и запустив команду восстановления. Но что же происходит с файлом после того, как Корзина была очищена?

Если вы имеете опыт работы с компьютерами, вам наверняка известно, что при удалении файла хранившиеся в нем данные физически не удаляются с диска. Вместо этого Windows заменяет первый символ в названии файла символом с шестнадцатеричным кодом E5, запрещая отображение этого файла в каких бы то ни было каталогах. Кроме того, ссылка на этот файл удаляется из таблицы размещения файлов (FAT), разрешая системе использовать дисковое пространство, которое этот файл занимал раньше. В результате любой новый, скопированный либо увеличившийся в размерах файл может занять это дисковое пространство.

При помощи редактора шестнадцатеричных кодов (утилиты, способной просматривать и редактировать данные в шестнадцатеричном виде),

можно проанализировать сектора жесткого диска и вручную восстановить удаленный файл, прочитав информацию о занимаемых им секторах. Это довольно нудная работа, поскольку чаще всего кусочки одного файла оказываются разбросанными по всему жесткому диску. Поэтому гораздо проще воспользоваться утилитами автоматического восстановления удаленных файлов.

Вероятность успешного восстановления удаленного файла связана обратной зависимостью с периодом времени, прошедшим с момента его удаления. То есть вероятность восстановить файл, удаленный несколько дней назад, намного выше, чем файл, удаленный полгода назад, – ведь занимаемое им дисковое пространство могло быть перезаписано информацией из других файлов.

Таким образом, поскольку содержимое удаленных файлов может оказаться превосходным источником доказательств, вы не должны забывать о следующих операциях:

- Необходимо проверить, нет ли в Корзине недавно удаленных файлов.
- Следует воспользоваться одной из утилит для восстановления удаленных файлов, рассматриваемых в разделе «Средства сбора доказательств» данной главы. Даже если вам не удастся восстановить файл целиком, в качестве улик вы можете использовать его отдельные фрагменты.

**ФАЙЛЫ СПУЛИНГА ПЕЧАТИ.** Операционная система Windows использует спулинг при печати любых документов – это необходимо для того, чтобы печать могла осуществляться в фоновом режиме, пока пользователь продолжает работу с исходным файлом.

Спулинг при печати подразумевает создание временных файлов, содержащих собственно сами данные для печати и сведения, необходимые для выполнения задания на печать. Существует два типа файлов спулинга: EMF и RAW.

- Формат EMF, название которого расшифровывается как расширенный метафайл, используется при отправке заданий на печать в Windows по умолчанию. Любой документ перед началом печати преобразовывается в метафайл.
- Формат RAW используется не Windows-приложениями. Этот формат содержит полностью готовые к печати данные, не требующие преобразования в метафайл.

Дополнительно для файлов и форматов EMF и RAW при отправке каждого задания на печать создаются файлы с расширениями .SPL и .SHD. Файлы с расширениями .SHD (shadow) содержат информацию о самом задании. Файлы с форматом .SPL содержат либо сами данные для печати, либо имена файлов, в которых эти данные хранятся.

Обычно эти файлы имеют названия, начинающиеся с обозначения разновидности спулинга и заканчивающиеся расширением .TMR: например, ~EMFxxxxx.TMR. Все файлы .SPL, .SHD и .TMR удаляются сразу после завершения процесса печати.

Временные файлы, создаваемые в процессе печати, также могут представлять собой важные доказательства. Например, если подозреваемый утверждает, что он никогда не распечатывал документы, размещенные на его жестком диске, восстановленные файлы спулинга могут послужить доказательством обратного. Даже если исходные документы были удалены с жесткого диска, обнаруженные файлы спулинга позволяют восстановить их содержимое.

Чтобы подробнее узнать о процессе спулинга печати, найдите темы «EMF» и «RAW» на веб-сайте Microsoft: [www.microsoft.com/technet/](http://www.microsoft.com/technet/).

**ВРЕМЕННЫЕ ФАЙЛЫ, ОСТАВЛЯЕМЫЕ ПРОГРАММОЙ ПРОВЕРКИ ДИСКА.** Каждый раз при некорректном завершении сеанса работы в Windows, будь то по причине системного сбоя, отключения питания либо из-за неправильного завершения работы пользователем, во время последующей загрузки компьютера осуществляется запуск утилиты ScanDisk для проверки целостности файловой системы. В ходе своей работы эта утилита может создавать временные файлы с расширением .CHK в корневом каталоге логического диска. Нередко ScanDisk не удаляет их за собой, в результате чего эти временные файлы так и остаются на диске. Вы должны изучить каждый такой файл, поскольку в них могут содержаться фрагменты других файлов, которые могут выступать в качестве доказательств.

**АЛЬТЕРНАТИВНЫЕ ПОТОКИ ДАННЫХ.** В файловой системе NTFS под Windows NT/2000/XP вы имеете возможность связать с определенным файлом или папкой дополнительную информацию, которая носит название альтернативного потока данных (Alternate Data Stream – ADS). В этом альтернативном потоке можно сохранить текстовые данные и даже исполняемые файлы, которые не видны из Проводника Windows и не отображаются при выполнении команды dir из окна приглашения MS-DOS. Альтернативный поток данных можно удалить только при удалении родительского файла или папки.

Многие пользователи и даже компьютерные полицейские не знают о существовании альтернативных потоков данных, поэтому данная возможность отлично подходит для скрытия важной информации. Чтобы разобраться, как все это работает на самом деле, предлагаем вам выполнить следующие действия:

1. Воспользовавшись стандартным Блокнотом, создайте файл с именем test.txt в корневой папке диска, введите в него произвольный текст и сохраните файл.
2. Проверьте в Проводнике Windows размер файла.

## Тактика: использование Корзины

Любой следователь и компьютерный эксперт должны хорошо понимать принцип работы Корзины в Windows.

Итак, Корзина на самом деле представляет собой скрытую системную папку под названием Recycled в Windows 9x/Me и Recycler в Windows NT/2000/XP. При помещении пользователем файла в Корзину Windows перемещает файл из папки, где он находился раньше, в папку Recycled, после чего добавляет дополнительную информацию в скрытый файл с названием INFO или INFO2. В операционных системах Windows NT/2000/XP внутри папки Recycler создается папка с названием, соответствующим уникальному идентификатору (SID) бюджета текущего пользователя системы.

Файл INFO содержит следующую информацию:

- имя удаляемого файла;
- дату и время помещения файла в папку Recycled;
- исходное местоположение файла.

Эти данные могут быть чрезвычайно полезны при сборе доказательств, поскольку они подтверждают факт преднамеренного удаления файлов пользователем (операционная система и приложения не используют для этих целей Корзину). По ним можно также узнать время удаления файлов и исходное место их размещения.

Файл INFO удаляется при очистке Корзины пользователем, однако, как и любой другой файл, его можно попытаться восстановить при помощи специальных утилит.

Более подробно об удалении файлов в Windows вы можете узнать из статьи под номером 136517 базы знаний Microsoft:  
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;136517>.

- 3.** Теперь откройте диалоговое окно Run и наберите в командной строке следующее: notepad test.txt:alternate.txt. Программа спросит вас, хотите ли вы создать такой файл, – ответьте «да». Затем введите в него некоторый текст и сохраните.
- 4.** Далее задайте поиск на диске только что созданного вами файла alternate.txt. Вы не найдете его ни в одной папке, и даже поиск файла, содержащего введенный вами текст, не даст результата. Открыв файл test.txt в hex-редакторе, вы не увидите ничего, кроме текста основного файла test.txt; даже размер файла test.txt останется без изменений. Согласитесь, весьма хитрый способ хранения информации.

5. Чтобы убедиться в существовании файла alternate.txt, снова наберите в окне команды Run строку notepad test.txt:alternate.txt. Только так вы сможете вновь получить доступ к данным, хранимым в ADS.

Если ваш подозреваемый обладает глубокими компьютерными познаниями и использует операционную систему Windows NT/2000/XP с файловой системой NTFS, вам обязательно нужно проверить наличие в системе альтернативных потоков данных. Одну из свободно распространяемых утилит под названием Crucial Security, которая позволяет обнаруживать альтернативные потоки данных, вы можете загрузить с сайта [www.crucialsecurity.com](http://www.crucialsecurity.com).

## ОСТАТКИ КЛАСТЕРОВ

Операционные системы Windows оперируют фиксированными порциями данных (дискового пространства), которые называются кластерами. Кластер представляет собой наименьший объем данных, который может занимать файл; сам файл обычно состоит из целой серии кластеров. Если файл либо его часть занимают объем, меньший размера кластера, под его хранение все равно выделяется весь кластер. Оставшееся неиспользуемое дисковое пространство между окончанием одного файла данных и началом другого называют «остатками кластеров». В DOS и предыдущих версиях Windows, где использовалась 16-битная адресация FAT, приходилось использовать кластеры большего размера. К примеру, для жесткого диска объемом 2 Гб размер кластера составлял 32 Кб. Таким образом, если текстовый файл занимал всего 10 Кб, под его хранение все равно выделялись все 32 Кб, в результате чего 22 Кб пропадали впустую. Современные версии Windows используют дисковое пространство более экономично, работая с кластерами меньших размеров.

Остатки кластеров представляют немалый интерес для компьютерного эксперта, поскольку в них могут содержаться фрагменты давно удаленных файлов, чьи кластеры теперь относятся к новым файлам и являются частично перезаписанными (некоторые компьютерные эксперты утверждают, что объем неиспользуемого дискового пространства, относящегося к остаткам кластеров, может достигать 25% от общего объема жесткого диска). Существуют специальные программы, позволяющие собирать вместе все остатки кластеров и записывать их в один общий файл, предназначенный для последующего просмотра и анализа.

## СВОБОДНОЕ ПРОСТРАНСТВО

К свободному пространству на жестком диске или других носителях информации относятся не используемые никакими файлами кластеры. Это либо пустые кластеры, в которые информация никогда не записывалась, либо кластеры, содержащие фрагменты удаленных файлов. Как и в случае с остатками кластеров, эти области диска могут хранить ценную информацию. Существуют также специальные утилиты, с помощью

которых содержимое неиспользуемого дискового пространства также может быть записано в один файл для последующего рассмотрения и анализа.

## ФАЙЛ ПОДКАЧКИ WINDOWS

Все версии Windows используют файл подкачки (называемый также страничным файлом). Файл подкачки располагается на жестком диске компьютера, являясь неотъемлемой частью системы управления памятью Windows. Данные, по мере необходимости, переносятся из оперативной памяти на жесткий диск, а затем, в нужный момент, извлекаются обратно.

Допустим, что для работы с электронной почтой вы используете Outlook. Кроме этого в данный момент вы занимаетесь поиском информации в Интернете, и одновременно у вас запущен текстовый редактор для составления коммерческого предложения. Существует немалая вероятность того, что некоторые данные из сообщений электронной почты с посещавшихся вами веб-сайтов и из коммерческого предложения в целях экономии оперативной памяти будут перенесены в файл подкачки. То есть в принципе в файле подкачки может храниться все, что угодно, – доказательства, включая пароли, номера кредитных карточек и другие личные данные.

В зависимости от используемой вами версии операционной системы, файл подкачки называется:

- Win386.swp в Windows 9x/Me,
- Pagefile.sys в Windows NT/2000/XP.

Файл подкачки может иметь размер от нескольких десятков до нескольких сотен мегабайт, причем он постоянно эксклюзивно используется системой. Для того чтобы открыть этот файл и увидеть, что у него внутри, вам понадобится загрузить компьютер при помощи альтернативной операционной системы (DOS или Linux), а затем использовать специальные программы для просмотра.

Компьютерные полицейские применяют программы для поиска уникальных строк символов в файле подкачки, например, часто используемых названий для файлов с детской порнографией либо терминов, связанных с наркоторговлей. В некоторых случаях возникает необходимость в ручном анализе файла подкачки, когда нужно найти хоть какие-то зацепки, которые помогли бы сдвинуть дело с мертвой точки.

Благодаря относительной дешевизне оперативной памяти на сегодняшний момент, пользователь может установить на свой компьютер такое количество памяти, при котором вообще отпадает нужда в файле подкачки (и его отсутствие не повлияет на производительность системы). Кроме того, можно выполнить удаление файла подкачки перед повторной загрузкой Windows (удалить его из работающей операционной системы вам не удастся).

## СИСТЕМНЫЙ РЕЕСТР

Настоящим кладезем ценной информации, в том числе и доказательств, является системный реестр. В реестре хранятся пароли, списки недавно открывавшихся файлов, перечень установленных в системе программ и другая информация, которая может представлять для вас ценность. Большинство пользователей понятия не имеют о том, что собой представляет реестр и какая информация в нем хранится. Поэтому, перед тем как обсудить тему поиска доказательств в реестре, рассмотрим, что же такое реестр и как с ним взаимодействует операционная система.



Более подробную информацию по системному реестру Windows вы можете прочесть на веб-сайте [www.regedit.com](http://www.regedit.com) ([www.winguides.com/registry/](http://www.winguides.com/registry/)).

Начиная с Windows 95, Microsoft стала активно применять концепцию файлов базы данных, вместе составляющих единый системный реестр, предназначенный для хранения информации и настроек операционной системы и приложений. До этого системные параметры и настройки приложений хранились в текстовом виде в файлах с расширением .INI. Недостатками этой технологии хранения настроек являлись неэффективность и низкое быстродействие. Хранение данных в реестре позволило решить эти проблемы:

- В Windows 9x/Me реестр состоял из двух файлов: USER.DAT и SYSTEM.DAT.
- В Windows NT/2000/XP содержимое реестра хранится в нескольких файлах (включая NTUSER.DAT USRCLASS.DAT), размещенных в папках \windows\system32\config и Documents and Settings\{ИмяПользователя}.

Реестр имеет иерархическую структуру (дерево), каждая ветка которого называется «ключом». Каждый ключ может включать в себя другие ключи и значения. Реальные данные (значения), хранимые в ключе, могут иметь формат String, Binary и DWORD.

Системный реестр делится на пять ветвей (в Windows 9x/Me их было шесть), каждая из которых хранит определенный тип информации:

- HKEY\_CLASSES\_ROOT. Содержит информацию о типах файлов и данные OLE для приложений, поддерживающих эту технологию.
- HKEY\_CURRENT\_USER. Ссылается на часть ветви HKEY\_USERS, связанную с текущим пользователем.
- HKEY\_LOCAL\_MACHINE. Хранит информацию обо всем установленном в системе программном и аппаратном обеспечении. Текущая конфигурация оборудования определена в ветви HKEY\_CURRENT\_CONFIG.

- **HKEY\_USERS.** Здесь записаны настройки всех пользователей системы. В Windows 9x/Ме ветвь default содержала сведения о текущем пользователе системы. В Windows NT/2000/XP, в ветви default хранятся шаблоны для всех создаваемых пользователей.
- **HKEY\_CURRENT\_CONFIG.** Ссылается на часть ветви HKEY\_LOCAL\_MACHINE, связанную с текущей конфигурацией оборудования.
- **HKEY\_DYN\_DATA** (только в Windows 9x/Ме). Указывала на информацию по устройствам Plug and Play в ветви HKEY\_LOCAL\_MACHINE.

Операционная система и приложения постоянно обращаются к реестру путем вызова API-функций чтения и записи данных в ветвях и ключах реестра. Содержимое реестра можно просматривать и изменять с помощью стандартной программы RegEdit. Эта программа представляет содержимое реестра в виде дерева, подобно Проводнику Windows, как показано на рис. 5.1. Вы можете раскрывать ветви и вложенные ключи для просмотра интересующей вас информации.



Если вы не знаете наверняка, что делаете, – не изменяйте значения ключей в реестре вручную, поскольку вы можете нарушить работу как отдельных приложений, так и системы в целом.

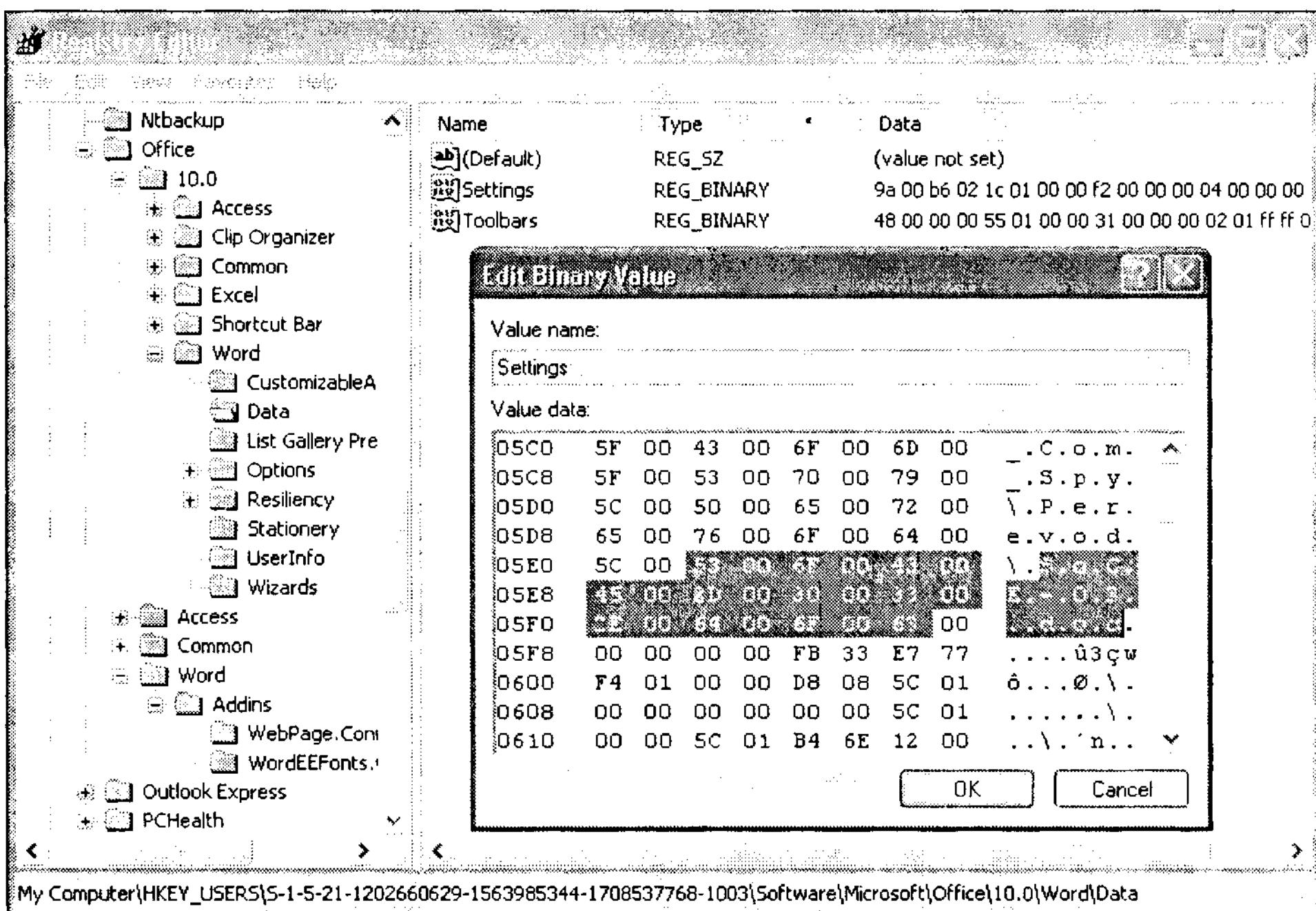
Даже после удаления ключей и значений реестра с помощью программы RegEdit, эти значения продолжают физически храниться в файлах реестра. Поэтому изучение файлов реестра вручную с помощью редактора шестнадцатеричных кодов позволяет обнаруживать неожиданные доказательства. Единственный способ, при котором пользователь может быть уверен в невозможности восстановления удаленных ключей реестра, – выполнение полной перестройки и сжатия реестра.



Взамен программы RegEdit для ручного анализа значений отдельных ключей предлагаем вам загрузить бесплатно распространяемую утилиту DumpReg с сайта компании Somarsoft: [www.systemtools.com/somarsoft/](http://www.systemtools.com/somarsoft/). Эта утилита позволяет записать все содержимое реестра в один текстовый файл, который может быть впоследствии легко просмотрен из любого текстового редактора.

## СПИСКИ НЕДАВНО ПРОСМОТРЕННЫХ ФАЙЛОВ

Во многих приложениях хранятся списки последних файлов, с которыми работал пользователь. Такой список обычно располагается в нижней части меню Файл и содержит имена этих файлов и пути к ним. Эта информация помогает определить, над какими документами в последнее время работал пользователь. Перечень недавно просмотренных файлов может также храниться в ключах реестра.



**Рис. 5.1.** Вид реестра Windows, открытого с помощью программы RegEdit, в окне которой отображено имя последнего открытого документа Word в ключе Settings

## БУФЕР ОБМЕНА

Если в ходе операции конфискации компьютерной техники машина включена и работает, проверьте содержимое буфера обмена – возможно, в нем сохранилась недавно копировавшаяся информация. Не забывайте, что содержимое буфера обмена постоянно изменяется, а при перегрузке системы просто теряется. Просмотреть содержимое буфера обмена можно с помощью утилиты из стандартного набора программ Clipbrd.exe.

## ИНТЕРНЕТ-БРАУЗЕРЫ

Во время работы интернет-браузера остается множество следов, по которым можно определить, когда и какие веб-узлы Интернета посещал пользователь. Поэтому, разыскивая доказательства, в первую очередь проверяйте используемые браузером временные файлы и папки.

**КЭШ.** Кэширование подразумевает сохранение часто посещаемых веб-страниц и графики на жестком диске компьютера. Для пользователей это означает более быструю загрузку веб-страниц. Для вас – возможность быстрого обнаружения всех интересующих вас улик.

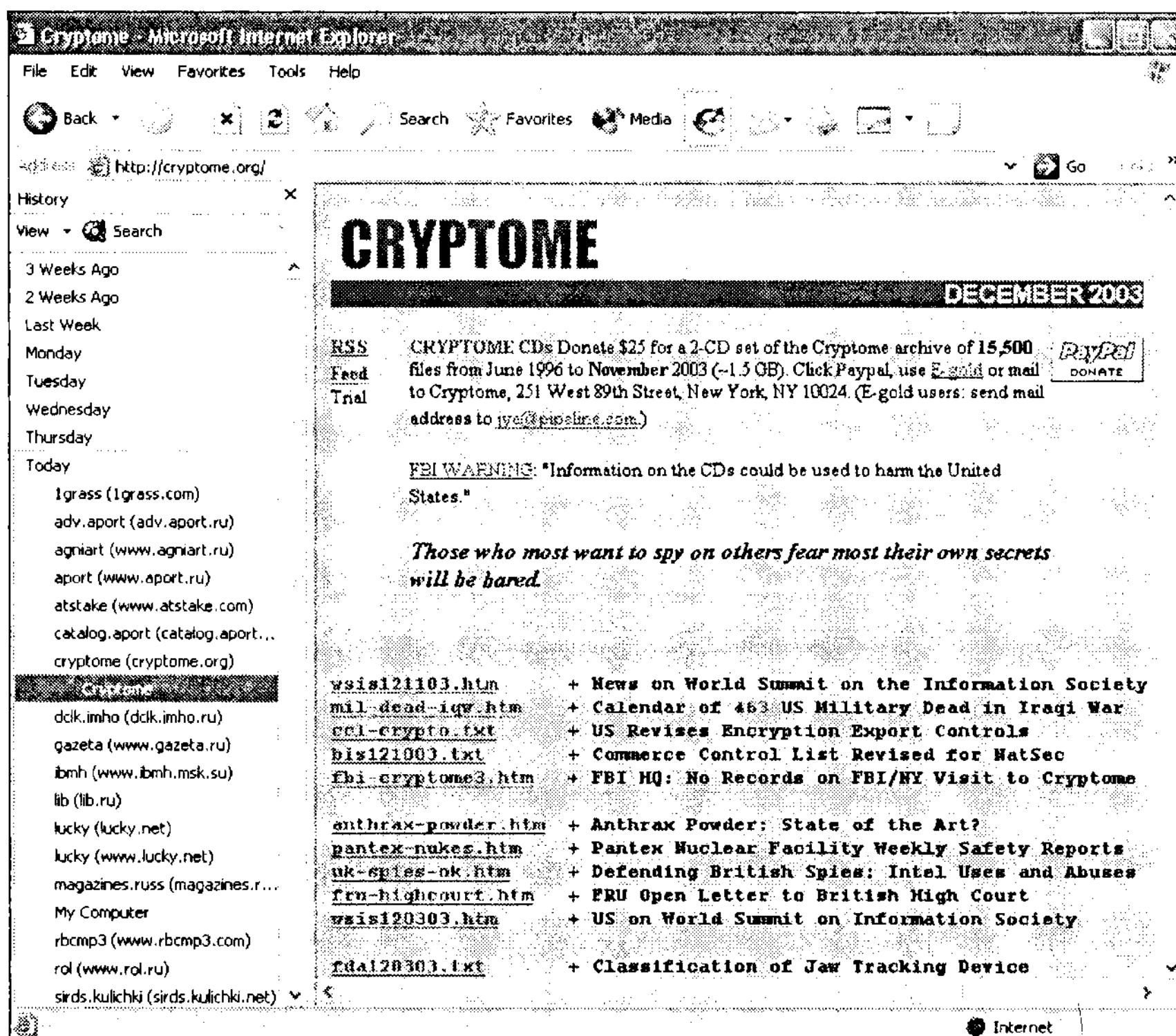
Кэширование информации осуществляется по принципу «первый пришел – первый ушел». То есть в кэш постоянно добавляются новые страницы до тех пор, пока объем информации не достигнет определенного порога; после этого постепенно удаляются самые старые страницы, освобождая место для новых. По умолчанию во многих браузерах настроено использование под кэш максимального объема дискового пространства, благодаря чему вы сможете проследить долгую историю работы пользователя.

Internet Explorer помещает кэшируемые файлы в папку под названием \Temporary Internet Files, где они находятся в несжатом виде и потому могут быть просмотрены любым браузером.

**ИЗБРАННОЕ.** Список часто посещаемых пользователем сайтов также может подсказать вам, где искать улики. Чтобы узнать, на какие веб-страницы часто заходил пользователь, щелкните на кнопке Избранное. Перед вами предстанет окно, содержащее гиперссылки на любимые сайты или страницы пользователя. Щелкните правой кнопкой мыши по ссылке и выберите в появившемся контекстном меню пункт Свойства. Здесь вы сможете узнать, когда данная ссылка была добавлена в избранное и сколько раз она посещалась (хотя эта информация может и отсутствовать). Узнать список избранных веб-страниц можно и без помощи Internet Explorer – вручную просмотрев содержимое папки Избранное (Favorites).

**ИСТОРИЯ.** Все браузеры позволяют просматривать историю посещения веб-страниц за последние дни или недели. В Журнале автоматически каталогизируются все посещавшиеся в последнее время сайты. Чтобы просмотреть историю посещений из Internet Explorer, вам потребуется щелкнуть кнопку Журнал (History) на панели инструментов, после чего на отдельной панели будет выведен список сайтов, просмотренных за последнее время (см. рис. 5.2). Таким образом, с помощью одного только Журнала вы сможете получить массу информации об онлайновых привычках пользователя.

**ФУНКЦИЯ АВТОЗАПОЛНЕНИЯ.** По умолчанию Internet Explorer сохраняет все данные, вводимые пользователем в веб-формы. Сюда относятся названия учетных записей, пароли, адреса и другие виды личной информации. При повторном посещении веб-сайта пользователем информация, заданная им в первый раз, подставляется автоматически. Это весьма удобная функция для пользователя и не менее удобная для следователя, ищущего улики. Данные автозаполнения можно выяснить, подключившись к сайтам, перечисленным в журнале, либо проверив содержимое ключей реестра, связанных с Internet Explorer. (Просмотрите содержимое ключей HKEY\_CURRENT\_USER или HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion и поищите ключи с названиями «Explorer» и «Internet Settings», либо вложенные ключи в HKEY\_CURRENT\_USER и HKEY\_LOCAL\_MACHINE\Software\Microsoft\Internet Explorer.)



**Рис. 5.2.** Журнал Internet Explorer позволяет получить массу ценных сведений об онлайновых действиях подозреваемого

**ФАЙЛЫ COOKIES.** Не вдаваясь в технические детали, поясним, что файлы cookies представляют собой небольшие фрагменты данных, которые веб-серверы сохраняют локально на вашем компьютере. В начале 1990-х, когда Интернет только начинал набирать популярность, велись ожесточенные дебаты вокруг использования онлайновыми компаниями файлов cookies для сбора личной информации о своих пользователях. Хотя такая практика и имела место, однако противники cookies сдались, когда общественность признала, что файлы cookies не представляют серьезной угрозы для частной жизни пользователей (а если и представляют, то этого должны осторегаться только отдельные индивидуумы). Хотя cookies в первую очередь необходимы веб-узлам для взаимодействия с пользователями, изучив их содержимое, вы сможете выяснить, чем занимался подозреваемый и какие веб-сайты он посещал, поскольку файлы cookies ссылаются на посещавшиеся пользователем веб-страницы и хранят информацию о времени последнего обращения и модификации.

По умолчанию в большинстве веб-браузеров разрешено использование файлов cookies. Internet Explorer хранит эти файлы в папке \Cookies. Вы можете просмотреть их с помощью Блокнота или же любого другого текстового редактора.

## ПОЧТОВЫЕ КЛИЕНТЫ

Еще одним ценным источником доказательств могут выступать такие программы, как почтовые клиенты. Электронная почта используется повсеместно – по самым приблизительным оценкам, по всему миру ежедневно отправляется около 31 миллиарда электронных сообщений. Многие люди даже не вдумываются в содержание отправляемых и получаемых ими сообщений, хотя текст посланий может представлять собой ценную находку для следователя, прямо или косвенно указывающую на причастность пользователя к определенному роду деятельности.

### Тактика: файлы .DAT

Internet Explorer создает скрытые файлы под названием index.dat в папках кэша, файлов cookies и журнала. Эти файлы содержат информацию, необходимую для индексации. Кроме того, в файлах index.dat хранится подробная история всех сетевых обращений пользователя. Файлы index.dat записываются в три папки:

- **Папка кэша.** Файл index.dat в папке \Temporary Internet Files хранит имена ссылок, метки даты и времени и указатели на кэшированные данные, разбросанные по различным подкаталогам данной папки.
- **Папка файлов cookies.** Файл index.dat в папке \Cookies хранит информацию о ссылках, метки даты и времени и указатели на файлы cookies в данной папке.
- **Папка журнала.** Файл index.dat в папке журнала (\History) содержит информацию о посещавшихся за последнее время веб-страницах, метки даты и времени. Internet Explorer использует эти данные для вызова функции автозаполнения и выделения другим цветом уже посещавшихся ссылок на данной веб-странице.

Местоположение этих папок зависит от используемой версии Windows:

- **для Windows 9x/Me:** эти папки размещены внутри папки \Windows;
- **для Windows 9x/Me, в которой используются профили отдельных пользователей:** \Windows\RPOFILES\Имя\_пользователя;
- **для Windows NT/2000/XP:** в папке Documents and Settings\Имя\_пользователя\Local Settings.

Хотя файл index.dat не является текстовым, вы все равно можете просмотреть его при помощи Блокнота или другого текстового редактора и выяснить немало ценной информации. Существуют также специальные утилиты для просмотра индексных файлов, которые вы можете найти на веб-сайте [www.exits.ro/index-dat-viewer.html](http://www.exits.ro/index-dat-viewer.html).

Прежде всего, для того чтобы использовать сообщения электронной почты в качестве доказательств, необходимо идентифицировать почтовый клиент, с которым работал подозреваемый. Нужно выяснить, как работает данное приложение, какие функции в нем предусмотрены, какие операции чаще всего выполняются. Убедитесь в том, что вы понимаете принципы работы почтового клиента, прежде чем применять его для поиска улик. Несмотря на огромное количество существующих почтовых клиентов, широкое распространение получили только 5...6 из них: Microsoft Outlook, Outlook Express, AOL Mail, Eudora, Pegasus и почтовые клиенты Netscape Communicator\*.

Независимо от используемого вами программного обеспечения, одна из главных уязвимостей большинства почтовых клиентов состоит в том, что паролем защищено только само подключение к учетной записи электронной почты. То есть, получив физический доступ к компьютеру, вы преспокойно можете просматривать уже загруженные входящие сообщения, послания, перемещенные в папку Удаленные, а также отправленные ранее сообщения (если пользователь настроил сохранение копий отправленных сообщений).

Еще одно уязвимое место почтовых клиентов – возможность сохранения имени учетной записи и пароля, для того чтобы пользователю не приходилось вводить их каждый раз. Хотя изначально данная опция предназначалась для обеспечения удобства пользователя, она представляет собой дополнительную опасность, поскольку любое лицо, получившее доступ к компьютеру, преспокойно сможет запустить почтового клиента и с его помощью как принимать, так и отправлять сообщения.

Занимаясь поиском улик в электронной почте, обратите внимание на следующие возможные места их расположения:

- **Папка Входящие.** Эту папку следует проверять в первую очередь, поскольку именно в ней хранятся все полученные пользователем сообщения. Советуем вам изучить расширенные сведения о заголовке сообщения, чтобы уточнить оригинального отправителя.
- **Папка Отправленные.** Большинство приложений почтовых клиентов позволяют сохранять копии отправленных сообщений. Если пользователь не забыл включить данную опцию, в вашем распоряжении окажется настоящий кладезь ценных сведений: содержимое всех отправленных им сообщений с указанием адресатов.
- **Вложения.** Каждый раз, когда пользователь отсылает письмо с вложением, почтовое приложение преобразовывает копию файла-вложения в допустимый формат, пригодный для пересылки через Интернет (обычно в формат MIME – Multipurpose Internet Mail Extensions). Конвертированные MIME-файлы автоматиче-

\* В России и странах бывшего СССР широкой популярностью пользуется также The Bat – благодаря своей надежности, простоте и универсальности. – Прим. ред.

ски удаляются после отправки сообщений. Если восстановить эти удаленные файлы, впоследствии их можно конвертировать назад в оригинальный формат при помощи утилиты Minpack.exe (задайте тип pack на поисковом портале, и вы найдете сайты, с которых можно загрузить данную утилиту). Не забудьте также просмотреть временные папки, в которых могут быть сохранены вложения электронной почты.

- **Папка Черновики.** Если вам повезет, немало интересных доказательств можно обнаружить среди черновиков и отложенных к отправке сообщений.
- **Папка Удаленные.** Многие приложения электронной почты используют принцип Корзины при удалении сообщений. Удаленное сообщение вначале переносится в отдельную папку (обычно папку Удаленные) и хранится там до тех пор, пока пользователь явным образом не очистит всю папку либо не удалит отдельные сообщения. До этого момента вы сможете прескокойно просматривать все удаленные сообщения.

## СЛУЖБЫ МГНОВЕННЫХ СООБЩЕНИЙ

В последнее время резко возросла популярность служб мгновенных сообщений, таких как IRC (Internet Relay Chat), ICQ и аналогичных служб America Online, Yahoo и Microsoft. Если на исследуемой системе установлена служба мгновенных сообщений, вы получаете в свое распоряжение еще один источник ценной информации. Списки адресатов и отправителей, история сообщений – все это может пригодиться вам в качестве улик.



Если вам удастся выяснить пароль учетной записи службы обмена мгновенными сообщениями (что достаточно легко сделать с помощью средств, перечисленных в главе 7 книги), вам ничто не помешает заняться сбором доказательств, выдавая себя за подозреваемого и общаясь с людьми из списка друзей.

### Разоблачения: копы против Коппа

Джеймс Копп, активист движения против абортов, обвиненный в убийстве доктора Барнетта Эй Слепиана 23 октября 1998 года, был задержан в апреле 2001-го. Сообщалось, что Копп стрелял и смертельно ранил доктора Слепиана в его собственном доме из русского карабина.

ФБР рьяно взялось за поиски Коппа и уже в июне 1999 года внесло его в список наиболее разыскиваемых преступников. Что любопытно, в то же самое время в черный список ФБР попал и Осама Бен Ладен.

Коппу удалось покинуть территорию Соединенных Штатов, в результате чего правоохранительным органам пришлось гоняться за ним по всей Европе, прежде чем им удалось его поймать. После ареста Коппа ФБР задержало двух предполагаемых соучастников, Лоретту Марра и Дениса Малваси из Бруклина, штат Нью-Йорк. Соучастникам Коппа были предъявлены обвинения после прослушивания их телефонных разговоров, апартаментов, в которых они проживали, а также наблюдения за электронной почтой.

Как и следовало ожидать, Копп и Марра использовали для общения между собой электронную почту. Однако, вместо того, чтобы пересылать сообщения с одного ящика на другой, они использовали одну и ту же учетную запись, оставляя сообщения друг для друга в папке Черновики. Обладая определенными знаниями по вопросам безопасности, злоумышленники понимали, что пересылаемые через Интернет сообщения достаточно легко перехватить, и избежали этой опасности, поскольку никогда не отправляли сообщения. Тем не менее они забыли учесть, что при обращении к веб-серверу, предоставляемому услуги электронной почты, записывается IP-адрес компьютера, с которого поступил запрос, а провайдеры услуг Интернета и электронной почты, как известно, обязаны сотрудничать с правоохранительными органами и сообщать им нужную информацию. ФБР заявило, что в процессе расследования использовались программы для отслеживания входящих/исходящих адресов в электронных сообщениях. Наблюдение велось за почтовым сайтом, предоставляющим услуги электронной почты, журнал обращений к которому показал, что подключение к данной учетной записи осуществлялось из некоторого интернет-кафе во Франции. За этим интернет-кафе велось постоянное наблюдение, пока Копп не совершил роковую ошибку, посетив его повторно, в результате чего и был задержан.

В марте 2003 года Коппа признали виновным в предумышленном убийстве. Обвинители заявили, что будут требовать для него максимального наказания в виде 25 лет лишения свободы.

## ЖЕСТКИЕ ДИСКИ

Иногда в ходе расследования случается так, что в качестве электронных доказательств выступают жесткие диски, к которым невозможно получить доступ. Они могут быть сломаны, повреждены в результате воздействия воды или огня либо просто переформатированы для сокрытия улик. Но даже в таких экстремальных обстоятельствах можно попытаться скопировать уцелевшую информацию.

Существует два способа восстановления данных с жесткого диска: самостоятельное восстановление данных при помощи специального программного обеспечения либо обращение к услугам коммерческих фирм, специализирующихся на подобных услугах.

- **ПО для восстановления.** Если жесткий диск не имеет физических повреждений, можно воспользоваться специальными утилитами для восстановления информации. Существуют утилиты, умеющие восстанавливать удаленные разделы и логические диски, а также локализировать и восстанавливать удаленные файлы и папки. Некоторые предназначенные для этой цели приложения перечислены в разделе «Средства сбора доказательств» данной главы.
- **Коммерческие фирмы, специализирующиеся на восстановлении данных.** Вы можете поступить и проще – отправить жесткий диск в сервисную компанию, специализирующуюся на восстановлении информации. Здесь квалифицированные специалисты разберут ваш жесткий диск на части и займутся восстановлением информации при помощи специализированного оборудования и программного обеспечения. Даже если повреждения коснулись пластин жесткого диска, существует вероятность восстановления хотя бы части поврежденных данных. В таком случае будет произведено восстановление уцелевшей информации с исходных носителей и последующая ее запись на DVD-R или CD-ROM. Услуги подобных компаний, конечно, удовольствие не из дешевых, и успешное восстановление информации может обойтись вам в \$500...1500 (неудачные попытки стоят значительно дешевле).

Практически исчерпывающий список коммерческих компаний, занимающихся восстановлением данных в США и Европе, можно найти на веб-странице [www.datarecoverylinks.com](http://www.datarecoverylinks.com). Двумя крупнейшими и наиболее известными компаниями, сотрудничающими со многими корпорациями и правоохранительными органами, считаются Ontrack Data International (один из лидеров в индустрии восстановления данных, приобретенный Kroll Incorporated в июне 2002 года; подробности вы можете узнать на официальном веб-сайте компании [www.ontrack.com](http://www.ontrack.com)) и DriveSavers Data Recovery (компания основана в 1985 году, она гарантирует восстановление данных в кратчайшие сроки – от 24 до 48 часов; адрес в Интернете: [www.drivesavers.com](http://www.drivesavers.com)).

## ГИБКИЕ ДИСКИ

Из-за своей малой вместимости гибкие диски все реже используются в качестве носителей информации. Тем не менее они продолжают повсеместно использоваться для переноса небольших объемов информации и фигурируют практически во всех расследованиях компьютерных преступлений. Для восстановления данных с гибких дисков могут применяться те же программные утилиты, что и при восстановлении информации с жестких дисков, и точно так же вы можете обращаться за услугами в специализированные компании.

При восстановлении информации с гибкого диска следует учитывать следующие два момента:

- Даже если злоумышленник воспользовался утилитами безвозвратного удаления файлов с дискеты (чтобы не допустить восстановления информации при помощи специальных средств), этот способ применительно к гибким дискам менее надежен, чем по отношению к жестким дискам. Дело в том, что ширина дорожек на дискете намного больше, а точность позиционирования магнитной головки привода намного ниже, поэтому некоторые программные утилиты способны восстанавливать даже якобы перезаписанные данные с другого края дорожки.
- Компьютерная судебная лаборатория Министерства обороны (DCFL), размещенная в Мэриленде, разработала технологию склеивания дисков, позволяющую реконструировать 3,5- и 5,25-дюймовые дискеты, которые были разрезаны, порваны, помяты, частично расплавлены и извлечены из защитной коробочки. После склеивания таких дисков производится попытка восстановления информации с них. Существует документ, «предназначенный только для представителей правоохранительных органов», который описывает процесс восстановления дисков. Официальный сайт лаборатории размещен по адресу [www.dcf1.gov](http://www.dcf1.gov).

## ПАМЯТЬ

Если в момент конфискации компьютер находится во включенном состоянии, можно попытаться просмотреть содержимое оперативной памяти либо сохранить дамп памяти на диск для дальнейшего изучения. В памяти могут храниться пароли, документы и другие фрагменты информации, не представленные на жестком диске. (Помните, что сохранять дамп памяти на жестком диске изучаемого компьютера нежелательно, поскольку тем самым вы изменяете содержимое оригинального носителя.)

## Средства сбора доказательств

Различными компаниями разработано множество программных средств, предназначенных для сбора и анализа цифровых доказательств. Многие из этих утилит являются многофункциональными, причем изначально большинство из них предназначалось для работы системных администраторов. В то же время существует ряд программ, которые были созданы специально для работы компьютерных судебных экспертов. И если простейшие утилиты командной строки, как правило, являются свободно распространяемыми, сложные коммерческие программные продукты стоят немалых денег. На сегодняшний день этот рынок далек от насыщения, однако, в связи с ростом спроса на подобные программные продукты и благодаря ужесточению конкуренции между компаниями, производящими

подобные утилиты (в особенности утилиты, свободно распространяемые по принципу открытого кода), в ближайшее время можно ожидать снижения цен и увеличения ассортимента.



Дэн Мэйерс, проработавший в индустрии создания приложений для компьютерных экспертов в течение достаточно долгого времени, является автором нескольких широко известных программных утилит. На его сайте [www.maresware.com/maresware/linksto\\_forensic\\_tools.htm](http://www.maresware.com/maresware/linksto_forensic_tools.htm) вы можете найти массу полезных ссылок по программному и аппаратному обеспечению для компьютерных экспертов.

## УТИЛИТЫ ДЛЯ ДУБЛИРОВАНИЯ СОДЕРЖИМОГО ДИСКОВ

В этом разделе речь пойдет об утилитах, предназначенных для создания точных образов жесткого диска. Вместо копирования отдельных файлов, с их помощью создается побитовая копия жесткого диска. Обычно к компьютеру эксперта подключаются два жестких диска: один с компьютера подозреваемого, а другой – абсолютно чистый (с которого были удалены все данные). Затем с дискеты загружается альтернативная операционная система, после чего запускается утилита копирования диска. Некоторые наиболее популярные утилиты перечислены в следующих абзацах:

**SAFEBACK.** Утилита SafeBack существует еще с начала 90-х, и поэтому для ее использования достаточно среды DOS. Она позволяет обращаться к IDE-устройству напрямую, минуя функции проверки геометрии диска в BIOS, дублировать содержимое одного жесткого диска на другой, а также на магнитную ленту и другие сменные носители. Она может добавлять информацию о контрольной сумме, с помощью которой можно проверить, изменилось ли содержимое диска. Эта утилита пользуется популярностью у правоохранительных органов, военных и разведывательных организаций, ей даже присвоен номер в каталоге Администрации общих служб США (GSA) для упрощения процедуры заказа программного продукта со стороны правительственные служб. Стоимость программы составляет \$595, что совсем не дешево, однако оправдывается ее высокой эффективностью. Подробнее о программе Safeback вы можете узнать на веб-сайте [www.forensics-intl.com/safeback.html](http://www.forensics-intl.com/safeback.html).

**NORTON GHOST.** Изначально программа Norton Ghost предназначалась для использования системными администраторами в целях создания резервных копий жестких дисков. Благодаря легкости использования, низкой цене и своей универсальности она приобрела большую популярность среди компьютерных полицейских и судебных экспертов. Программу Norton Ghost можно купить всего за \$69,95. Более подробную информацию вы сможете получить на сайте компании-производителя [www.symantec.com](http://www.symantec.com).

**LINUX DD.** Для людей, знакомых с операционной системой Linux, либо следователей с ограниченным бюджетом в качестве альтернативы подойдет такая утилита, как dd (data dumper). Первоначально предназначенная для обмена данными между файлами, эта утилита отлично справляется и с дублированием жестких дисков. Самый большой ее недостаток – отсутствие дружественного пользователю интерфейса, так что опции командной строки могут показаться чересчур загадочными для компьютерных экспертов, привыкших к работе в Windows. К примеру, чтобы выполнить дублирование структуры жесткого диска при помощи программы dd, вам понадобится набрать в командной строке dd if=/dev/had of=/dev/rst0.



В августе 2002 года Министерство юстиции выпустило специальный отчет, касающийся использования dd для дублирования информации компьютерными экспертами. Если вы хотите узнать подробности, посетите веб-сайт [www.ncjrs.org/pdffiles1/nij/196352.pdf](http://www.ncjrs.org/pdffiles1/nij/196352.pdf).

## АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА СБОРА ДОКАЗАТЕЛЬСТВ

Поиск и анализ доказательств на жестком диске и других цифровых источниках информации, как правило, является весьма нудным и длительным процессом. Обычно для извлечения и обработки компьютерных улик следователи применяли целую серию утилит командной строки. Только в последние пять-шесть лет на рынке начали появляться простые в использовании автоматизированные средства сбора и обработки доказательств. Благодаря подобным программам значительно сократилось время сбора и анализа доказательств и одновременно снизились требования к уровню технических знаний судебных экспертов, необходимых для проведения квалифицированного расследования. В настоящее время широкое распространение получили три предназначенные для работы судебных экспертов специализированных программных пакета, которые сочетают в себе множество различных функций.

**ENCASE.** На сегодняшний день из всех представленных на рынке программ EnCase является наиболее популярным и распространенным автоматизированным программным пакетом, применяемым в судебной практике (согласно статистике, на момент написания книги копии этой программы использовались в более чем двух тысячах подразделениях правоохранительных органов по всему миру). Поскольку EnCase превратилась в программный продукт, используемый де-факто в большинстве судебных расследований, основное внимание мы уделим именно ему.

В плане аппаратного обеспечения EnCase может работать на большинстве современных компьютеров под управлением операционной системы Windows 98/Ме или Windows NT/2000/XP. В целях защиты от пиратства, программа EnCase требует подключения к USB или параллельному порту заглушки (представляющей собой аппаратное средство защиты программного обеспечения и данных от несанкционированного копирования).

Информация извлекается и без заглушки, однако в этом случае дальнейший анализ данных невозможен.

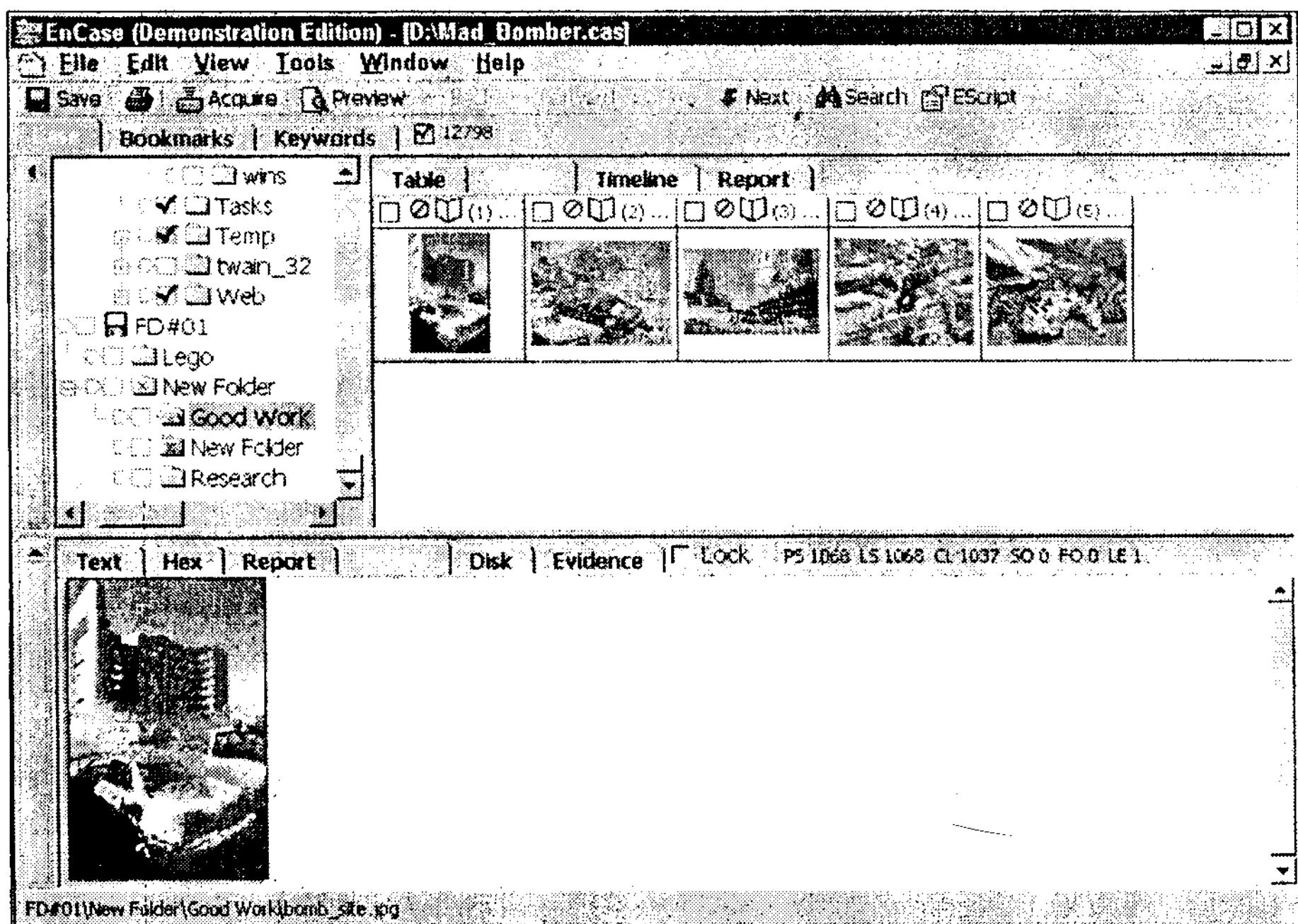
EnCase создает специальную загрузочную дискету DOS, которая используется для загрузки исследуемого компьютера. Затем этот компьютер связывается при помощи сетевого кабеля, параллельного порта или нуль-модемного кабеля с удаленным компьютером, на котором запущена копия EnCase. Таким образом, загрузив компьютер подозреваемого с дискеты и удаленno подключив его к рабочей станции с запущенным пакетом EnCase, компьютерный эксперт может предварительно просмотреть содержимое информационных носителей на исследуемом компьютере без внесения каких-либо изменений. Предварительный просмотр нужен для выяснения необходимости более тщательного анализа либо поверхностного изучения системы.

Разумеется, в пакете EnCase предусмотрена опция сохранения доказательств. Однако, вместо побитового копирования жесткого диска подозреваемого на другой диск, программа EnCase создает точный файл-образ содержимого жесткого диска, доступный только для чтения и защищенный от фальсификации (многие суды принимают эти файлы в качестве допустимых доказательств). Создать образ жесткого диска можно, соединив два компьютера между собой напрямую через некоторый порт или по сети, либо путем подключения жесткого диска, извлеченного с компьютера подозреваемого, к рабочей станции компьютерного следователя.

В пакете EnCase реализован целый ряд функций анализа доказательств, включая: расширенный поиск символьных строк и отображение графических файлов (как показано на рис. 5.3); изучение формата файла на случай, если его расширение было изменено в целях скрытия улик; просмотр удаленных файлов и отображение времени создания, открытия и последнего изменения файлов на временной оси. В процессе анализа следователь может делать заметки касательно обнаруженных доказательств, не выходя из программы, кроме того, в EnCase встроено средство автоматической генерации отчетов по найденным уликам.

Программный пакет имеет немалую стоимость – \$2495 (\$1995 для государственных учреждений), однако если вам необходимо выполнять большие объемы работ, то эти деньги достаточно быстро окупятся за счет сэкономленного времени. Узнать подробности об этом продукте вы сможете, посетив его страницу в Интернете: [www.encase.com](http://www.encase.com).

**FORENSIC TOOLKIT.** Компания AccessData, один из лидеров по выпуску утилит для восстановления паролей, не так давно осуществила прорыв и на рынке программных утилит для анализа данных и доказательств, выпустив пакет под названием Forensic Toolkit (FTK). FTK позволяет выполнять расширенный поиск, обладает возможностями просмотра более 270 различных типов файлов, умеет восстанавливать удаленные данные и разделы жесткого диска, а также анализировать сжатые файлы и архивы электронной почты. Стоимость программного пакета Forensic Toolkit составляет \$595, а его пробную версию вы можете загрузить на сайте [www.accessdata.com](http://www.accessdata.com).



**Рис. 5.3.** Пользовательский интерфейс пакета EnCase позволяет отображать содержимое графических файлов на жестком диске подозреваемого

**ILOOK.** Если вы служите компьютерным полицейским, жестко связанным рамками бюджета, советуем вам обратить свой взор на такую программу, как ILook. Разработанная Элиотом Спенсером для отдела уголовных расследований внутренней налоговой службы Министерства финансов США, эта свободно распространяемая утилита обладает многими возможностями поиска и анализа данных, встречающимися в коммерческих продуктах. За более подробной информацией по программе ILook обращайтесь на сайт [www.ilook-forensics.org](http://www.ilook-forensics.org).

## ИНСТРУМЕНТЫ ЭКСПЕРТА

Даже при условии наличия специализированного программного обеспечения для автоматического сбора доказательств, вы должны иметь в своем арсенале несколько программ общего назначения:

- **Дисковый редактор или редактор кодов.** Необходим для поиска информации на жестком диске и других электронных носителях, а также для открытия и просмотра файлов в виде шестнадцатеричных кодов или в формате ASCII.
- **Средство просмотра файлов.** Такая утилита нужна для просмотра файлов различных форматов без помощи приложений, в которых они были созданы.

## Тактика: пять признаков настоящей улики

Любое обнаруженное вами электронное доказательство должно обладать следующими пятью признаками:

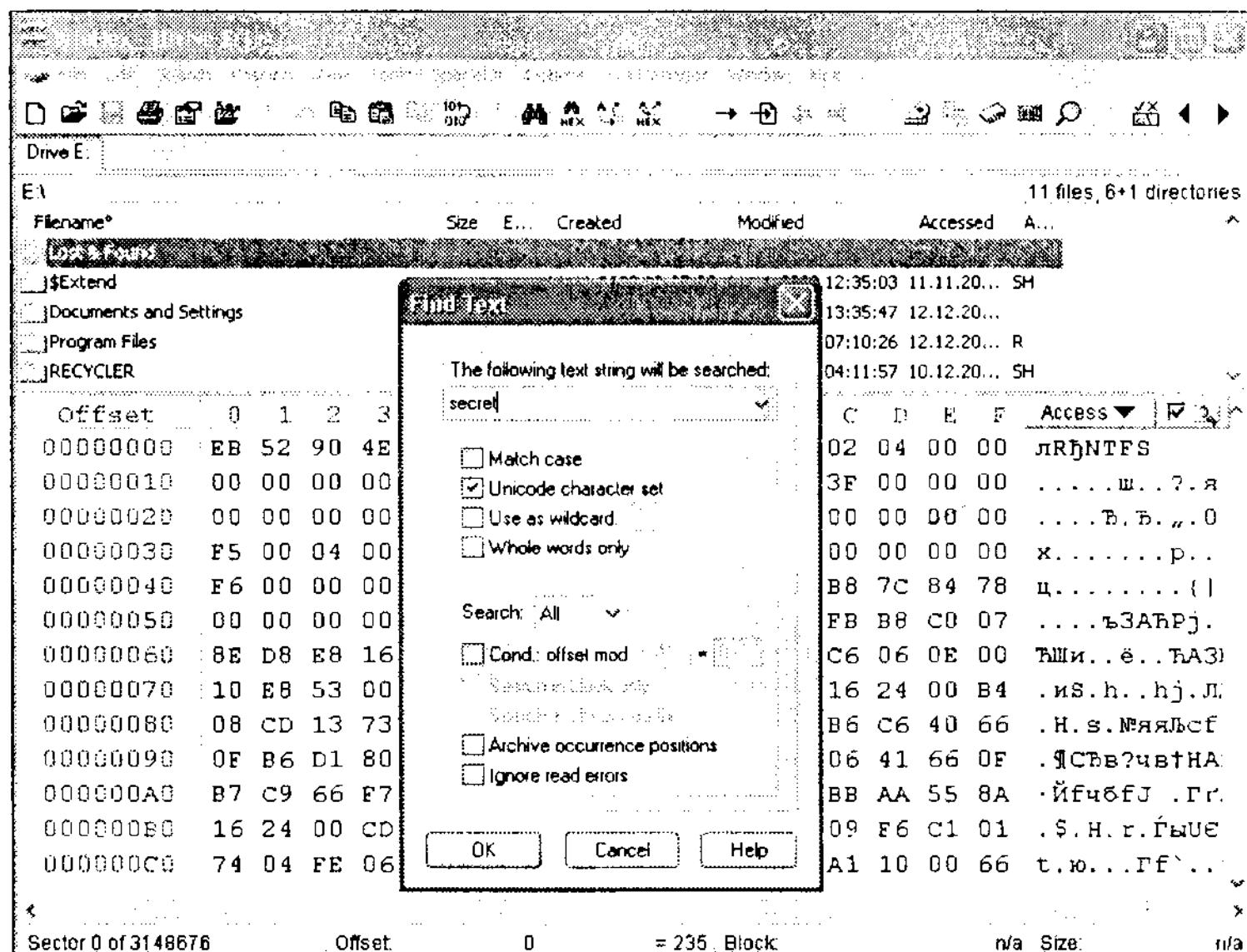
- 1. Приемлемость.** Обнаруженная улика должна приниматься судом в качестве допустимой. Допустимость улики определяется на основе существующих законов и состава преступления, вследствие чего использование некоторых улик окажется невозможным.
- 2. Аутентичность.** Вы должны доказать, что рассматриваемая улика имеет непосредственное отношение к делу.
- 3. Завершенность.** Собранные вами доказательства должны характеризовать преступление с обеих сторон (улики должны указывать не только на то, что субъект действительно совершил данное преступление, но и представлять факты, которые могут служить доказательствами его невиновности; ваша задача – объяснить суду и присяжным, почему вы склоняетесь к мнению о виновности подозреваемого). Среди адвокатов такие улики носят название «доказательств невиновности».
- 4. Надежность.** Способ получения и анализа улики не должен вызывать сомнений в ее достоверности.
- 5. Правдоподобность.** Улика должна быть представлена так, чтобы ее смысл был четко определен, и ее можно было принять на веру.

Если обнаруженное вами доказательство лишено хотя бы одного из пяти вышеперечисленных признаков, судья либо адвокаты могут посчитать доказательство не заслуживающим доверия. Хотя эти правила касаются в первую очередь рассмотрения улик в гражданских и уголовных дела, их следует применять для сбора доказательств любого типа.

Двумя наиболее популярными программами этой категории среди компьютерных полицейских и судебных экспертов считаются:

**WINHEX.** Эта программа, изначально позиционируемая на рынке в качестве дискового редактора или редактора шестнадцатеричных кодов, со временем приобрела массу других полезных функций. С помощью WinHex вы можете просматривать и считывать содержимое оперативной памяти, восстанавливать удаленные файлы, клонировать диски, считывать остатки кластеров и неиспользуемое дисковое пространство для дальнейшего

изучения, а также выполнять поиск символьных строк (как показано на рис. 5.4). Кроме того, программа настолько мала, что вполне может уместиться на одну дискету. Версия WinHex для специалистов, включающая специальные экспертные функции, стоит около \$100. Оценочную копию программы вы можете загрузить с сайта [www.winhex.com](http://www.winhex.com).



**Рис. 5.4.** Редактор WinHex позволяет выполнять поиск символьной строки на жестком диске. В главном окне программы представлены данные сектора жесткого диска в шестнадцатеричном представлении и в виде кода ASCII

**QUICK VIEW PLUS.** Весьма популярная среди судебных экспертов утилита, выпущенная компанией Jasc, которая позволяет просматривать и распечатывать более 200 различных файловых форматов (графику, документы, таблицы, базы данных, презентации и сжатые файлы). Ее стоимость составляет всего \$39, а оценочная версия доступна на сайте [www.jasc.com](http://www.jasc.com)\*.

## СРЕДСТВА ВОССТАНОВЛЕНИЯ ДАННЫХ

На рынке представлено огромное количество разнообразных утилит, предназначенных для восстановления удаленных данных, исправления ошибок на испорченных носителях и извлечения информации с поврежденных носителей. Любой компьютерный следователь обязан иметь хотя бы пару подобных программ в своем арсенале.

\* Программа доступна также на многих архивных порталах, распространяющих бесплатные и условно-бесплатные программы, например <http://tucows.nordnet.ru/preview/302331.html>. - Прим. ред.

К двум наиболее популярным программным продуктам этой группы относятся:

**NORTON UTILITIES.** Программный пакет Norton Utilities от компании Symantec существует уже много лет и за это время успел завоевать популярность среди компьютерных полицейских, использующих это «швейцарское оружие» в мирных целях – для восстановления файлов и данных. Цена пакета Norton Utilities составляет \$49,95, а его демонстрационная версия размещена на официальном сайте компании [www.symantec.com](http://www.symantec.com).

**EASYRECOVERY PROFESSIONAL EDITION.** Эта программа, выпущенная компанией OnTrack, также предназначена для восстановления данных и при этом обладает рядом расширенных возможностей. Помимо восстановления информации из удаленных файлов и поврежденных разделов жесткого диска, программа умеет «лечить» запорченные документы Microsoft Office и удаленные сообщения электронной почты (из файлов .PST и .OST Microsoft Outlook). Стоимость пакета EasyRecovery составляет \$499. Пробную версию (демонстрирующую данные, которые могут быть восстановлены, но не восстанавливающую их) можно загрузить с сайта [www.ontrack.com](http://www.ontrack.com).

## Контрмеры

В этом параграфе мы поговорим не о том, как можно избежать правосудия, перехитрив компьютерных полицейских. На самом деле все технически грамотные преступники и так уже знают о шифровании, утилитах удаления файлов без возможности восстановления и других средствах уничтожения доказательств. С другой стороны, если вы выступаете в роли компьютерного полицейского или судебного эксперта, вам необходимо иметь представление о возможных контрмерах, чтобы суметь распознать попытки злоумышленников скрыть следы преступления и принять адекватные меры. Если правонарушители должным образом подошли к использованию контрмер, тогда вы можете не тратить лишнее время на изучение компьютерных улик и направить свои усилия в другом направлении. (Хорошая новость для вас, как полицейского, состоит в том, что для эффективного сокрытия доказательств необходима дисциплина в применении всех контрмер, а большинство преступников достаточно ленивы по своей природе и не слишком умны. Стоит обратить внимание хотя бы на количество преступлений, которые были раскрыты всего лишь по отпечаткам пальцев. Если многие злоумышленники забывают об использовании такой элементарной меры предосторожности, как ношение перчаток, то вряд ли стоит ожидать от них повального применения технических контрмер для защиты от компьютерных полицейских.)

Даже если вы не являетесь представителем правоохранительных органов (либо преступником, старающимся избежать ответственности), вы должны понимать, что шпион, занятый нелегальным подслушиванием и подсматриванием за вами, будет использовать те же методы, что и компьютерные полицейские для поиска и извлечения информации с вашего компьютера. Вы можете заниматься полностью законной деятельностью, и тогда контрмеры понадобятся вам для защиты от незаконного шпионажа.

## Шифрование

Вы наверняка знаете о шифровании, если только последний десяток лет вам не пришлось провести в пещере или на необитаемом острове. Просто говоря, шифрование представляет собой преобразование данных с помощью математического алгоритма в форму, которая не позволяет их прочесть без использования специального ключа (в качестве него может выступать пароль, смарт-карта или другое средство идентификации). Если термин *криптография* мы определили как науку создания кодов и шифров, то *криptoанализ* – это наука их взлома.

В этом параграфе мы не станем обсуждать принципы работы *криптосистем*, нюансы использования s-box, реализацию квантовой криптографии или другие технические вопросы, связанные с шифрованием (рассмотрение которых может растянуться на отдельную книгу или послужить просто для заполнения книги ненужной информацией). Вместо этого мы проведем краткий экскурс в историю современной криптографии, дадим некоторые советы и рекомендации по использованию приложений для шифрования, а также приведем список рекомендуемых программных продуктов.



Если вы хотите больше узнать о такой науке, как криптография, обратитесь к следующим веб-ресурсам: <http://world.std.com/~fran?crypto.html>, где вы найдете общие ссылки на информационные ресурсы; [www.counterpane.com/crypto-gram.html](http://www.counterpane.com/crypto-gram.html) – с отличными ежемесячными информационными бюллетенями по безопасности и криптографии; а также зайдите на сайт Центра демократии и технологий, где доступны публикации по вопросам шифрования (по адресу [www.cdt.org/crypto/](http://www.cdt.org/crypto/)), рассматривающие вопросы криптографии с точки зрения законодательства.

## КРАТКАЯ НОВЕЙШАЯ ИСТОРИЯ

До середины 90-х годов XX века криптография являлась монополией государства. Только государственные организации имели право создавать и взламывать коды. Даже стандартом шифрования DES (Data Encryption Standard), используемым в банковской индустрии, как и многими другими технологиями шифрования, владели Управление национальной безопасности и другие представители разведывательного сообщества Соединенных Штатов.

Однако в середине 1990-х джин был выпущен из бутылки. Благодаря компании PGP (название которой расшифровывается как «Pretty Good Privacy» – высоконадежное шифрование) и таким специалистам по криптографии, как Фил Зиммерман, Брюс Шнайер, Уитфилд Диффи и Рон Ривест – и это только начало списка, – внезапно широкая общественность получила доступ к средствам шифрования уровня Министерства обороны, которые госучреждения оказались не в состоянии взломать. Кстати, криптографическая технология отнесена к той же категории, что и ракеты, и другое оружие массового поражения, в плане ограничений на экспорт.

Тот факт, что отныне люди смогут безопасно общаться друг с другом через электронные средства связи, не боясь быть подслушанными, весьма огорчил немалое число людей в правительстве, особенно представителей ФБР, потративших в конце 90-х немало времени на попытки узаконить «условное депонирование ключей». То есть правительственные службами предпринимались попытки заставить производителей коммерческих утилит шифрования включать в свои продукты возможность расшифровки с помощью резервного ключа, чтобы в случае необходимости иметь доступ к зашифрованным данным; либо чтобы копия ключа, используемого для шифрования данных, хранилась в правительственной организации или у третьей стороны, дабы при расследовании преступления правоохранительные органы могли получить доступ к этому ключу. Однако идея «депонирования ключей» было суждено умереть в зародыше, ограничения на экспорт криптографических технологий со временем были смягчены, и утилиты шифрования стали доступны для всех желающих защитить свою частную и деловую жизнь, причем ситуация не изменилась даже после событий 11 сентября.

Наш краткий экскурс в новейшую историю можно завершить констатацией того факта, что кем бы вы ни являлись – компьютерным экспертом либо шпионом, – вам придется смириться с тем, что сейчас люди имеют доступ к утилитам шифрования, которые ни вы, ни ФБР, ни Управление национальной безопасности, ни (вставьте название организации, на которую вы работаете) не в состоянии взломать «в лоб». Поэтому, когда дело дойдет до расшифровки электронных доказательств, вам придется действовать творчески (а уж мы постараемся подкинуть вам парочку интересных идей).

## ОБЩИЕ РЕКОМЕНДАЦИИ

Хотя повсеместное шифрование информации не сулит приятных перспектив потенциальному шпиону, но для человека, стремящегося защитить свою частную жизнь либо коммерческие тайны, эту новость можно отнести к разряду хороших. Надежное шифрование в содружестве с применением других мер безопасности эффективно против шпионов, занимающихся сбором информации или доказательств.

Если вы уже используете либо планируете начать использование утилит шифрования данных, послушайте несколько простых советов:

- Выбирайте приложения, в которых применяются известные и прошедшие экспертную оценку алгоритмы шифрования (такие, как AES, 3DES, Blowfish, IDEA, и т. п.). Не доверяйте программам с засекреченными алгоритмами шифрования: они могут содержать потайные ходы и потому их следует по возможности избегать.
- Предпочтительнее использовать приложения, распространяемые по принципу открытого кода. Благодаря доступности исходного кода, эксперты имеют возможность тщательного его изучения и поиска секретных лазеек или ошибок, а если вы достаточно опытный программист, то можете проанализировать этот программный код и скомпилировать его самостоятельно.
- На данный момент достаточно защищенными можно считать 128-битные ключи для симметричного шифрования и 1024-битные ключи для ассиметричного шифрования (имеется в виду технология использования пары открытого и секретного ключей). Если вы хотите гарантировать защищенность информации в будущем, подумайте об использовании ключей большей длины.
- Придерживайтесь строгой политики в отношении паролей и выбирайте устойчивые пароли!
- В зависимости от обстоятельств, постарайтесь хранить ваше программное обеспечение, предназначенное для шифрования, на дискете или CD-ROM. Если утилиты шифрования будут обнаружены непосредственно на жестком диске, они могут вызвать подозрения и заставить злоумышленника направить свои силы на взлом программы.
- Шифрование не является идеальной защитой на все случаи жизни. Брюс Шнайер, знаменитый криptoаналитик и гуру в вопросах безопасности, повторял это в течение многих лет и оказался прав. Шифрование должно являться составной частью многоуровневой защиты и серии контрмер.

Все программное обеспечение для шифрования данных можно поделить на три большие категории: приложения для шифрования сообщений электронной почты, приложения для шифрования файлов и приложения для шифрования «на лету».

## УТИЛИТЫ ШИФРОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ

Хотя для безопасного общения по электронной почте вы можете использовать любые известные вам программные средства, золотым стандартом в этой области стала утилита PGP (Pretty Good Privacy). Конечно, существуют и другие протоколы безопасной передачи данных по сети, однако благодаря своему широкому международному распространению PGP превратилась де-факто в стандарт безопасного общения по электронной почте.

**PGP.** Эта программа была разработана Филом Зиммерманом в 90-х годах XX века. Утилита, свободно распространяемая по принципу открытого кода, приобрела мировую славу благодаря своей устойчивости и невозможности взлома даже со стороны правительственные разведывательных учреждений (если вы хотите больше узнать об этой программе, посетите сайт разработчика [www.philzimmermann.com](http://www.philzimmermann.com)). Изначально разработанная в Соединенных Штатах и подпавшая под действие закона об экспорте криптографических технологий, PGP выскользнула за пределы США и распространилась по всему миру через Интернет.

В PGP используется принцип шифрования при помощи открытого ключа (также известного как метод асимметричного шифрования). Этот алгоритм основывается на применении двух ключей: открытого, который может распространяться между теми, кто заинтересован в безопасной передаче вам сообщений, и секретного, с помощью которого вы будете расшифровывать отосланые вам сообщения. (Вы не сможете расшифровать данные с помощью чьего-то открытого ключа.) Именно это является основным отличием данного алгоритма от технологии симметричного шифрования, в которой один и тот же ключ используется как для шифрования, так и для дешифрования информации.

Открытый и секретный ключи генерируются вами при первом использовании PGP (ключи генерировать достаточно просто, и они сохраняются в файлах). К примеру, если вы хотите гарантировать неприкосновенность вашей переписки с Эллис, которая также использует PGP, вам вначале придется обменяться открытыми ключами (PGP позволяет сделать это при помощи электронной почты). Затем, чтобы послать Эллис сообщение в зашифрованной виде, вам понадобится вначале создать сообщение, а затем зашифровать его в PGP при помощи открытого ключа, присланного Эллис. Получив ваше сообщение, Эллис может воспользоваться своим секретным ключом для его расшифровки, введя пароль, связанный с ее секретным ключом. (Углубившись в чтение книг по криптографии, вы будете постоянно встречать такие имена, как Эллис, Боб, Кэрол и, возможно, Ив. Эти имена никак не связаны с персонажами известного фильма 1969 года «Боб и Кэрол, Тэд и Эллис», просто использовать имена людей в сценариях шифрования гораздо удобнее, чем буквы А, В, С, Д и т. д.).

Еще одной причиной сенсационной популярности PGP может считаться ее способность работать практически на любой операционной системе. В начале своего существования PGP представляла собой простую утилиту DOS, не слишком удобную для использования. С тех пор прошло немало времени, и PGP успела обзавестись удобным и весьма дружественным интерфейсом Windows. Кроме того, появилось множество дополнительных подключаемых модулей для популярных почтовых клиентов, позволяющих интегрировать функции PGP непосредственно в вашу почтовую программу.

Коммерческая версия PGP ранее предлагалась компанией Network Associates, однако в 2002 году данная компания отказалась от продажи

этого продукта. В результате была сформирована новая независимая компания PGP Corporation, которая с июля 2002 года начала получать прибыль от продажи PGP. Новая коммерческая версия продукта, полностью совместимая с операционной системой Windows XP, должна была появиться в конце 2002 года\*. Детальная информация по PGP размещена на сайте [www.pgp.com](http://www.pgp.com).

Версия PGP, свободно распространяемая по принципу открытого кода, которая несколько ограничена в своих функциональных возможностях по сравнению с коммерческой версией, может быть загружена с веб-узла [www.pgpi.org](http://www.pgpi.org).

**GNUPG.** GNU представляет собой рекурсивный акроним\*\*, который расшифровывается как «GNU's Not Unix». Проект GNU стартовал в 1984 году для поддержки Unix-подобных свободно распространяемых операционных систем (более подробно о проекте GNU читайте на веб-узле [www.gnu.org](http://www.gnu.org)). В соответствии с принципами GNU и идеями свободно распространяемого программного обеспечения, построенного по принципу открытого кода (согласно общедоступной лицензии Фонда бесплатно распространяемых программ), и появилась такая программа, как GnuPG (GNU Privacy Guard).

Один из нюансов оригинального проекта PGP заключается в том, что в этой программе использовались алгоритмы, лицензированные у компании RSA (охранной компании, обладающей рядом патентов на криптографические алгоритмы) и запатентованный алгоритм шифрования данных IDEA (International Data Encryption Algorithm). Основной целью создания GnuPG послужила идея отойти от программного кода, имеющего ограничения на использование, сохраняя общую совместимость с PGP. На сегодняшний день GnuPG по-прежнему представляет собой утилиту командной строки, хотя для нее реализованы интерфейсы и надстройки под Windows. Если вы хотите узнать больше о проекте GnuPG и попробовать в деле саму программу, посетите веб-сайт [www.gnupg.org](http://www.gnupg.org).

## ПРОГРАММЫ ДЛЯ ШИФРОВАНИЯ ФАЙЛОВ

В отличие от шифрования сообщений электронной почты для обеспечения конфиденциальности переписки и ее защиты от прочтения в случае перехвата, программное обеспечение для шифрования файлов необходимо для защиты данных, постоянно хранимых на жестком диске, CD-R и других носителях информации.

При шифровании файлов обычно используются симметричные алгоритмы, в которых один и тот же ключ применяется как для шифрования, так и для расшифровки данных. С помощью специального программного обеспечения вы шифруете содержимое файла, а затем расшифровываете его при повторном обращении к файлу. Предположим, у вас есть файл с

---

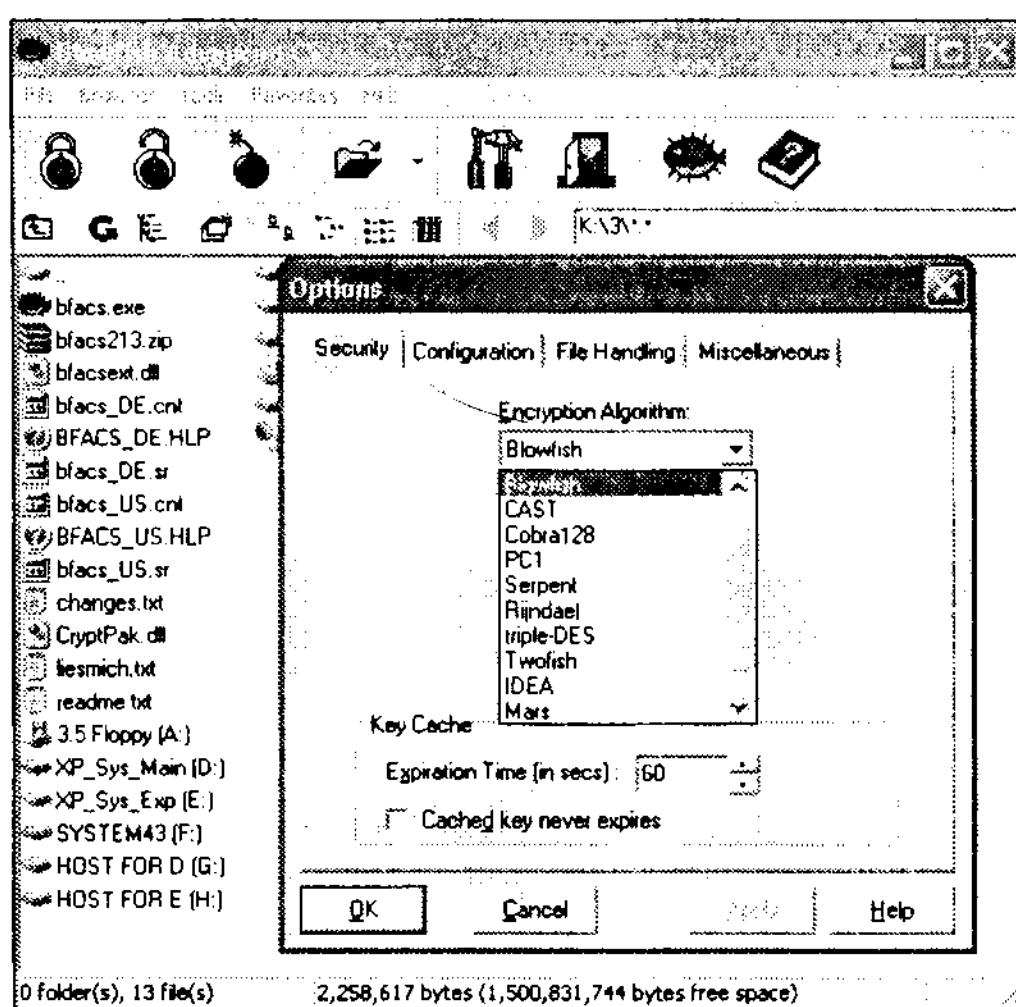
\* В настоящее время продается версия 8.0.3, полностью совместимая с Microsoft XP и Microsoft Office 2003. – Прим. ред.

\*\* Акроним, ссылающийся сам на себя. – Прим. перев.

таблицами, в которых содержится конфиденциальная финансовая информация. Завершив работу над созданием файла, вы сохраняете изменения и затем шифруете его содержимое. Когда вам снова понадобится поработать с этим файлом, вам придется расшифровать его, чтобы приложение по обработке таблиц могло открыть данный документ. Если некое неуполномоченное лицо получит доступ к вашему жесткому диску, оно все равно не сможет прочесть зашифрованную информацию, если только ему не будет известен еще и ваш пароль.

PGP также обладает функциями симметричного шифрования для файлов, однако в этой программе отсутствуют многие возможности, упрощающие выполнение регулярного шифрования и дешифрования файлов. Поэтому в качестве альтернативы мы предлагаем вам рассмотреть две другие программные утилиты, описания которых приводятся далее.

**BLOWFISH ADVANCED CS.** Blowfish Advanced CS – это свободно распространяемая по принципу открытого кода программа для шифрования файлов, автором которой является Маркус Хан. Она позволяет шифровать содержимое файлов и папок при помощи 11 современных алгоритмов шифрования (разумеется, включая оригинальный алгоритм Blowfish), как показано на рис. 5.5. В приложении также реализована возможность безвозвратного удаления файлов и ряд других функций диспетчера файлов. Сама утилита со всеми вспомогательными файлами легко умещается на одну дискету. Программу Blowfish Advanced CS вы можете скачать с сайта <http://maakus.dyndns.org/software.html>.



**Рис. 5.5.** Выбор пользователем алгоритма шифрования в Blowfish Advanced CS

**ABI-CODER.** Еще одной популярной программой для шифрования файлов, в которой используются алгоритмы Blowfish, 3DES и AES, является программа под названием Abi-Coder. При помощи этой утилиты вы сможете зашифровать множество файлов и папок и создавать саморасшифровывающиеся файлы. Полная версия Abi-Coder доступна для загрузки на сайте [www.abi-soft.net/bo.html](http://www.abi-soft.net/bo.html). Если вам понравится это приложение, то стоимость лицензии на него составляет всего \$12,99.



Если вы хотите найти другое бесплатное или условно бесплатное программное обеспечение для шифрования данных, просмотрите ссылки в разделе Security-Privacy сайта [www.webattack.com](http://www.webattack.com).

## ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ШИФРОВАНИЯ «НА ЛЕТУ»

Главный недостаток всех вышеперечисленных программ для шифрования файлов заключается в необходимости вручную выбирать файлы и папки для шифрования, а затем, опять-таки вручную, их расшифровывать, когда возникает необходимость работать с каким-то из зашифрованных файлов. Кодирование «на лету» позволяет решить эту проблему путем создания на жестком диске или другом носителе информации дополнительного зашифрованного тома. При помощи специального программного обеспечения создается том фиксированного размера, который затем шифруется и доступ к которому в дальнейшем вы сможете получить, только вызвав приложение расшифровки «на лету» и задав корректный пароль. После успешного подключения тома существующие файлы могут переписываться с него и на него с выполнением автоматического шифрования и дешифрования. Большинство приложений с возможностью шифрования на лету позволяют отключать зашифрованный том по нажатию «горячей клавиши» либо после определенного периода бездействия.

Программные пакеты, позволяющие выполнять шифрование на лету, позволяют сэкономить массу времени, поскольку вам не придется постоянно зашифровывать и расшифровывать файлы и папки вручную. Кроме того, подобное ПО очень удобно в использовании: после его установки в системе появляется как бы еще один логический диск, с которым можно работать как с любым другим диском.

**STEGANOS SECURITY SUITE.** Steganos Security Suite – это популярная в Европе программа, включающая в себя возможности шифрования на лету, функции безвозвратного удаления файлов и ликвидации доказательств, а также ряд других средств обеспечения безопасности. В приложении применяются устойчивые алгоритмы шифрования AES и BlowFish, кроме того, оно также является весьма удобным в использовании. Стоимость пакета Steganos Security Suite составляет \$29,95, а если вы вначале хотите увидеть его «живьем» – загрузите пробную версию с веб-сайта [www.steganos.com](http://www.steganos.com).

**BESTCRYPT.** BestCrypt – это одна из самых старых программ на рынке утилит шифрования на лету, позволяющая выполнять шифрование при помощи алгоритмов AES, GOST (Российский стандарт шифрования),

Blowfish и Twofish. Компания Jetico, разработчик программы, выпускает версии BestCrypt для операционных систем Windows и Linux, так что зашифрованные файлы могут читаться на любой из этих систем. Стоимость BestCrypt составляет \$89,95, а оценочная версия программы размещена на сайте [www.jetico.com](http://www.jetico.com).

## Контрмеры: файловая система EFS

В Windows 2000/XP может использоваться шифрованная файловая система EFS. Эта функциональная возможность шифрования файлов и папок «на лету», разработанная компанией Microsoft, ограничивает доступ к вашим документам только теми лицами, которые сумеют успешно войти в систему под вашей учетной записью. Однако с использованием файловой системы EFS под Windows 2000 связано два уязвимых места:

- Первоначальная версия Windows 2000, согласно правилам экспорта криптографических технологий, поддерживала только 56-битное шифрование, которое нельзя назвать устойчивым по сегодняшним меркам. Если вы являетесь «счастливым» обладателем старой версии Windows 2000, вам следует обновить ее, по крайней мере, до Service Pack 2 и установить 128-битный High Encryption Pack, доступный для загрузки с сайта компании Microsoft: [www.microsoft.com/windows2000/downloads/recommended/encryption/](http://www.microsoft.com/windows2000/downloads/recommended/encryption/).
- Во всех версиях Windows 2000, любое лицо, имеющее привилегии администратора, может получать доступ к файлам и папкам, зашифрованным с помощью EFS без дополнительного пароля. В Windows XP Professional эта ошибка была исправлена, и теперь только пользователь, указавший соответствующий пароль, может получить доступ к защищенным данным.

Хотя файловая система EFS хорошо выглядит на бумаге и в ее защите не обнаружено серьезных изъянов, вы вполне можете заняться поиском приложений сторонних разработчиков для защиты конфиденциальных данных из-за не слишком надежной репутации Microsoft в вопросах, касающихся защиты информации, и не в последнюю очередь из-за того, что система шифрования встроена в саму операционную систему (известные и неизвестные ошибки которой могут угрожать целостности данных).



Сара Дин в свое время составила полный (хотя на сегодняшний день и немного устаревший) список программ, предназначенных для шифрования данных «на лету», ознакомиться с которым вы можете по адресу [www.fortunecity.com/skyscraper/true/882/Comparison\\_OTFCrypto.htm](http://www.fortunecity.com/skyscraper/true/882/Comparison_OTFCrypto.htm).

**DRIVECRYPT.** DriveCrypt представляет собой коммерческую утилиту для шифрования дисков, которая была разработана на основе свободно распространяемых по принципу открытого кода программ Scramdisk и E4M. Их вы можете найти на сайте [www.samsimpson.com/scramdisk.php](http://www.samsimpson.com/scramdisk.php). Программа Scramdisk предназначена для работы в операционных системах Windows 9x/Me, и E4M (Encryption for the Masses) – для Windows 9x/Me/NT/2000. Помимо базовых существуют специализированные версии программы DriveCrypt, использующие код USB в качестве ключа или позволяющие выполнять шифрование диска целиком под Windows NT/2000/XP. Стоимость DriveCrypt составляет \$49,95, а испытательная версия программы и дополнительная информация по ней размещены на веб-странице [www.drivecrypt.com](http://www.drivecrypt.com).

## Стеганография

Стеганографию можно назвать искусством и наукой одновременно. Она ставит своей целью скрытие секретных сообщений среди другой, неsekретной информации. Сама концепция стеганографии далеко не нова:

- Еще 2,5 тысячи лет назад древние греки удаляли воск с дощечек для письма и выцарапывали секретные послания на самом дереве. Затем дощечки покрывались свежим слоем воска, который скрывал по-настоящему важное донесение. Кроме того, они наносили татуировки на выбритые головы своих рабов, ожидали, пока у тех отрастут волосы, после этого отправляли их в качестве секретных посланников.
- Во время Первой мировой войны оба воюющих лагеря использовали стеганографию для передачи шпионских сообщений. К примеру, немецкий агент должен был передать следующее сообщение: «Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oil», которое звучит в переводе довольно загадочно: «Предположительно, протесты нейтральных лиц были не приняты в расчет и проигнорированы. Айсмен тяжело ранен. Факт блокады служит предлогом для введения эмбарго на поставки побочных продуктов, кроме почечного сала и растительных масел». Однако если вы выпишите вторые буквы из каждого слова, то получите совершенно другое сообщение: «Pershing sails from NY June 1», т. е. «Першинг отплывает из Нью-Йорка 1 июня».
- В ходе Второй мировой войны немцы разработали технологию микроточек, позволяющую сжимать сообщение до размеров символа точки печатной машинки. Эти микроточки могли добавляться к точке в конце предложения, так что обнаружить их мог только получатель, который знал об их существовании.

Стеганография в современной интерпретации сводится к использованию цифровых носителей для передачи секретных посланий. К примеру, вы можете взять графический файл формата .jpeg и внедрить в него зашифрованное текстовое сообщение с помощью специального программного обеспечения. По условию, сама фотография при этом должна открываться в графическом приложении без каких бы то ни было искажений. Только тот, кому известно о существовании тайного послания внутри файла, может воспользоваться соответствующим программным обеспечением, чтобы извлечь его. Графические и звуковые файлы идеально подходят для стеганографии, поскольку их формат предполагает побитовое кодирование информации, в котором легко зашифровать сообщение, которое внесет лишь небольшие (как правило, незаметные) помехи в исходный файл. Для транспортировки секретных сообщений подходят файлы следующих форматов:

- |                                |                               |
|--------------------------------|-------------------------------|
| <input type="checkbox"/> .AU   | <input type="checkbox"/> .MP3 |
| <input type="checkbox"/> .BMP  | <input type="checkbox"/> .PCX |
| <input type="checkbox"/> .GIF  | <input type="checkbox"/> .PDF |
| <input type="checkbox"/> .HTML | <input type="checkbox"/> .PNG |
| <input type="checkbox"/> .JPG  | <input type="checkbox"/> .WAV |

Подобно тому, как это делали немцы во время Первой мировой, для шифрования сообщений вы можете воспользоваться и текстовыми файлами. Такие услуги всем желающим предлагает веб-сайт SpamMimic. Ваше короткое сообщение будет зашифровано в виде электронного письма «спамового» характера. Вам останется только скопировать получившееся послание в ваш почтовый клиент (или временную учетную запись электронной почты в Интернете, которую трудно отследить) и отправить его адресату. Когда тот получит ваше сообщение, то для его расшифровки ему также потребуется посетить сайт SpamMimic. Адрес сайта в Интернете: [www.spammimic.com](http://www.spammimic.com).

Стеганография может использоваться в качестве контрмеры для скрытия ключевой информации среди массы других документов. Это может оказаться критичным для стран, в которых использование шифрующего программного обеспечения запрещено законом, или в ситуациях, когда наличие зашифрованных файлов способно возбудить подозрение и привлечь ненужное внимание.

Если вы решили воспользоваться техникой стеганографии, вам необходимо придерживаться следующих правил:

- Не оставлять улики, указывающие на использование вами стеганографической утилиты. Если следователь найдет на вашем компьютере копию такой программы, как S-Tools, например (сама утилита будет обсуждена чуть позже), у него, разумеется, возникнет мысль, а не пользуетесь ли вы случайно ею для сохранения информации внутри других файлов.

## Тактика: шифровальщик Осама Бен Ладен?

В феврале 2001 года стеганография вышла из мира призраков и вырвалась на первые полосы газет. По сообщениям газеты USA Today, для общения с членами террористических групп через Интернет Осама Бен Ладен использовал стеганографию. Якобы террористическая сеть Аль-Каида передавала информацию при помощи более чем 2 000 000 000 сайтов и около 28 000 000 000 картинок, распространяемых через Интернет, зашифровывая свои послания в файлах совершенно невинного содержания.

После террористической атаки 11 сентября слухи поползли с новыми силами. Из разных источников поступали сообщения о том, что последователи Бен Ладена пересылали сотни зашифрованных сообщений электронной почты, скрытых в цифровых фотографиях eBay; исламский веб-сайт Azzam.com хранил фотографии со скрытыми посланиями; а организация Аль-Каида обменивалась электронными сообщениями через фотографии порнографического содержания, размещенные на веб-сайтах, ориентированных на взрослую аудиторию. Имеются сведения об обнаруженной связи между снимками, содержащими зашифрованные послания, и обращениями к ним из интернет-кафе в Пакистане и публичных библиотек по всему миру.

Тем не менее никто из официальных представителей правительства не подтвердил, что Аль-Каида либо какая-то другая террористическая группировка использовали стеганографию в своих целях. (Возможно, эти приемы использовались в единичных случаях, но явно не в таких масштабах, как утверждают слухи.)

Компьютерный исследователь из университета в Мичигане Ниэлс Превос провел в ноябре 2001 года в группе новостей USENET поиск фотографий, которые могли содержать зашифрованные сообщения. Эта сфера поиска была избрана им потому, что распространение через группы новостей секретных посланий – наилучший способ уйти от ответственности, поскольку здесь достаточно сложно определить как отправителя, так и главного получателя зашифрованных сообщений. Команда под руководством Ниэлса изучила более двух миллионов цифровых снимков и не нашла никаких доказательств присутствия в них скрытых посланий.

Отчеты о результатах исследования вы можете прочесть в Интернете по адресу [www.citi.umich.edu/u/provos/stego/usenet.php](http://www.citi.umich.edu/u/provos/stego/usenet.php).

- Всегда шифруйте любые сообщения, которые вы намерены передать методом стеганографии.
- Используйте для сохранения сообщений файлы, которые не вызовут подозрений. К примеру, поместив искомый текст сообщения в файл формата mp3 и сделав его доступным через сеть обмена файлами P2P (Peer to Peer), например Kazaa, вы не привлечете к себе особого внимания. Но обмен электронными сообщениями, содержащими вложенные снимки Юпитера (если только вы и ваш адресат не астрономы), может показаться весьма подозрительным.
- Не применяйте в качестве носителей файлы, которые можно встретить повсеместно в сети Интернет, – вы же не хотите, чтобы противник мог сравнить ваш файл с оригиналом и найти различия. Поэтому широко распространенные в Интернет фотографии, клипы и т. д. явно не стоит использовать в качестве несущих файлов.
- Не делайте ставку исключительно на методы стеганографии, если вашим противником являются правительственные разведывательные управлении. В 1999 году Andreas Westfeld и Andreas Fietzmann (<http://os.inf.tu-dresden.de/~westfeld/publikationen/ihw99.pdf>) описали алгоритм визуального и статистического анализа для обнаружения вложенных стеганографических сообщений. Ниэлс Провос из Мичиганского университета написал программу Stegdetect, умеющую обнаруживать наличие скрытых посланий, созданных при помощи большинства популярных утилит стеганографии (этую программу вы можете загрузить с сайта [www.outguess.org](http://www.outguess.org)). Несложно догадаться, что разведуправления имеют в своем распоряжении достаточно инструментальных средств для обнаружения данных, скрытых посредством различных утилит цифровой стеганографии.

Среди всего разнообразия утилит для стеганографии мы предлагаем вам обратить внимание на две наиболее популярные и простые в использовании программы, с помощью которых вы сможете поэкспериментировать с приемами стеганографии и лучше понять данную методику.

## S-TOOLS

Программа S-Tools, написанная Эндрю Брауном, стала одной из первых стеганографических программ для ОС Windows. Хотя новые версии не выходили вот уже несколько лет, она по-прежнему считается удобной в использовании программой с мощными возможностями. Программа S-Tools позволяет добавлять сообщения в файлы форматов .BMP, .GIF и .WAV в виде простого текста либо в зашифрованном виде. Эта утилита является свободно распространяемой и загрузить ее можно с веб-сайта <ftp://ftp.uni-stuttgart.de/pub/rus/security/win95/s-tools4.zip>.

## WBSTEGO

Утилита под названием wbStego4, разработанная Урнером Бэйлером, позволяет помещать данные внутри файлов изображений, текстовых файлов ASCII и ANSI, файлов .HTML и документов Adobe Acrobat (.PDF). Программа имеет дружественный интерфейс и обладает поддержкой шифрования. Стоимость wbStego4 составляет \$20, а ее оценочная версия доступна по адресу <http://wbstego.wbailer.com/>.



Достаточно полный список различного программного обеспечения для стеганографии вы можете найти по адресу <http://stegoarchive.com>.

## Программы безвозвратного удаления файлов

Очевидно, что полагаться на Windows в плане эффективного удаления файлов без возможности восстановления нельзя. Если вы хотите обеспечить безопасность удаляемых файлов, вам понадобятся для этой цели специальные утилиты. Принцип работы подобных утилит заключается в том, что они перезаписывают содержимое файла перед его удалением. Таким образом, даже если удаленный файл будет восстановлен, в нем не будут содержаться исходные данные.

Существует четыре подхода к удалению файлов с жесткого диска без возможности восстановления: DoD NISPOM, DoD 5200.28 STD, Gutmann и перезапись содержимого файла псевдослучайными данными.

- Руководство по Национальной программе промышленной безопасности Министерства обороны (Department of Defense National Industrial Security Program Operating Manual – DoD NISPOM) содержит основные рекомендации по безопасному удалению конфиденциальной информации с различных носителей (онлайновая версия этого руководства доступна на сайте [www.css.mil/isec/chapter8.htm](http://www.css.mil/isec/chapter8.htm)). Чтобы не допустить прочтения информации, вы можете применить метод размагничивания жесткого диска с помощью устройств разового стирания первого и второго типов, перезаписать информацию на носителе путем записи последовательности «символ – его дополнение – случайный символ» с проверкой. Если носитель содержал информацию под грифом «совершенно секретно», он должен быть разобран, сожжен, измельчен механическим способом либо расплавлен. Во многих из существующих программ удаления файлов используется стандарт Министерства обороны для безвозвратного удаления информации (но не забывайте, что правительство однозначно оговаривает, что подобный метод удаления информации не подходит для данных категорий «совершенно секретно»).
- Стандарт Министерства обороны 1985 года по критериям оценки надежных компьютерных систем 5200.28 STD (Trusted Computer System Evaluation Criteria) пришел из Оранжевой книги

«радужной» серии стандартов компьютерной безопасности. Стандарт предусматривает многократную запись случайной информации в файл перед его удалением. (Отличным информационным ресурсом по безопасному удалению информации с разных типов носителей является Руководство по безопасности в отношении остаточной намагниченности, изданное Военно-морским флотом США в 1993 году, электронная версия которого доступна на сайте [www.fas.org/irp/doddir/navy/5239\\_26.htm](http://www.fas.org/irp/doddir/navy/5239_26.htm).)

- В 1996 году Питер Гутман опубликовал документ под названием «Безопасная очистка памяти, в которой для хранения информации используются магнитные или полупроводниковые материалы». (Этот документ можно найти в сети Интернет по адресу [www.cs.auckland.ac.nz/~rgut001/pubs/secure\\_del.html](http://www.cs.auckland.ac.nz/~rgut001/pubs/secure_del.html).) В соответствии с аргументами Гутмана, исходя из существующего алгоритма записи информации на жесткий диск, даже при перезаписи файлов возможно восстановление первоначальных данных при помощи электронного микроскопа. Гутман заявил, что невозможность восстановления данных таким способом гарантируется только после приблизительно 30-кратной перезаписи. Правило Гутмана также учитывается во многих программах безвозвратного удаления файлов.
- Еще один метод удаления информации без возможности восстановления сводится к записи на носитель псевдослучайной информации. Многие утилиты безопасного удаления файлов действуют подобным образом, обладая функциями задания количества проходов перезаписи.

Какой метод удаления информации наилучшим образом подходит для вас? Для ответа на этот вопрос определите, кто может быть заинтересован в получении доступа к вашей информации и какими средствами располагает ваш потенциальный противник. Если вам не нужна защита от шпионажа правительенного уровня, однопроходной перезаписи данных перед удалением файла будет вполне достаточно. (Учтите, что перезапись информации требует времени.)

Итак, мы выяснили, что одним из инструментов восстановления исходных данных после перезаписи является электронный микроскоп. Согласно документу Гутмана, даже после перезаписи информации существует остаточная намагниченность (от ранее записанных данных), по которой в лабораторных условиях при помощи электронного микроскопа может быть восстановлена исходная информация. Электронный микроскоп действительно представлял серьезную угрозу в 1996 году, когда был обнародован данный документ. Но с тех пор технология записи данных на жесткие диски подверглась усовершенствованиям, и во многих современных носителях теперь применяется расширенный алгоритм PRML (Partial Response Maximum Likelihood – частичный ответ, максимальное подобие) в сочетании с новейшими дизайнерскими решениями. Поэтому восстановить данные с современных жестких дисков намного сложнее по сравнению с дисками, выпущенными несколько лет назад.

## Разоблачения: Анна Белен Монтес

Анна Белен Монтес работала на должности старшего аналитика в Разведывательном управлении Министерства обороны США в Вашингтоне, округ Колумбия. Поступив на работу в Разведывательное управление еще в 1985 году, с 1992 года она стала специализироваться на делах, связанных с Кубой. Занимая ответственную должность, Анна имела доступ ко многим секретным документам, являясь отличным кандидатом на роль резидента кубинской разведки.

Для координации действий своих шпионов кубинская разведка использует технологию так называемых цифровых станций. Как следует из названия, эти станции с неизвестным местонахождением передают в эфир на коротких волнах последовательность цифр. Неизвестный голос, как правило женский, медленно зачитывает эту последовательность. Подобные станции существуют по всему миру и вещают на разных языках. Эти радиопередачи предназначены для секретного общения со шпионами. Хотя настроиться на волну определенной станции может каждый обладатель коротковолнового приемника, однако в состоянии расшифровать эти сообщения только те, кому они были адресованы. (Информацию по цифровым станциям и реальные записи их вещания в эфире вы можете увидеть и услышать в Интернете по адресу [www.spurnumbers.com](http://www.spurnumbers.com).)

Инструкции из Кубы Монтес получала, прослушивая цифровые станции на своем портативном приемнике производства фирмы Sony. По мере прослушивания она записывала числа на свой мобильный компьютер, а затем расшифровывала сообщения.

ФБР начало подозревать Анну в шпионаже, и в мае 2001 года агенты Федерального Бюро провели санкционированное судом тайное проникновение в ее жилище, сделав дубликат содержимого жесткого диска. Технические специалисты восстановили удаленные с жесткого диска файлы, которые помогли доказать причастность Монтес к факту шпионажа. В одном из файлов содержался следующий текст на испанском:

«Ты обязательно должна удалять каждый файл при помощи программы безопасного удаления, как мы обсуждали в ходе нашего контакта. Это необходимо делать всегда, когда ты получаешь от нас радиосообщение или какой-то диск».

К сожалению, Монтес не послушалась наставлений своего руководства и теперь расплачивается за свою несознательность 25-летним сроком заключения.

В отличие от жестких дисков, дискеты, благодаря своим конструктивным особенностям, позволяют достаточно легко восстанавливать исходную информацию даже после ее перезаписи. Поэтому в соответствии со стандартами NISPOM дискеты следует уничтожать физически.

На рынке представлено огромное множество программ, предназначенных для безопасного удаления файлов. Одной из лучших можно считать утилиту Eraser, свободно распространяемую по принципу открытого кода, автором базовой версии которой является Сэмми Толванен. Помимо безопасного удаления отдельных файлов, Eraser умеет очищать неиспользуемое дисковое пространство. Загрузить программу вы можете из Интернета по адресу [www.heidi.ie/eraser/](http://www.heidi.ie/eraser/).



Полный перечень и описание программ, предназначенных для удаления файлов без возможности восстановления, можно найти по адресу: [www.fortunecity.com/skyscrapers/true/882/Comparison\\_Shredders.htm](http://www.fortunecity.com/skyscrapers/true/882/Comparison_Shredders.htm).

## Программное обеспечение для уничтожения доказательств

Разумеется, вы можете начать уничтожение доказательств вручную, воспользовавшись программами безопасного удаления файлов, стандартной утилитой RegEdit либо набором пакетных файлов для очистки диска от оставленных браузером артефактов, временных файлов и записей реестра. Но если вы хотите облегчить свой труд, советуем вам обратить внимание на ряд коммерческих утилит, предназначенных для автоматического уничтожения улик на вашем жестком диске. Большинство из них обладают схожим набором функций: удаление файлов, оставленных после себя браузерами, и ссылок на недавно использовавшиеся файлы; безопасное удаление временных файлов и уничтожение других электронных доказательств. Благодаря таким программам вы сможете сэкономить массу времени, необходимого для ручной очистки системы от потенциальных доказательств.

Однако при выборе программ подобного рода (и любых приложений, позиционируемых на рынке как средство уничтожения электронных доказательств) не нужно слепо полагаться на рекламу. Из-за роста популярности программного обеспечения для уничтожения улик, рекламу таких программ можно встретить в самых неподходящих местах, причем иногда в качестве рекламы используются довольно сомнительные приемы. Хотя разработчики, как правило, честно решают поставленные задачи, однако никто не может дать вам гарантии, что после запуска данного программного продукта информация с вашего диска действительно не будет подлежать восстановлению. Поскольку для такого рода программ не предусмотрены службы поддержки, куда вы могли бы направить отчет об обнаруженных неисправностях, а на вашем жестком диске имеется конфиденциальная информация, которой может кто-то заинтересоваться, –

после применения выбранного вами программного обеспечения для уничтожения доказательств необходимо обязательно проверить возможность восстановления удаленных данных при помощи средств восстановления информации. Итак, теперь, когда вы получили достаточно информации, ресурсов и средств, вы можете примерить на себя шпионское обличье и проверить, насколько надежными являются используемые вами меры. (При этом не забывайте классифицировать ваших противников на возможных и вероятных. Большинству простых обывателей вряд ли стоит из кожи вон лезть, чтобы приобрести электронный микроскоп стоимостью \$50 000 только для проверки возможности восстановления с жесткого диска удаленных данных.)

Среди популярных приложений, предназначенных для уничтожения электронных доказательств, можно перечислить следующие:

### **WINDOW WASHER**

Window Washer стала одной из первых программ, позволяющих убирать «хвосты» после работы браузеров. Теперь это приложение с широкими возможностями, которое позволяет выполнять очистку остатков кластеров, безопасно удалять заданные пользователем файлы, папки и ключи реестра. В нем также можно задавать расписание для автоматической очистки компьютера от возможных доказательств. Для программы Window Washer существует более 150 подключаемых модулей, позволяющих работать с различными приложениями для удаления любых потенциальных улик с жесткого диска вашего компьютера. Цена программы составляет \$29,95, а ее демонстрационная версия размещена на сайте [www.webrobot.com/washer.htm](http://www.webrobot.com/washer.htm).

### **SURFSECRET PRIVACY PROTECTOR**

Программа SurfSecret Privacy Protector обладает дополнительными возможностями, такими как очистка диска по расписанию и режим «невидимки». Стоимость программы составляет \$39,95, а пробную версию можно загрузить с веб-сайта [www.surfsecret.com](http://www.surfsecret.com).

### **CYBERSCRUB**

Еще одно приложение, предназначенное для уборки оставляемых браузером «хвостов» и уничтожения других электронных доказательств, называется CyberScrub. Профессиональная версия CyberScrub стоит \$49,95, а демонстрационная версия доступна на сайте [www.cyberscrub.com](http://www.cyberscrub.com).

## Заключение

Как видите, из вашего компьютера можно извлечь целый ворох доказательств. Компьютерные полицейские и судебные эксперты бывают достаточно настойчивы, когда речь заходит о необходимости получения доступа к этим данным, причем используемые ими методы и средства не менее активно применяются и обычными шпионами.

Таким образом, для того чтобы защитить себя от сбора доказательств с жесткого диска и других носителей информации, вы можете прибегнуть к трем основным контрмерам:

- шифрованию конфиденциальных сообщений электронной почты;
- шифрованию конфиденциальных документов;
- безопасному удалению всех артефактов, оставляемых программами или самой операционной системой.

Не следует всецело полагаться на технологические решения для обеспечения безопасности вашей системы. Помимо использования различных инструментальных средств необходимо строго соблюдать соответствующую политику безопасности – например, иметь надежные пароли, использовать шифрование и своевременно уничтожать улики. При этом политика безопасности должна соблюдаться не только вами лично, но и на уровне организации в целом (помните, что политика представляет собой всего лишь набор базовых принципов; вам не нужно быть служащим огромной корпорации, чтобы составить собственную политику безопасности). Учтите также, что в большинстве случаев для сохранности конфиденциальных данных человеческий фактор представляет большую опасность, чем технологические огехи.

## Глава 6

# Взлом защищенных данных

«Какая частота, Кэннет?»

R.E.M., «What's the Frequency, Kenneth?» *Monster*

Факт проникновения в компьютерную систему еще не означает, что вы немедленно получите доступ ко всей информации или доказательствам, хранимым на жестком диске. Смекалистые, подозрительные либо просто страдающие паранойей пользователи, которые заинтересованы в защите информации, часто прибегают к шифрованию данных (возможно, даже при помощи одной из утилит, описанных в главе 5 книги, либо, по крайней мере, защищают файлы при помощи встроенной парольной защиты, имеющейся в большинстве коммерческих программных продуктов).

Когда заходит речь о защите информации, принимаются во внимание два фактора, способных ввести пользователя в заблуждение о надежности защиты данных. Первый связан с использованием нестойких алгоритмов шифрования, которые легко взломать, а второй – с ненадежностью пароля, который легко угадать. Причем оба фактора тесно взаимосвязаны друг с другом: нестойкий алгоритм шифрования может свести на нет все усилия по придумыванию замысловатого пароля, а в случае с ненадежным паролем использование стойкого алгоритма шифрования также бесполезно. Шпиону достаточно наличия одного из вышеперечисленных факторов, и тогда ваши данные окажутся под угрозой.

В этой главе мы обсудим возможности взлома защищенных данных путем использования слабостей человеческой натуры и уязвимых мест технологий, а также шаги, которые должны быть предприняты вами для защиты конфиденциальной информации от посторонних глаз.

## Шпионская тактика

Даже если файл зашифрован, никто не может гарантировать вам, что защищенная информация не может быть взломана. Опытный компьютерный шпион знает о существовании множества шпионских утилит и технологий расшифровки защищенных данных. Сейчас мы и вам представим возможность приобрести некоторый опыт в данной области.

Итак, примерьте снова ваши темные очки и неброский плащ и представьте себя в роли тайного агента, работающего на безымянное разведывательное управление, в задачи которого входит проникновение в ряды международной террористической организации в стране третьего мира (звучит достаточно актуально, не правда ли?). В ходе расследования вы вышли на подозреваемого, который, возможно, причастен к поставкам оружия и поддержке известной террористической группы. При содействии местных властей было организовано тайное проникновение в жилище подозреваемого, где вы надеялись найти что-нибудь интересное, пока объект отправился в поход по магазинам. Воспользовавшись техникой тайного проникновения, изученной в главе 3, вы вторглись в его дом. На столе вы обнаружили старенький ноутбук фирмы Compaq, работающий под управлением операционной системы Windows 95 (даже если этот человек действительно имеет отношение к террористической организации, она явно не страдает от избытка финансирования). Предположительно, подозреваемый будет отствовать не более 15 минут. У вас нет времени снимать образ всего жесткого диска, поэтому вы быстренько копируете несколько папок с наиболее интересными названиями на дискеты. Затем вы фотографируете помещение и планируете вернуться сюда еще раз, когда в вашем распоряжении будет достаточно времени, чтобы скопировать жесткий диск целиком.

Вы проверяете, не остались ли случайно следы вашего пребывания в доме, после чего покидаете здание и обходными путями добираетесь в свой офис. Сбросив черный плащ и смыв грим, вы вставляете одну из дискет в накопитель вашего компьютера и щелкаете на файле таблицы Excel. Программа загружается, однако перед вами появляется окно ввода пароля. Вы разражаетесь ругательствами, поскольку никаких бумажек с паролями вы не нашли ни на столе, ни где-либо еще в квартире подозреваемого и у вас отсутствуют какие-либо соображения по поводу возможного пароля. В сердцах вы щелкаете на кнопке Отмена и закрываете приложение. Затем вы пытаетесь просмотреть файл в редакторе шестнадцатеричных кодов, чтобы найти хоть какую-нибудь зацепку, однако файл выглядит совершенно безнадежно. Все остальные документы и электронные таблицы также оказываются зашифрованными. Время работает против вас, поскольку источники в разведке сообщают о возросшей активности зашифрованных телефонных переговоров и обмена информацией через онлайновые чаты, что свидетельствует о подготовке очередного террористического акта в ближайшем будущем. А изъятые вами документы могут содержать планы террористов. Технических специалистов внутри страны вы найти не можете, зашифрованный канал связи с Ленгли\* не работает, а на передачу файлов для расшифровки в США через дипломатическую почту нет времени. Что вы предпримете для взлома зашифрованной информации?

---

\* Город в штате Виргиния в США, где размещается штаб-квартира ЦРУ. – Прим. ред.

## Использование слабых мест

В данной ситуации у вас есть несколько вариантов решения проблемы. Когда дело касается получения доступа к секретной информации, применяют все доступные методы: поиск уязвимых мест с технической точки зрения и использование человеческого фактора. Поэтому вам необходимо иметь общие представления о способах защиты данных в конкретном приложении и о том, какие действия человека могут понизить эффективность защиты информации.

### НЕСТОЙКОЕ ШИФРОВАНИЕ

Первое место в списке технологических изъянов принадлежит использованию нестойких алгоритмов шифрования. В этих случаях, несмотря на внешнюю защищенность, информация может быть легко взломана из-за следующих факторов:

- **Нестойкий алгоритм шифрования.** Программист (или его начальник) могли безответственно отнестись к реализации данной технологии защиты. Возможно, разработчики не обладали квалификацией в плане криптографии либо вообще не ставили себе целью обеспечение должной защищенности программного продукта. В конце концов, если клиенты не требуют высокого уровня защиты данных, тогда почему этот вопрос должен волновать компанию по производству программного обеспечения? К примеру, большинство коммерческих приложений, выпущенных в начале, да и в середине 1990-х, использовали для шифрования документов простейшую схему XOR (логические операции «исключающего ИЛИ») – для расшифровки подобных документов требовались считанные секунды. Эрик Томпсон, основатель компании AccessData, пионера в области восстановления утерянных паролей, признал, что в своих ранних программах он использовал пустые циклы для увеличения времени подбора пароля, чтобы пользователи считали, что применяемые ими алгоритмы шифрования достаточно надежны и для взлома зашифрованной с их помощью информации требуется немало времени.
- **Ошибки и недостатки алгоритмов шифрования.** Этот пункт следует рассматривать отдельно от предыдущего, поскольку здесь речь пойдет о достаточно стойких алгоритмах шифрования, в которых были допущены явные или скрытые ошибки. В качестве примера можно привести алгоритм шифрования CSS (Content Scrambling System), метод шифрования, используемый для защиты DVD-дисков от пиратского копирования и поддержки региональных ограничений. Этот алгоритм оказался совершенно ненадежным: в 1999 году 15-летний норвежский студент восстановил алгоритм и разработал утилиту дешифрования под

названием DeCSS, позволяющую взламывать зашифрованный DVD и переписывать его в расшифрованном виде на жесткий диск.

- **Криптографические программы с «черным ходом».** Еще один способ облегчения доступа к защищенным данным состоит в модификации исходного кода приложения, в результате чего в приложении начинает применяться нестойкий алгоритм шифрования (облегчающий взлом данных) либо осуществляется запись пароля на диск. К примеру, можно модифицировать программный код PGP таким образом, чтобы при шифровании использовался не 1024-битовый, а всего 40-битовый ключ, делая зашифрованные сообщения легкой добычей шпиона. Подменив оригинальную версию программы PGP на компьютере пользователя, можно добиться того, что все шифруемые в дальнейшем файлы будут использовать алгоритм шифрования с нестойким ключом.

Быстрое распространение информации по сети Интернет, особенно той, что связана с вопросами безопасности, позволяет злоумышленникам постоянно находиться в курсе событий, оперативно узнавать обо всех только что обнаруженных уязвимых местах крипtosистем и новых средствах для расшифровки данных, зашифрованных при помощи недостаточно стойких алгоритмов. Примером может служить дело, связанное с алгоритмом CSS: несмотря на то, что в 2001 году федеральный судья запретил журналу 2600 распространять программу DeCSS на своем сайте, эта утилита со своим исходным кодом и подробным анализом алгоритма CSS настолько успела распространиться по сети, что загнать однажды выпущенного джина обратно в бутылку теперь не представляется возможным.



Когда дело касается криптографии, каждый шпион обязан изучить два нетехнических документа под авторством Брюса Шнейера, в которых обсуждаются сильные и слабые стороны криптографических технологий, а также наиболее распространенные подводные камни. Речь идет о документах «Почему криптография намного сложнее, чем это кажется на первый взгляд» (<http://www.schneier.com/essay-whycrypto.html>) и «Подводные камни криптографии» (<http://www.schneier.com/essay-pitfalls.html>).

## НЕНАДЕЖНЫЕ ПАРОЛИ

В качестве пресловутого человеческого фактора в нашей задаче выступают пароли, предназначенные для аутентификации пользователей. Если вам известен пароль, значит, вы именно тот человек, который имеет право на доступ к информации. Поскольку большинство приложений полагаются в первую очередь на пароль при защите информации путем шифрования и дешифрования, то именно пароль является первичной целью на пути любого шпиона. (То же самое верно и в случае преодоления уровня защиты операционной системы, о чем шла речь в главе 4 данной книги.)

Пароль может быть правильным или неправильным. Кроме того, пароли можно разделить на надежные и ненадежные. Ненадежный пароль – это имя вашей жены, дата рождения домашнего зверька, любое слово из словаря, ваша фамилия с добавленной цифрой в конце либо любая другая комбинация букв и цифр длиной менее семи-восьми символов. Ненадежные пароли легко могут быть угаданы хакером вручную либо при помощи специальных утилит. Надежные пароли, с другой стороны, устойчивы к подобным видам атак.

Если ненадежные пароли представляют собой такую угрозу безопасности, тогда почему же люди продолжают использовать их? Чтобы ответить на этот вопрос, нам понадобится изучить психологию выбора пароля. Перефразируя рыцарей джедаи (да простят мне они мою дерзость), можно сказать: «Сила может победить благодаря слабым паролям».



Существует масса литературы, посвященной шпионажу, которую вам стоило хотя бы пролистать. Конечно, эти источники могут показаться несколько устаревшими и не всегда уместными (поскольку они не относятся к теме паролей в Windows), но на самом деле они помогут вам прийти к современному пониманию проблемы паролей. Среди этих источников: статья «Безопасность, обеспечиваемая паролями: история одного дела», опубликованная в 1979 г. под авторством Кена Томпсона и Роберта Морриса (<http://lambda.cs.yale.edu/cs422/doc/unix-sec.pdf>); статья «Защита в UNIX с помощью паролей, 10 лет спустя», опубликованная в 1990 г. под авторством Дэвида С. Филдмайера и Филиппа Р. Карна (<http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C89/44.PDF>); и статья Дэниела В. Клейна «Расстраиваем планы хакера: исследование и повышение безопасности с помощью паролей», опубликованная в 1991 г. (<http://geodsoft.com/howto/password/klein.pdf>).

**КАК ЛЮДИ ВЫБИРАЮТ ПАРОЛИ.** Когда перед вами встает задача взлома защищенных данных, очень важно понять принцип, которым руководствовался тот или иной пользователь при выборе пароля. Почему, зная, что в стандартной программе проверки орфографии содержится до 100 000 слов, некоторые люди продолжают использовать в качестве паролей слова, которые можно найти в словаре? Но прежде чем углубляться в изучение психологии среднестатистического компьютерного пользователя, приведем для начала некоторые общие соображения.

- **Безопасность – это обуза.** Большинство компьютерных пользователей считают применение мер безопасности излишней головной болью и поэтому всячески стараются избегать их ради собственного удобства и экономии времени. Такое отношение приводит к использованию простых и коротких паролей, которые легко запомнить, вроде общепринятых терминов либо последовательного нажатия клавиш (например, 12345 или qwerty).

- **Люди не надеются на свою память.** Хотя мозг человека можно считать одним из мощнейших суперкомпьютеров, ему недостает надежности в плане хранения информации в памяти. Запоминание паролей как раз и относится к той области, в которой человеческий мозг не слишком преуспел. Данный фактор также обуславливает использование коротких и легко запоминающихся паролей.
- **Осведомленность в вопросах безопасности не является приоритетной.** Давайте поставим вопрос ребром: если вы читаете эту книгу, значит, вы не принадлежите к тем рядовым пользователям компьютера, которые не используют брандмауэр для своего кабельного модема, работают с антивирусной программой, базы к которой не обновлялись в течение года, и могут случайно заразить вирусом Klez половину компьютеров вдоль Восточного побережья. Подавляющее же большинство компьютерных пользователей либо вообще не понимают, насколько уязвимыми они являются в плане безопасности, либо их это абсолютно не заботит. В любом случае мы опять возвращаемся к проблеме ненадежных паролей.

Теперь попытаемся понять психологию пользователей и причины, побуждающие их выбирать определенные пароли. Раньше, не считая последних несколько лет, каких-то серьезных исследований в области психологических аспектов, влияющих на выбор паролей пользователем, не велось. В настоящее время становятся известными результаты исследований, содержащие любопытные взгляды на проблему подбора паролей для защиты информации. Эти результаты в первую очередь интересуют шпионов, которым необходимо подбирать пароли для взлома зашифрованных данных. Приведем результаты одного из недавних исследований, проведенных британскими психологами, в ходе которого 1200 клеркам был задан вопрос о том, какие пароли они используют.

- 30% пользователей были отнесены к категории «фанатов», поскольку их пароли можно легко разгадать, изучив обстановку кабинета и рабочий стол. Предположим, что во время проникновения в дом подозреваемого в связях с террористическими организациями вы обнаружили на стене портрет бейсболиста из «Сиэтл Маринер» с автографом, постер Ичиро Судзуки и бейсбольную биту, подписанную Луи Финелла. Все ясно! Если верить результатам опроса в Британии, то подобные «фанаты» нередко используют в качестве паролей вариации на тему названий спортивных команд, имен чемпионов, а также реальных или вымышленных звезд шоу-бизнеса. Учтя этот факт и увидев, что обитель подозреваемого немного напоминает бейсбольный мемориал, можете начинать перебирать в памяти известные вам названия команд.

- 50% паролей представляют собой имя или фамилию кого-то из членов семьи, партнеров или домашних любимцев. Найти эту информацию очень легко, нужно только знать, где искать. Ценным источником подобных сведений могут выступать поисковики вроде Google или сайты компаний, предоставляющих онлайновые отчеты о кредитных операциях. Как показывает практика, этих пользователей нельзя причислить к категории компьютерных асов. Учитывайте этот фактор, когда вам придется шпионить за пользователем бесплатных почтовых служб, в отличие от клиента, работающего с несколькими компьютерами под управлением Linux, подключенными к одной абонентской линии.
- 11% пользователей были охарактеризованы как «себялюбы», применяющие пароли вроде «sexy», «stud» или «goddess». Ох уж эта гордыня! Вспомните старую поговорку: «Дьявол гордился, да с неба свалился», – в данном случае излишняя гордыня чревата не меньшей опасностью – подобный пароль очень легко взломать, поскольку эти слова короткие и их можно найти в любом словаре (более подробно эту тему мы затронем в нашем следующем разделе).
- Оставшиеся 9% пользователей применяют пароли, к которым хорошо подходит определение «замысловатый». Таковыми можно считать пароли, состоящие из трудно угадываемых последовательностей букв, цифр и символов. Обычно такие пароли выбирают компьютерщики с немалым опытом, особенно в вопросах обеспечения безопасности. Скорее всего, к этой категории принадлежит и тот подозреваемый, о котором мы говорили в нашем примере.

Очевидно, что пользователя не всегда можно четко отнести к той или иной группе, поэтому нельзя быть уверенным в том, что все клиенты бесплатной почтовой службы обязательно выбирают в качестве пароля имя своей второй половины. Однако общий вывод по результатам данного опроса можно сформулировать так: около 90% пользователей используют простые для угадывания пароли. Этот показатель значительно вырос с того времени, когда подобные опросы проводились среди пользователей операционных систем Unix, что свидетельствует об увеличении процента технически неграмотных пользователей, которые к тому же несведущи в вопросах безопасности. А это плохая новость для системных администраторов, но хорошая для шпионов. (Подробности этого социологического исследования опубликованы в сети Интернет по адресу [www.centralnic.com/page.php?id=77](http://www.centralnic.com/page.php?id=77).)

**КАРТОЧНЫЙ ДОМИК ПАРОЛЕЙ.** В те далекие времена, когда пасьянсы раскладывались еще бумажными картами (а это было всего каких-то 20...30 лет назад), иногда игру в карты начинали с постройки карточного домика, аккуратно ставя одну карту на другую и пытаясь сделать его как

можно выше. Это занятие требовало терпения и четко отработанных движений во время постройки пола, стен и крыши. Стоило допустить единственную ошибку, и плоды всех ваших стараний рушились в долю секунды.

## Разоблачения: ФБР против российских взломщиков, часть II

В первой главе книги мы рассказывали вам об операции по захвату двух российских взломщиков, проведенной ФБР (см. врезку «Разоблачения: хороший полицейский или плохой полицейский?»). Эти двое россиян поверили объявлению о приеме на работу, опубликованному фиктивной компанией, специализирующейся в области компьютерной безопасности, и впоследствии были арестованы агентами ФБР. ФБР использовало keylogger для перехвата сведений об именах учетных записей и паролях, необходимых для подключения к компьютерам взломщиков в России (именно этими паролями и воспользовались агенты Федерального Бюро для сбора доказательств).

Один из подозреваемых, Алексей Иванов, вез с собой персональный ноутбук Toshiba. После ареста Иванов дал разрешение одному из агентов на просмотр содержимого компьютера. Ноутбук Иванова был защищен при помощи пароля BIOS. Агентам нужен был пароль, и Иванов сообщил его. (Вы бы удивились, узнав, насколько часто люди, находящиеся под следствием, соглашаются на такие уступки.)

Пароль BIOS выглядел как «FupjyKj[», и любой назвал бы подобный пароль устойчивым, поскольку его длина достигала 8 символов, а выглядел он как случайная последовательность символов. ФБР был также известен псевдонимом Иванова «subbst» и адрес одного из удаленных компьютеров в России, к которому он подключался. Однако им не были известны имя учетной записи и пароль.

Один из ведущих агентов воспользовался службой Telnet для подключения к удаленному компьютеру в России, введя в качестве имени учетной записи «subbst», а в качестве пароля – «FupjyKj[». Пароль оказался верным, и сотруднику Федерального Бюро удалось успешно проникнуть в удаленную систему. Таким образом, несмотря на надежность самого пароля, его неправильное применение привело к крушению всего карточного домика системы безопасности.

Подобная ситуация нередко наблюдается при использовании паролей. Эксперты по безопасности, заботливые начальники и журнальные статьи предупреждают пользователей о необходимости использовать

сложные, трудно угадываемые пароли, устойчивые к ручным и автоматическим методам подбора, забывая об одном маленьком нюансе: уровень безопасности в целом зависит от соблюдения правил применения пароля.

Предположим, что ваш гипотетический подозреваемый в терроризме использует утилиту PGP для шифрования и дешифрования сообщений электронной почты, выбрав при этом достаточно стойкий пароль. Вам же позарез необходимо выяснить содержание отправляемых им сообщений. Вам удалось перехватить его секретный ключ, однако не повезло с паролем. Поэтому вы начали вести мониторинг его подключений к сети Интернет и обнаружили, что подозреваемый использует пароль «D2fitHPoR?» для подключения к одному из онлайновых форумов. Обнаруженные вами документы в формате Word и Excel зашифрованы с использованием не слишком стойкой схемы шифрования, поэтому вы без труда взламываете их с помощью специальных утилит менее чем за секунду (причем пароль, используемый для этих документов, оказался таким же – «D2fitHPoR?»). Сам по себе такой пароль отгадать сложно, но что если он же используется и в утилите PGP? Попробуем! Подставив этот пароль в PGP, вы без труда смогли расшифровать все сообщения подозреваемого и за свои успехи были награждены похвальной грамотой разведчика.

Использование одинаковых паролей в приложениях с различным уровнем безопасности несет в себе потенциальную угрозу. Применение одинаковых паролей – одна из человеческих слабостей, которой вы можете воспользоваться. Рашина Дамия, исследователь из Калифорнийского университета в Беркли, подсчитал, что рядовой пользователь вынужден вводить от 10 до 100 паролей в разных местах, используя при этом от одного до семи различных паролей. Таким образом, когда один пароль становится известен посторонним лицам, часть, а то и весь карточный домик системы безопасности рушится.

## АТАКА ЗАЩИЩЕННЫХ ДАННЫХ

Легче всего атаковать защищенные данные, найдя пароль (написанный на клочке бумажки и приkleенный к компьютерному монитору либо спрятанный в столе). На этом игра заканчивается, поскольку ваша работа оказывается выполненной. Однако, поскольку террористы не столь опрометчивы в своих действиях и способны осложнить вашу жизнь, меняя свои пароли и обновляя версии Microsoft Word, вам придется поискать другие способы раскрытия паролей. Возможные способы приведены ниже (в произвольном порядке):

- судебный ордер (по крайней мере, в Соединенных Штатах);
- шантаж;
- взятки;
- секс;
- наркотики;
- техническое наблюдение (установка «жучков»);

- приемы социотехники;
- пытки (криптоанализ с помощью резинового шланга).

К сожалению, поскольку ваш оперативный бюджет и ресурсы несколько ограничены (и вдобавок данная книга посвящена в большей степени компьютерному шпионажу), в вашем распоряжении остаются четыре классических способа атаки защищенных данных: подбор пароля вручную, автоматический подбор при помощи словаря, взлом посредством «лобовой атаки» или же применение криптоанализа, то есть взлом самого алгоритма шифрования.

**ОТГАДЫВАНИЕ ПАРОЛЯ ВРУЧНУЮ.** Первый метод, который используется большинством людей при подборе пароля, сводится к простому угадыванию – вводу наиболее вероятных паролей. Когда приложение запрашивает у вас пароль, вы вводите предполагаемый пароль на основе имеющихся у вас сведений о пользователе данного компьютера. Логическое угадывание должно базироваться на следующих предсказуемых штампах поведения пользователя:

- **Общее поведение.** Большинство компьютерных пользователей чрезвычайно предсказуемы, когда речь заходит о паролях: они используют в качестве пароля имя учетной записи, слово «password», задают пустой пароль, используют пароль по умолчанию либо повсеместно применяют один и тот же пароль. (Поскольку вы являетесь правительственным агентом, вы, скорее всего, осведомлены в вопросе поведенческих характеристик иностранных пользователей.)
- **Особое поведение.** Если вы собрали информацию о подозреваемом и составили на него или нее досье, вы можете испробовать такие пароли как девичья фамилия супруги, код социального страхования, даты юбилеев или дней рождения, а также любую другую значимую для объекта информацию, которую достаточно легко запомнить. (Классический пример из кино – фильм «Военные игры» (*“War Games”*), снятый в начале 1980-х, в котором Метью Бродерик проникает в компьютер Объединенного командования ПВО североамериканского континента (NORAD), задав в качестве пароля имя умершего сына ученого, Джошуа.)

Угадывание паролей иногда может принести на редкость успешные результаты, а иногда – потребовать значительного количества времени, особенно если вам приходится вводить каждый вариант пароля вручную в диалоговом окне приложения. К тому же некоторые приложения могут блокировать возможность ввода пароля после нескольких неудачных попыток. Если вы не преуспели в угадывании пароля после нескольких попыток или в течение нескольких минут, лучше перейдите к автоматической атаке при помощи словаря (мы поговорим о ней в следующем разделе). Составив досье по интересующему вас объекту, вы можете использовать в программе автоматического подбора пароля список выбранных ключевых слов.

## Тактика: Саддам, вам письмо!

В октябре 2002 г. внештатный корреспондент и специалист по вопросам безопасности Брайан МакУильямс посетил официальный сайт правительства Ирака [www.uruklink.net/iraq](http://www.uruklink.net/iraq). Он обратил внимание на то, что на сайте существует ссылка, щелкнув по которой вы можете отправить письмо президенту Ирака Саддаму Хусейну. Адрес электронной почты имел вид [press@uruklink.net](mailto:press@uruklink.net) (непонятно, то ли ящик назывался таким образом, поскольку предназначался в первую очередь для прессы, то ли его название представляло собой сокращение от «президент Саддам»).

Кроме того, пользователям этого сайта предоставлялась возможность онлайновой проверки своей электронной почты. Полагаясь на классический прием угадывания пароля, он ввел «press» в качестве имени учетной записи и то же самое в качестве пароля. Когда после некоторой паузы Брайен уже хотел было сдаться, перед ним открылась полная сообщений папка «Входящие» данной учетной записи.

В папке хранились сообщения за последние несколько месяцев (начиная с августа 2002 г.). Ни одно сообщение не было прочитано, а почтовый ящик достиг своего максимального размера, не позволяющего принимать новые сообщения. МакУильямс загрузил около 1000 сообщений, адресованных Хусейну. Помимо сообщений спамового характера, угроз или писем от фанатов с просьбами прислать фотографии и автографы, МакУильямс обнаружил предложения о сотрудничестве, поступившие от нескольких американских компаний, которые пытались договориться с Хусейном о продаже товаров или услуг, несмотря на официальный запрет ведения торговых отношений в соответствии с политикой Соединенных Штатов.

Хотя информация об этом инциденте успела быстро распространиться по различным сайтам новостей в Интернете, МакУильямс заявил, что правительство ни разу не обращалось к нему с просьбой о предоставлении загруженных сообщений. Отметив отсутствие интереса со стороны госслужб, он предположил, что одно из американских разведывательных управлений уже взламывало почтовый ящик Хусейна и вело за ним активное наблюдение.

МакУильямс сменил пароль, перед тем как сообщить о своем открытии, вскоре после чего некто [urulink.net](http://urulink.net) повторно изменил пароль. Скорое падение режима Хусейна в апреле 2003 г. не позволило хакерам-добровольцам попрактиковаться во взломе других Иракских сайтов во время войны. Тем не менее помните, что взлом серверов Оси зла хотя и выглядит патристично, но по-прежнему считается незаконным.



Пол Бобби является автором отличной статьи по созданию тематических словарей, предназначенных для взлома пользовательских паролей. Этот процесс включает сбор информации о целевом пользователе с последующим подбором возможных паролей, руководствуясь заданными правилами их изменения. Этот документ вы можете найти в сети Интернет по адресу [rr.sans.org/authentic/cracking.php](http://rr.sans.org/authentic/cracking.php).

**АТАКА ПРИ ПОМОЩИ СЛОВАРЯ.** Наиболее эффективным способом взлома защищенных данных является подбор пароля при помощи словаря, слова из которого последовательно проверяются на соответствие паролю. Такой тип атаки особенно эффективен при разгадывании ненадежных паролей, представляющих собой популярные термины и т. д. Большинство утилит для подбора паролей позволяют задавать один и более файлов со списками слов, предварительно составленных вами или кем-то еще. Программа считывает слово из списка и проверяет, можно ли с его помощью расшифровать данный документ. Если результат положительный, атака считается завершенной и искомый пароль отображается на экране.

В сети Интернет можно обнаружить практически любые словари, включающие общеупотребительные имена, персонажей из научной фантастики, религиозные термины, имена популярных ведущих, названия известных кинофильмов и телевизионных передач. Вы можете найти словарные списки даже на русском, хорватском, немецком, французском или японском языках. Если вы потратили некоторое время на предварительное изучение стиля жизни и поведения вашего объекта, вам должно быть известно, слова из какой области могут выступать в качестве пароля.

Многие утилиты для взлома паролей обладают дополнительными возможностями, например, умеют подставлять варианты слов с первой заглавной буквой, заменять букву «о» на цифру «0» либо добавлять в конец слова символы пунктуации (все это достаточно распространенные приемы, используемые более грамотными компьютерными пользователями для увеличения надежности пароля).

Статистика показывает, что подбор пароля при помощи словаря – наиболее эффективная методика, поскольку, в соответствии с результатами многочисленных опросов, от 50 до 90% компьютерных пользователей используют для защиты важных документов слова, которые можно встретить в словаре.

Обязательно воспользуйтесь методикой подбора паролей с помощью словаря, перед тем как прибегать к другим, более радикальным методам. Но для эффективной атаки с помощью словаря необходимо предварительно подготовиться: разыскать максимальное количество различных словарей, записать их на CD-R или скопировать на раздел жесткого диска (так вы немного ускорите процесс подбора за счет большей скорости поиска и чтения данных с накопителя на жестком диске).

\* В настоящее время статья доступна по адресу [http://www.totse.com/en/hack/hack\\_attack/162116.html](http://www.totse.com/en/hack/hack_attack/162116.html). – Прим. ред.



Сеть Интернет изобилует различными электронными словарями, распространяемыми совершенно бесплатно либо за достаточно символическую цену. Кроме того, несколько свободно распространяемых словарных списков на английском и других языках, пригодных для подбора паролей с их помощью, размещены на сайте компании AccessData ([www.accessdata.com/dictionaries.htm](http://www.accessdata.com/dictionaries.htm)), компании ElcomSoft ([www.elcomsoft.com/prs.html](http://www.elcomsoft.com/prs.html)) и Оксфордского университета (<ftp://ftp.ox.ac.uk/pub/wordlists/>).

**АТАКИ «В ЛОБ».** Если ваша жертва оказалась достаточно умна, и подбор пароля с помощью словаря не увенчался успехом, следующий прием, который вы должны попробовать, заключается в использовании «лобовой» атаки. Речь идет о переборе всех возможных комбинаций букв, цифр, знаков препинания и символов. Алгоритм такой же, как при подборе пароля при помощи словаря, только на этот раз мы будем выбирать не из конкретного списка слов, а проверять все возможные сочетания символов.

Успешность «лобовой» атаки напрямую зависит от длины пароля. Чем длиннее пароль, тем меньше вероятность благоприятного (для вас) исхода. Вообще-то, если длина пароля больше некоторой критической величины, то необходимое для проведения исчерпывающего перебора символов время (с учетом быстродействия современной техники) выходит за разумные пределы, в результате чего взлом пароля методом перебора становится невозможным.

Выполним небольшой математический расчет. Пароль может состоять из комбинации 95 различных символов (128 символов ASCII минус 33 непечатаемых символа, к которым относятся управляемые символы, такие как, например, ASCII 7 – выдача звукового сигнала). Существует также 128 символов из расширенного набора (например, ASCII 142 соответствует символу Ё или букве «О» в кодировке кириллицы). Однако большинство англоязычных пользователей никогда не используют подобные символы (применение их само по себе могло бы служить отличной контрмерой). Кроме того, далеко не все приложения позволяют использовать символы из расширенного набора в качестве пароля.

Итак, предположим, что наш гипотетический террорист использовал пароль длиной в 8 символов в приложении с устойчивым алгоритмом шифрования. Если он выберет только печатаемые символы ASCII, мы будем иметь дело с  $6,6 \times 10^{15}$  уникальных комбинаций. В данном случае полный перебор потребует помощи от нескольких грядущих поколений, поскольку на перебор такого количества паролей при скорости миллиард операций в секунду уйдет более 200 лет. (Конечно, здесь мы не учли Закон Мура, в соответствии с которым количество транзисторов на квадратный сантиметр удваивается каждый год, приводя к дальнейшему увеличению производительности компьютеров, и не приняли в расчет возможность прорыва в технологии криptoанализа.)

Теперь попробуем предположить, что наш террорист не соблюдал политику безопасности и воспользовался паролем из 5 символов, представляющим

собой произвольное сочетание любых из 95 различных символов. Тогда количество уникальных комбинаций уменьшится до  $7,7 \times 10^9$ , что при той же скорости (миллион комбинаций в секунду) потребует максимум двух часов для перебора всех возможных комбинаций.

## Тактика: чем больше, тем лучше

Очевидно, что при выполнении «лобовой» атаки на отдельном компьютере существуют определенные временные ограничения. Однако что произойдет, если вы воспользуетесь несколькими компьютерами для взлома пароля? Этот подход называют «распределенной атакой», в которой участвуют сразу несколько компьютеров, каждый из которых работает только со своим диапазоном вариантов паролей или ключей.

До конца 1990-х стандарт шифрования данных DES (Data Encryption Standard) считался золотым стандартом шифрования информации, но, несмотря на стойкость алгоритма, возникали сомнения в его надежности при применении «лобовой» атаки из-за постоянно растущей вычислительной мощности компьютеров. (До этого, в течение достаточно долгого времени ходили слухи о том, что Управление национальной безопасности располагало компьютерами, достаточными для взлома информации, зашифрованной при помощи DES.)

В январе 1997 года компания RSA объявила для всех желающих конкурс по взлому данных, зашифрованных при помощи алгоритма DES, с различными денежными призами, в зависимости от использованной длины ключа. Так, например, приз в 1000 долларов получил исследователь из Беркли, Калифорнийского университета, который за 3,5 часа взломал экспортную версию DES с 40-битовым ключом, воспользовавшись для этого 250 компьютерами студенческого кампуса. Следующий конкурс оказался на порядок сложнее: на этот раз добровольцам предстояло взломать 56-битовый ключ, и первому, кому это удастся, было обещано вознаграждение в 10 000 долларов. (Напоминаем, что при увеличении длины ключа на один бит количество возможных комбинаций возрастает вдвое.)

Рок Версер, Мэт Кэртен и Джастин Долск организовали проект под названием DESCHALL, для реализации которого было решено задействовать компьютеры, подключенные к Интернету. Предстояло проверить 256 ключей (т. е. 72 057 594 037 927 936), для чего было написано специальное программное обеспечение под различные операционные системы и аппаратные платформы, позволяющее подключаться к центральному серверу, загружать часть ключей, среди которых должен производиться поиск, а затем сообщать о результатах на сервер.

Одновременно стартовали аналогичные проекты других групп, однако наибольшее количество участников собрал именно проект DESCHALL. В качестве участников проекта зарегистрировались более 78 000 IP-адресов. В один из 24-часовых периодов была отмечена одновременная работа более 14 000 компьютеров. Наконец, 17 июня 1997 года, после перебора 24,6% от общего количества возможных ключей (что составило около 18 000 000 000 000), спустя 96 дней с начала операции был найден искомый ключ. (Подробности данного проекта можно найти на сайте [www.interhack.net/pubs/des-key-crack/](http://www.interhack.net/pubs/des-key-crack/).)

Проект DESCHALL дал толчок развитию других проектов «распределенного» взлома ключей. Основной целью подобных проектов является демонстрация сильных и слабых сторон различных алгоритмов шифрования в случае применения «лобовой» атаки (существуют и другие проекты распределенных вычислений, не связанные с темой криптографии, например, проект SETI@home по поиску внеземных цивилизаций или проект Folding@home, изучающий свертываемость протеина и связанные с этим болезни).

Если вы полагаете, что ваш процессор иногда работает вхолостую, и вы хотите принять участие в подобных хакерских проектах, зайдите на сайт distributed.net, который в настоящее время спонсирует проект по взлому 72-битового ключа алгоритма RC5. В отличие от попыток с ключами меньшей длины, скорее всего, этот проект займет больше времени.

В ходе «лобовой» атаки необходимо учитывать закон «убывающего плодородия» для доступных компьютерных ресурсов. Это правило действует в любой ситуации, работает ли вы с суперкомпьютером Управления национальной безопасности или отдельным ПК. При достижении определенной длины пароля или ключа разгадывание его становится бессмысленным, поскольку для этого может потребоваться больше времени, чем вы в состоянии себе позволить. Вы можете и не знать действительную длину пароля, однако вы должны установить для себя максимальный порог, по достижении которого следует прекратить перебор, основываясь на имеющихся в вашем распоряжении компьютерных ресурсах и времени, которое вы можете посвятить взлому пароля.

Необходимо также сделать правильную оценку важности информации. Стоит ли тратить целые месяцы на ее разгадку? Не потеряет ли информация к тому моменту свою ценность? Допустим, вы перехватили зашифрованное сообщение от поставщика наркотиков к его наркодиллеру, и его взлом занял у вас полгода, в результате чего выяснилось, что в нем шла речь о поставках, которые должны были произойти через неделю после перехвата сообщения. Оправданы ли в данном случае затраты времени и ресурсов на взлом этого сообщения? (Мы полагаем, что наши преступники

достаточно умны и регулярно меняют пароли, поэтому раскрытие этого пароля не позволит читать через полгода другие сообщения.)

**КРИПТОАНАЛИЗ.** Криptoанализом называют изучение алгоритмов шифрования и криптосистем (систем, предназначенных для шифрования и дешифрования информации). Криptoанализ применяется с целью извлечения из зашифрованного текста исходного сообщения (незашифрованной информации). Его можно называть наукой и искусством одновременно, ведь специалисты-практики криptoанализа используют для разрешения криптографических проблем не только строгую математику, но и привлекают себе в помощники любопытство, интуицию, упорство и везение.

Людей, занимающихся взломом кодов и шифров, можно поделить на две группы:

- **Правительство.** Управление национальной безопасности (NSA – National Security Agency) держит в своем штате больше математиков и криптографов, чем любое другое правительственное управление либо частная корпорация (NSA также является крупнейшим покупателем компьютерного оборудования в мире). Часть профессионалов криptoанализа работает также на военных, другие разведывательные управления и правоохранительные организации. Практически все работы и исследования по криптографии (за исключением деятельности Национального института стандартизации и технологии) являются засекреченными.
- **Ученые и компании.** До недавних пор криптография относилась к монополии государства, которое контролировало работу всех криптографов. Однако со временем влияние государства значительно уменьшилось, и в то же время вырос интерес к криптографии со стороны математиков (относящихся к научному сообществу), и увеличилась потребность в специалистах по криптографии со стороны частных предприятий, в особенности тех, чья деятельность связана с финансами, средствами связи или же обеспечением компьютерной безопасности. Новое поколение криптографов действует более открыто в своей работе, организовывая презентации и публикуя документы об обнаруженных в различных алгоритмах шифрования изъянах. Иногда после публикации информации об обнаруженных ошибках программисты, которые даже не являются специалистами по криптографии, берутся за написание программных утилит, позволяющих использовать найденные бреши в защите систем. Классический пример – протокол безопасности 802.11b Wired Equivalent Privacy. Вскоре после того, как увидели свет результаты научного исследования, описывающие уязвимые места протокола, на просторах виртуальной сети Интернет появились несколько утилит, позволяющих расшифровывать ключи WEP. Хотя многим программистам не достает навыков программирования или опыта для обнаружения изъянов в алгоритмах

шифрования, но зато они всегда могут трансформировать теоретические концепции в реальные утилиты (если эти изъяны были обнаружены кем-то другим).

Мы не станем слишком углубляться в работу криptoаналитиков и способы получения доступа к зашифрованным данным, поскольку это выходит за рамки данной книги, тем не менее советуем вам принять во внимание следующие важные моменты:

- Криptoанализ требует наличия соответствующих знаний (особенно по математике) и опыта, которые редко присущи рядовому хакеру или шпиону.
- Существуют профессионалы, которым либо платят за поиск уязвимых мест в алгоритмах шифрования, либо они занимаются этим из собственного любопытства. Результаты их работы иногда приводят к компрометации даже считавшихся надежными криптосистем.
- Хотя в наши дни появляется все больше талантливых криптографов (не работающих в госструктурах), которые умеют делать обоснованные прогнозы о возможностях Национального управления безопасности и других агентств, занимающихся взломом кодов, никогда не недооценивайте возможностей государственных управлений. В распоряжении правительства имеются грандиозные ресурсы, которые позволяют ему, по крайней мере, на несколько лет опережать научных деятелей и частный сектор по вопросам криптографии.
- Постоянные исследования и возрастающая процессорная мощность превращают криптосистемы, которые раньше считались стойкими, в весьма ненадежных сердечников, поэтому вам необходимо непрерывно следить за печатными и онлайновыми новостями по безопасности, чтобы находиться в курсе текущих событий. Однако не стоит сразу впадать в панику, едва завидев заголовок об обнаружении очередной ошибки в том или ином алгоритме шифрования. Хотя такая ошибка, с точки зрения научного исследователя, и может существовать, однако опасность не столь высока, как могло бы показаться, поскольку нужно еще уметь эффективно воспользоваться обнаруженной брешью.



В Интернете имеется масса информационных источников, посвященных теме криptoанализа. Советуем вам для начала прочесть «Часто задаваемые вопросы о сегодняшней ситуации в мире криптографии», размещенные на сайте лабораторий RSA ([rsasecurity.com/rsalabs/faq/](http://rsasecurity.com/rsalabs/faq/)), изучить «Основы криptoанализа» по «Армейскому руководству по обслуживанию в полевых условиях 34-40-2» ([www.fas.org/irp/doddir/army/fm34-40-2/](http://www.fas.org/irp/doddir/army/fm34-40-2/)) и пройти «Курс самостоятельного обучения криptoанализу блочных шифров» ([www.counterpane.com/cryptanalysis.pdf](http://www.counterpane.com/cryptanalysis.pdf)).

## Утилиты взломщика

Итак, вы сидите над зашифрованными документами, которые вам удастся скопировать с компьютера человека, подозреваемого в терроризме, и вам известно о существовании утилит, которые могут помочь получить доступ к исходной информации. Ваша бабушка, занимавшаяся взломом закодированных сообщений во время Второй мировой, рассказывала истории о математиках и других мастерах дешифровки, использовавших бумагу, ручку и примитивные компьютеры для взлома зашифрованных сообщений. Однако сегодня вам даже не нужно быть профессиональным криптоаналитиком, чтобы взломать один из распространенных видов защищенных документов. Далее мы рассмотрим некоторые коммерческие и свободно распространяемые утилиты, которые отличаются простотой использования и позволяют легко обходить защиту зашифрованных файлов.

### ПРИЛОЖЕНИЯ ДЛЯ ВЗЛОМА ПАРОЛЕЙ

Утилиты для взлома паролей занимают на рынке свою, довольно специфическую нишу, причем существует немало компаний, специализирующихся на написании приложений для взлома паролей. Обычно это делается путем инженерного анализа исходного кода программы, создающей зашифрованные документы, в ходе которого изучается используемый в программе алгоритм шифрования. На основе этой информации программист может написать утилиту, которая либо будет непосредственно пользоваться нестойкостью алгоритма шифрования и извлекать пароль, либо применять алгоритмы подбора паролей «в лоб» или с помощью словаря.

Почти для всех популярных приложений, в которых для защиты документов используются пароли, существуют утилиты от сторонних разработчиков, позволяющие взламывать зашифрованные этими приложениями документы. В зависимости от применяемого метода шифрования, иногда пароль может быть раскрыт немедленно, а иногда это может занять несколько недель. Чтобы вы оценили, насколько легко можно получить доступ к защищенным документам, ниже приводится список типов файлов, для которых компанией ElcomSoft, одним из лидеров по восстановлению паролей, предлагается программное обеспечение для взлома зашифрованных документов:

- Adobe Acrobat: файлы PDF.
- Архиваторы: файлы ZIP, RAR, ACE и ARJ.
- Продукты компании Corel: WordPerfect, QuattroPro и Paradox.
- Почтовые клиенты: Microsoft Internet Mail and News, Eudora, TheBat!, Netscape Navigator/Communicator Mail, Pegasus, Calypso, FoxMail, Phoenix Mail, Incredimail, @nyMail и QuickMail Pro.

- Службы мгновенных сообщений: ICQ, Yahoo, AOL AIM, MSN Messenger, Excite Messenger, Odigo, Trillian, AT&T IM Anywhere, T-Online Messenger, Match Messenger, Praize IM, ScreenFIRE, ACD Express Communicator, Imici Messenger, Prodigy IM, PowWow Messenger, Jabber IM, Kellster IM, PalTalk, Indiatimes Messenger, Miranda и Tiscali.
- Продукты компании Intuit: Quicken, Quicken Lawyer и QuickBooks.
- Продукты компании Lotus: SmartSuite, Organizer, WordPro, 1-2-3 и Approach.
- Продукты компании Microsoft: Office, Access, Excel, Outlook, Word, Excel, Outlook Express, Internet Explorer, Project, Money, Backup и Visual Basic для приложений.
- Symantec ACT!

Если вы далеки от шпионажа, вас может смутить этическая сторона дела: допустимо ли, чтобы компании выпускали программное обеспечение для взлома документов, созданных в других приложениях. Вдохните глубже, успокойтесь и вспомните, что, как любая другая технология, взлом паролей может осуществляться как на законных, так и незаконных основаниях. Законными основаниями можно считать необходимость восстановления ваших собственных защищенных документов, пароль к которым был потерян, запорчен либо забыт. Кроме того, взлом паролей может понадобиться в ходе полицейского расследования и поиска доказательств (правоохранительные организации являются главным покупателем подобного программного обеспечения).

Основное правило эффективности приложений для взлома паролей таково: чем быстрее работает процессор, тем быстрее будет найден искомый пароль при атаке «в лоб» или при помощи словаря. Вполне логично, если учесть, что количество перебираемых в секунду вариантов пароля напрямую зависит от тактовой частоты процессора. Чем выше частота, тем быстрее осуществляется перебор.

Большинство утилит для подбора паролей могут выполняться в фоновом режиме, пока вы работаете с другими приложениями. Однако чем больше параллельных процессов выполняются в системе и чем больше нагружают процессор другие приложения, тем медленнее выполняется подбор паролей. Некоторые приложения для подбора паролей позволяют задавать приоритет процесса, чтобы максимально использовать вычислительную мощность процессора, но лучше всего выделить для работы подобных утилит отдельный компьютер или даже несколько компьютеров.

Компании по производству программного обеспечения для взлома паролей часто выпускают обновления к своим программным продуктам, увеличивая скорость и эффективность их выполнения, а также добавляя поддержку новых методов защиты и шифрования, используемых производителями ПО. Помимо компаний по производству программного обеспечения для восстановления паролей, существуют даже специальные

службы, предоставляющие услуги по расшифровке документов. Большинство коммерческих утилит для восстановления утерянных паролей стоят не так уж дорого, поэтому подумайте над вложением денег в их приобретение: такие программы хорошо всегда иметь под рукой.

В следующих параграфах мы расскажем об основных компаниях, занимающихся выпуском коммерческих приложений для восстановления паролей.

## Инструментарий: оборудование для взлома паролей

Правительственные организации либо хорошо спонсируемые шпионские группировки могут позволить себе еще один прием «лобовой» атаки, заключающийся в использовании специального аппаратного обеспечения, предназначенного для взлома зашифрованных данных.

Хотя специализированное аппаратное обеспечение для взлома является экзотикой, и казалось, что позволить его себе может только Управление национальной безопасности, в 1998 году организация EFF (Electronic Frontier Foundation) собрала компьютер, предназначенный для взлома данных, зашифрованных с помощью алгоритма DES. Компьютер состоял из 1500 микросхем, каждая из которых, в свою очередь, состояла из 24 идентичных модулей поиска, способных проверять 2 500 000 ключей в секунду. Таким образом, суммарные возможности этого компьютера составляли 90 000 000 000 комбинаций в секунду, что требовало всего около 9 дней на перебор всех возможных комбинаций (всего пространства ключей).

В ходе официальной презентации ЭВМ смогла взломать сообщение, зашифрованное при помощи 56-битового ключа, менее чем за 56 часов (предыдущий рекорд, полученный методом распределенной атаки, составил 39 дней). В конце концов, и этот рекорд был побит при использовании специального аппаратного обеспечения в сочетании с методикой распределенных вычислений. Скорость перебора в этом случае составила 245 000 000 000 ключей в секунду, в результате чего нужный ключ был найден через 22 часа. (Подробное описание этого суперкомпьютера для взлома ключей алгоритма DES, включая фотографии, вы можете найти на веб-сайте [www.cryptography.com/resources/whitepapers/DES.html](http://www.cryptography.com/resources/whitepapers/DES.html).)

Подумайте сами: если бесприбыльная адвокатская группа смогла собрать пусть низкотехнологичное, но достаточно эффективное аппаратное обеспечение для взлома ключей стоимостью менее \$250 000, то, скорее всего, подобное оборудование имеется и в распоряжении правительства.

Возникает следующий вопрос: может ли специализированное аппаратное обеспечение справиться с более устойчивыми криптосистемами, такими как AES (Advanced Encryption Standard), в которой используется 128-битовый ключ? Предположим, вам удалось собрать достаточно распределенных ресурсов, чтобы взламывать 56-битовый ключ DES в течение секунды. Но даже такому мощному суперкомпьютеру понадобится около 149 000 000 000 000 лет, чтобы перебрать все возможные комбинации 128-битовых ключей AES. А это, согласитесь, немало, особенно если учесть, что возраст нашей Вселенной большинством ученых оценивается приблизительно в 20 000 000 000 лет.

**ACCESSDATA.** Компания AccessData, основанная в 1987 году, является одним из пионеров отрасли восстановления утерянных паролей. Компания предоставляла консалтинговые услуги и программное обеспечение правительству США, местным и федеральным управлению правоохранительных органов, оказав в результате помочь многим американским компаниям. За это время компания AccessData завоевала доверие у своих клиентов. Стоимость отдельных утилит восстановления утерянных паролей для многих популярных приложений составляет от \$35 до \$99, кроме того, можно приобрести полный пакет всех выпущенных модулей под названием Password Recovery Toolkit всего за \$495.

Компания AccessData также выпустила продукт под названием Distributed Network Attack (DNA), предназначенный для распределенной атаки защищенных документов Microsoft Office 97/2000 и файлов .PDF. DNA состоит из центрального сервера и некоторого числа сетевых клиентов, каждый из которых отвечает за поиск пароля в своем подмножестве, уменьшая таким образом общее время, необходимое для перебора всех возможных вариантов. Версия с десятью сетевыми клиентами стоит \$249, а с поддержкой сотни клиентов – \$995.

Если вы хотите подробнее узнать о выпускаемых компанией продуктах или загрузить демонстрационную версию пакета Password Recovery Toolkit, посетите ее официальный сайт по адресу [www.accessdata.com](http://www.accessdata.com).

**ELCOMSOFT.** Российская компания ElcomSoft, успевшая приобрести скандальную славу, также специализируется на выпуске программного обеспечения для восстановления утерянных паролей. Первая выпущенная компанией в 1997 году утилита предназначалась для подбора паролей к защищенным архивам в формате ZIP, с тех пор компания успела выпустить множество различных утилит для взлома паролей для большинства популярных приложений. Стоимость отдельных утилит составляет от \$30 до \$70 за однопользовательскую лицензию.

Компания ElcomSoft приобрела широкую известность в кругах, связанных с компьютерной безопасностью и защитой авторских прав на электронную собственность, летом 2001 года, когда сотрудник компании Дмитрий Скляров был арестован в Лас-Вегасе на конференции хакеров

после проведенной им демонстрации нестойкости алгоритма шифрования, используемого компанией Adobe для защиты электронных книг. Скляров являлся автором программы, выпущенной компанией ElcomSoft, которая позволяла расшифровывать электронные книги Adobe, в результате чего компания Adobe потребовала ареста Склярова по обвинению в нарушении Закона по защите авторских прав на цифровую интеллектуальную собственность (DMCA – Digital Millennium Copyright Act).

Скляров провел в заключении несколько недель, пока за него не был внесен залог в размере \$50 000, после чего, в конце концов, ему разрешили вернуться в Россию. (Александр Каталов, президент компании ElcomSoft, бывший сотрудник КГБ, позднее обратил внимание на пикантность ситуации, связанной с арестом Склярова агентами ФБР, ведь Федеральное Бюро являлось одним из покупателей продукции компании.) Хотя со Склярова и были сняты все обвинения, правительство решило предъявить те же обвинения компании ElcomSoft в целом, однако жюри присяжных признало ее невиновной в декабре 2002 года. (Компания Adobe, ставшая главным инициатором разбирательства, тихо ушла со сцены в тот самый момент, когда нескольких групп активистов начали угрожать бойкотом программных продуктов компании.)

Образцово-показательное применение Закона по защите авторских прав на цифровую интеллектуальную собственность к компании ElcomSoft не помешало ей продолжить выпуск других инновационных утилит для восстановления паролей. Демонстрационные версии программ и подробную информацию о компании вы можете найти в сети Интернет по адресу [www.elcomsoft.com](http://www.elcomsoft.com).

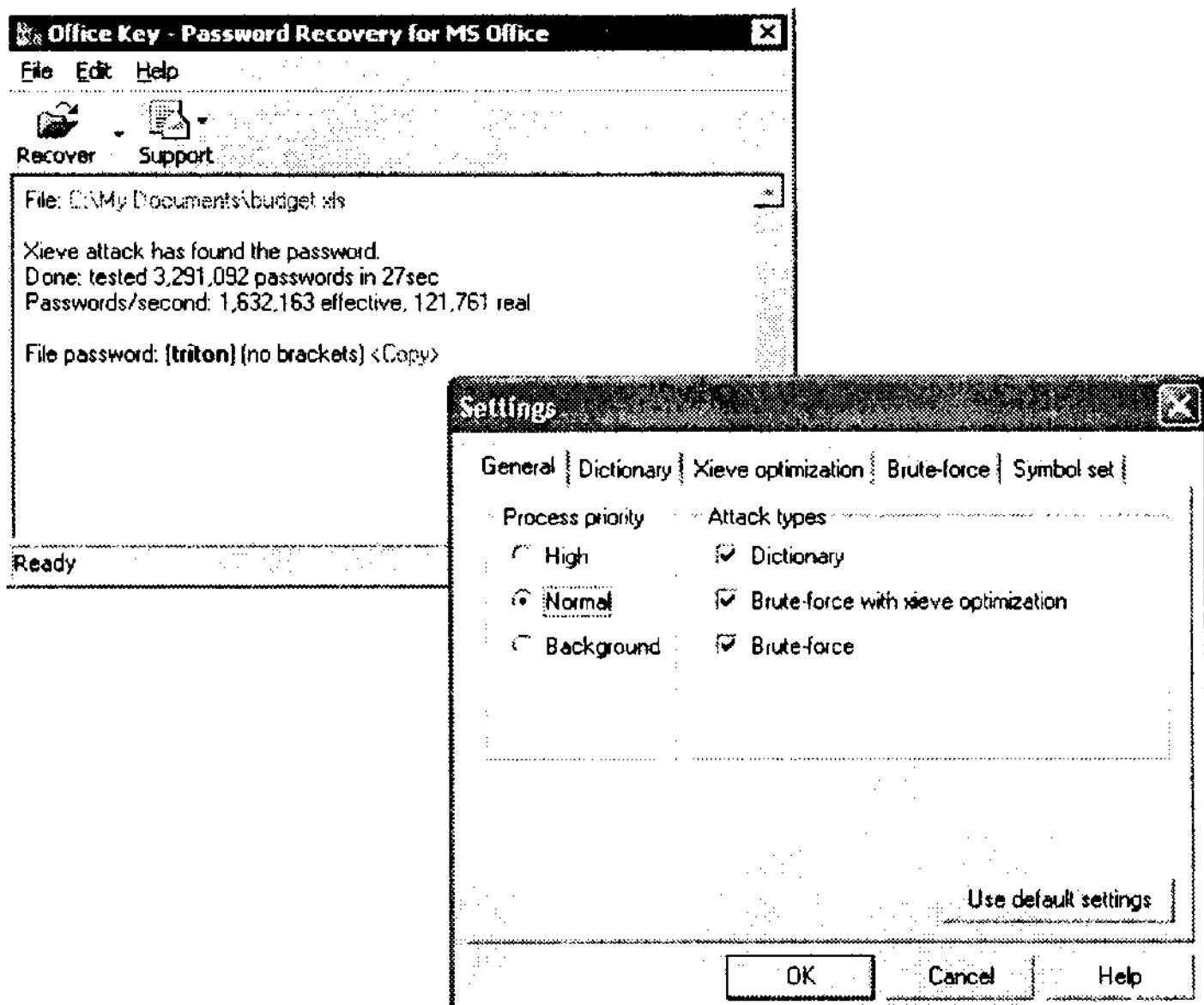
**PASSWARE.** Passware – это еще одна европейская компания, которая быстро вышла на рынок производителей программ для взлома паролей. Основанная в 1998 году в Эстонии (на территории бывшего Советского Союза можно найти немало хороших программистов, которым нравится работать в сфере компьютерной безопасности), эта компания предлагает программные утилиты для взлома паролей для многих популярных приложений по цене от \$45 до \$195 за отдельную программу либо \$395 за полный набор утилит под названием Passware Kit. Одна из таких программ показана на рис. 6.1. Детальную информацию и демонстрационные версии ПО можно найти по адресу [www.lostpassword.com](http://www.lostpassword.com).

**ДРУГИЕ УТИЛИТЫ ДЛЯ ВЗЛОМА ПАРОЛЕЙ.** Кроме программного обеспечения, производимого тремя вышеупомянутыми компаниями, можно найти немало других коммерческих и свободно распространяемых утилит, позволяющих взламывать зашифрованные с помощью паролей документы. Причем многие из бесплатных утилит не менее эффективны в плане взлома паролей, чем их коммерческие аналоги. Советуем вам посетить следующие общедоступные ресурсы:

- Одним из лучших и наиболее полным источником утилит для взлома паролей является сайт «Российских взломщиков паролей», поддерживаемый Павлом Семяновым. Здесь находится

обширный список свободно распространяемых и коммерческих программ, предназначенных для взлома паролей, который содержит краткие описания и комментарии касательно эффективности тех или иных приложений. Адрес сайта в Интернете: [www.password-crackers.com](http://www.password-crackers.com).

- Еще один отличный информационный ресурс по взлому паролей, нестойким алгоритмам шифрования и другим темам, связанным с безопасностью, – веб-сайт Джо Пещела «D.O.E. SysWork», размещенный по адресу <http://members.aol.com/jpeschel/>.
- И наконец, огромное количество свободно распространяемых утилит для различных операционных систем и приложений вы можете загрузить с посвященного безопасности многоуважаемого сайта компании Packetstorm по адресу [www.packetstormsecurity.org/assess.html](http://www.packetstormsecurity.org/assess.html).



**Рис. 6.1.** Утилита от компании Passware, предназначенная для взлома защищенных документов, созданных в предыдущих версиях Microsoft Word (95). Для нашего сценария с террористом, который мы рассматривали в начале главы, искомый пароль анализируемого файла – triton. Защищенные документы, созданные в последних версиях Word, требуют больше времени на взлом, однако по-прежнему являются уязвимыми. Описание алгоритма, используемого компанией Microsoft для шифрования документов, вы можете найти на сайте <http://support.microsoft.com/default.aspx?scid=KB;en-us;q290112>.

## ВЗЛОМ ХРАНИЛИЩА ПАРОЛЕЙ (.PWL) В WINDOWS 3.X, 9X, ME

Как мы уже говорили в главе 4, семейство операционных систем Windows 3.x, 9x и Me не предоставляет защиты от несанкционированного входа в систему. Диалоговое окно входа в систему не ограничивает доступ к компьютеру, поскольку при нажатии кнопки Cancel все равно происходит загрузка Windows, после чего вы получаете полный доступ к файлам на жестком диске.

Окно входа в систему только лишь персонализирует настройки Рабочего стола определенного пользователя и восстанавливает сетевые подключения к разделяемым ресурсам (папкам, принтерам и т. д.). Для упрощения процедуры установки сетевых подключений все сетевые пароли хранятся в файле с расширением .PWL, который расшифровывается при помощи пароля, введенного пользователем при входе в систему.

Главная цель взлома файлов профилей – раскрытие всех используемых паролей на тот случай, если они используются где-либо еще. Поэтому советуем вам скопировать все файлы .PWL с ноутбука нашего подозреваемого в терроризме и затем, добравшись до безопасного убежища, заняться расшифровкой хранящихся в них паролей.

Поскольку в различных версиях операционной системы Windows используются различные схемы шифрования, пожалуй, стоит провести краткий исторический экскурс.

- В Windows for Workgroups и Windows 95 использовалась очень ненадежная реализация алгоритма шифрования RC4, который легко может быть взломан при помощи таких простеньких утилит, как Glide.
- Microsoft исправила данную ошибку системы безопасности в Windows 95 OSR2 и последующих версиях своей операционной системы – Windows 98 и Me. Утилиты первого поколения для расшифровки файлов PWL вроде Glide и ей подобных не умеют восстанавливать пароли, используемые в более поздних версиях ОС Windows. Тем не менее для взлома этих версий файлов .PWL существуют два других способа. Во-первых, все хранимые в файле .PWL пароли кэшируются в память в виде простого текста. Если работающий компьютер был оставлен без присмотра, вы можете запустить утилиту вроде PWLView для просмотра всех существующих паролей. Если компьютер находится в выключенном состоянии, просто загрузите его с дисков и скопируйте все файлы с расширением .PWL на гибкий диск. Затем, возвратившись в офис, вы сможете воспользоваться такими утилитами, как PWLHack или PWLTool, для извлечения паролей.

Утилиты, предназначенные для расшифровки файлов .PWL, можно найти на многих сайтах, посвященных теме безопасности, а также хакерских веб-узлах. Наиболее популярные утилиты можно найти в сети Интернет по таким адресам:

- **Glide:** свободно распространяемая утилита, которую можно загрузить по адресу [members.aol.com/jpeschel/Glidepw1.zip](http://members.aol.com/jpeschel/Glidepw1.zip).
- **PWLView:** бесплатная утилита, доступная на сайте <http://lastbit.com/vitas/pwlview.asp>.
- **PWLTool:** утилита стоимостью \$40, демоверсию которой можно загрузить с сайта <http://lastbit.com/vitas/pwltool.asp>.
- **PWLHack:** свободно распространяемая программа, размещенная в Интернете по адресу [www.pilaos.org.ua/wisdom/download/pwlhack/pwl\\_h410.rar](http://www.pilaos.org.ua/wisdom/download/pwlhack/pwl_h410.rar)\*.

## УТИЛИТЫ ВЗЛОМА ПАРОЛЕЙ В ДИАЛОГОВЫХ ОКНАХ

Еще один способ взлома паролей, уместный в ряде ситуаций, сводится к использованию программного «рентгена» для некоторых диалоговых окон. Так, например, в диалоговых окнах входа в систему Windows вводимый пароль заменяется на экране символами звездочки (\*). Это сделано для того, чтобы пароль не могли подсмотреть находящиеся рядом с вами люди (заглядывая через плечо).

Для реализации данной функции в приложении программисты задают у элемента управления в качестве стиля редактирования `ES_PASSWORD`, в результате чего любой вводимый в данном элементе управления текст будет отображаться в виде символов звездочки. Однако, поскольку «реальный» текст все равно присутствует в памяти, его можно извлечь оттуда, обратившись к дескриптору элемента управления (по ссылке на область памяти).

Подобный прием используется во многих приложениях, использующих пароли для защиты данных. Например, популярная программа `WS_FTP` позволяет пользователям сохранять пароли учетных записей FTP, для того чтобы не требовать их ввода каждый раз при входе в систему; в диалоговом окне отображается имя компьютера, учетной записи и пароль (выводимый в виде звездочек).

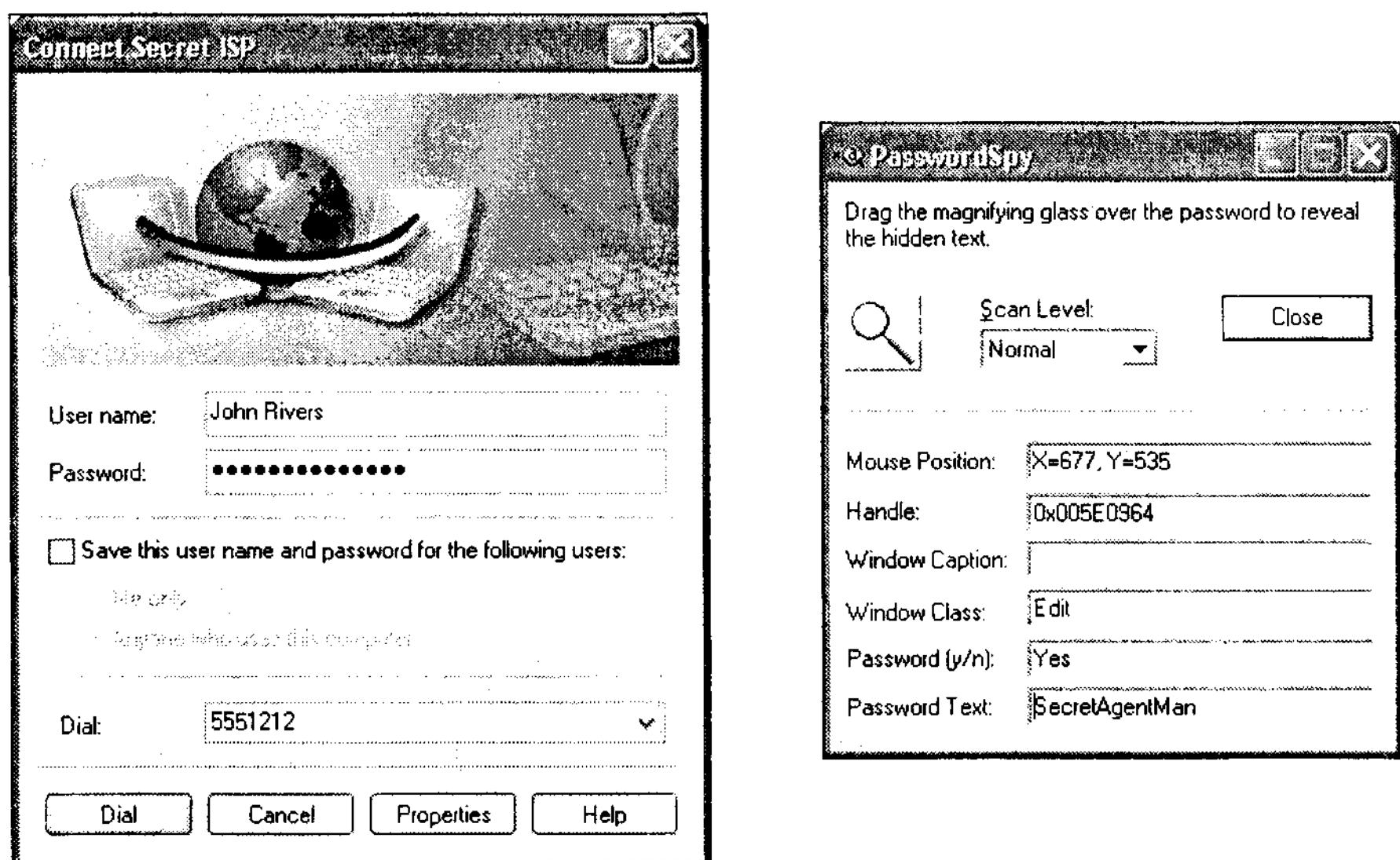
Подобно Супермену с его рентгеновским зрением, свободно распространяемые утилиты, такие как `Revelation` и `Snitch`, умеют «видеть» реальный текст и показывать нам, что скрывается под символами звездочки. Вам достаточно запустить эту утилиту, подвести курсор к полю с паролем, заполненному звездочками, и перед вами появится сам пароль.

В Windows 2000 и XP способ работы с этими элементами управления изменился, поэтому многие утилиты, хорошо зарекомендовавшие себя в предыдущих версиях Windows, оказались бессильны в новых версиях операционной системы от Microsoft. Приведем в качестве примера две

\* Утилита доступна также по адресу <http://www.madalf.ru/pwls.shtml>. –  
Прим. ред.

утилиты, которые позволяют раскрывать пароли во всех версиях Windows: это коммерческая программа под названием iOpus Password Recovery XP и свободно распространяемая по принципу открытого кода утилита PasswordSpy, показанная на рис. 6.2.

Взлом диалоговых окон, содержащих пароли, работает, увы, не для всех приложений (некоторым разработчикам приложений известно о подобной уязвимости, поэтому они включают в свои программы защитный код), но в тех случаях, когда такой способ взлома возможен, он является наилучшим.



**Рис. 6.2.** Утилита PasswordSpy в действии. Взламываем пароль подключения удаленного доступа в Windows XP

Ниже приводится список наиболее популярных утилит для взлома паролей в диалоговых окнах с указанием адресов в сети Интернет, откуда вы сможете их загрузить:

- **Revelation:** свободно распространяемая утилита, размещена на сайте [www.snadboy.com](http://www.snadboy.com);
- **Snitch:** свободно распространяемая утилита, размещена на сайте <http://ntsecurity.nu/toolbox/snitch/>;
- **iOpus Password Recovery XP:** коммерческая программа стоимостью \$29,95, демонстрационную версию которой вы можете загрузить с веб-узла [www.iopus.com/password\\_recovery.htm](http://www.iopus.com/password_recovery.htm);
- **PasswordSpy:** бесплатная утилита, распространяемая по принципу открытого кода. Программу и ее исходные коды можно загрузить по адресу [www.csc.calpoly.edu/~bfriesen/software/pwdspy.shtml](http://www.csc.calpoly.edu/~bfriesen/software/pwdspy.shtml).

## РАСШИФРОВКА ПАРОЛЯ ДЛЯ УДАЛЕННОГО СОЕДИНЕНИЯ

Еще одним слабым местом является пароль, задаваемый для подключений удаленного доступа. Эта служба позволяет пользователям модема легко настраивать учетные записи для подключения к сети Интернет через предоставляющих соответствующие услуги провайдеров и другие онлайновые службы. Одна из очень удобных функций диалога установки подключения удаленного доступа заключается в возможности сохранения пароля, чтобы вам не приходилось набирать его каждый раз вручную. Этот диалог особенно ненадежен в плане безопасности в операционных системах Windows 9x/Me, и вы можете найти в Интернете немало утилит командной строки, позволяющих взламывать зашифрованные сведения об учетной записи и пароле пользователя (поскольку для их шифрования применяются нестойкие алгоритмы). Приведем ссылки на некоторые свободно распространяемые утилиты:

- **Dialpwd:** [www.password-crackers.com/DOWNLOAD/dialpwd.zip](http://www.password-crackers.com/DOWNLOAD/dialpwd.zip),
- **PhoneBook Viewer v1.01c:** [www.password-crackers.com/DOWNLOAD/phbv101c.zip](http://www.password-crackers.com/DOWNLOAD/phbv101c.zip).

## ВЗЛОМ КРИПТОСИСТЕМ

Взлом защищенных документов, созданных при помощи различных приложений, как правило, не требует много времени, однако что если ваша цель – стойкие криптосистемы? Если только вы не являетесь патологическим везунчиком, вам придется туда при попытке взлома защищенных с их помощью данных. Современные криптосистемы, такие как PGP или Blowfish Advanced CS (и прочие утилиты, описанные в разделе «Контрмеры» главы 5), довольно устойчивы к атакам подобного рода по сравнению с приложениями, использующими ненадежные алгоритмы шифрования.

Но даже если в приложении используется устойчивый алгоритм шифрования, ключи имеют достаточную длину и произвести «лобовую» атаку путем перебора всех возможных комбинаций ключей практически невозможно, иногда оказывается эффективной ограниченная «лобовая» атака или атака с помощью словаря, если у пользователя ненадежный пароль. Существуют программы, позволяющие выполнять подбор паролей из словаря либо «лобовые» атаки, однако пользоваться ими не так просто, как, например, утилитами восстановления утерянных паролей для защищенных документов. Если вы достаточно подкованы в техническом плане, то, скорее всего, вы придете к необходимости написания собственной утилиты, в зависимости от алгоритма шифрования, используемого для защиты информации. (Либо, как в нашем гипотетическом примере с правительственным шпионом, вы можете передать данные на анализ группе технических специалистов.)

Дополнительная сложность при взломе защищенных данных сводится к тому, что вы не всегда знаете, какой алгоритм использовался при шифровании данных. Хотя некоторые приложения, такие как PGP,

оставляют заголовки в зашифрованных сообщениях, другие криптоисистемы могут не оставлять вам никаких зацепок. Незнание алгоритма, использовавшегося при шифровании (будь то IDEA, 3DES, Blowfish или любой другой из существующих алгоритмов), – серьезная помеха для начала словарной либо «лобовой» атаки. Поэтому никогда не упускайте случая предварительно проанализировать содержимое жесткого диска на предмет наличия на нем тех или иных утилит шифрования. Располагая этой информацией и воспользовавшись услугами поискового сервера, вы всегда можете найти информацию по уязвимым местам того или иного алгоритма и, если повезет, даже утилиты для взлома защищенной с его помощью информации.

Хорошая новость для вас, как для шпиона, состоит в том, что защита информации при помощи достаточно стойких алгоритмов шифрования встречается нечасто. В случае, когда вы все-таки столкнулись с защищенными таким образом данными, попробуйте прибегнуть к другим методам. Иногда намного проще установить программу keylogger, камеру наблюдения либо посадить «червя», чтобы выяснить пароль и получить доступ к нужным вам данным.

## Контрмеры

Итак, вы решили перестать прятаться и сменить обличье, поскольку работа в корпорации прельстила вас более высокой оплатой, чем оплата за шпионскую деятельность в общественной организации (и меньшим уровнем риска), и теперь вы целенаправленно занимаетесь обеспечением компьютерной безопасности в компании из списка Fortune 500\*. В ваши обязанности входит защита конфиденциальной информации от ваших бывших коллег, в особенности когда речь заходит об экономическом шпионаже.

Рассмотрим несколько простых и недорогих контрмер, основанных на использовании стойких систем шифрования и надежных паролей, являющихся неотъемлемой частью вашего плана защиты конфиденциальной корпоративной информации.

### Стойкое шифрование

Использование стойких алгоритмов шифрования – первоочередная мера безопасности. Если вам необходима надежная защита информации, не полагайтесь на встроенные функции защиты данных с помощью паролей, встречающиеся в большинстве коммерческих приложений. Используйте

\* Fortune 500 – ежегодно обновляемый список пятисот крупнейших компаний США, публикуемый журналом “Fortune” по результатам собственных экономических исследований. – Прим. ред.

специальные приложения для шифрования файлов или информации «на лету» (которые были перечислены в главе 5). В то же время не позволяйте стойкому алгоритму шифрования внушить вам ложное чувство собственной безопасности. Как вы уже убедились на примерах, способы шифрования информации бывают разные.

## Политики паролей

Вы думаете, что компьютерный шпионаж – это увлекательное и рискованное занятие? Тогда его противоположностью можно считать применение контрмер, которые обычно сводятся к нудной бюрократичной политике. Тем не менее хорошая политика безопасности – главное препятствие на пути потенциального шпиона. Наибольшую важность имеет политика паролей, поскольку именно пароль может оказаться той брешью в защите системы, которой не преминет воспользоваться шпион.

Вам не нужно являться сотрудником огромной корпорации, чтобы прийти к необходимости разработки собственных политик безопасности. Вам даже не обязательно оформлять эту политику в письменном виде (хотя это желательно, поскольку уменьшает шансы забыть о ней в текучке дел, а кроме того, в таком виде ее легче делиться с другими сотрудниками организации). В следующем параграфе мы поговорим об основных концепциях политики безопасности.

Помните, что ключом к успеху политики безопасности является ее соблюдение. Если вы или другие сотрудники не будете постоянно ее придерживаться, вы подвергнете себя риску атаки, угрожающей раскрытием конфиденциальной информации.

## «СТОЙКИЕ» ПАРОЛИ

На данный момент вы уже должны хорошо себе представлять, как выглядит «стойкий» пароль. На всякий случай напомним вам, что в качестве пароля нельзя использовать имена (особенно ваших вторых половин), даты (дней рождения), слова, встречающиеся в словаре, имена учетных записей и другие легко отгадываемые слова и сочетания букв. Устойчивый пароль должен обладать следующими характеристиками:

- состоять, по крайней мере, из восьми символов (чем больше, тем лучше, особенно если вы хотите защитить себя от противника, располагающего значительными ресурсами);
- не должен являться словом (любого языка), которое можно встретить в словаре;
- не должен основываться на личной информации;
- должен содержать символы верхнего и нижнего регистров (a-z, A-Z);

- помимо букв желательно, чтобы в нем содержались цифры и знаки пунктуации (0...9 и любые из нижеперечисленных символов: !@#\$%^&\*()\_-~=\\{}[]:;”<>?,./);
- являться легко запоминаемым для вас (чтобы его не пришлось записывать);
- использовать можно только тот пароль, который до этого никогда не записывался на бумаге или электронных носителях в незашифрованном виде.

Наилучший метод построения надежных паролей – использовать несколько слов и/или символов, формирующих запоминающуюся фразу, – например, Muscat\$Is1Fatty или Iht1tAM\* (I have traffic in the AM). Благодаря большой длине и псевдослучайному распределению символов, такие пароли весьма устойчивы к «лобовым» атакам.

В то же время ни в коем случае не забывайте, что хороший пароль без хорошего алгоритма шифрования абсолютно бесполезен. Нашему гипотетическому террористу не помог стойкий пароль, поскольку он использовал его для документов, сохраненных в старых версиях Word с недостаточно надежным алгоритмом шифрования.

## ПАРОЛИ, ГЕНЕРИРУЕМЫЕ СЛУЧАЙНЫМ ОБРАЗОМ

Некоторые эксперты в сфере компьютерной безопасности рекомендуют своим клиентам использовать случайным образом сгенерированные пароли – псевдослучайные последовательности букв, цифр и символов (по-настоящему случайную последовательность обычно очень трудно получить). Логическим обоснованием данной рекомендации служит тот факт, что пользователи часто выбирают слишком простые (зато легкие для запоминания) пароли. Найти утилиты, предназначенные для генерации псевдослучайных паролей, вы можете в сети Интернет при помощи вашего любимого поискового сервера.

Несмотря на обоснованность подобного подхода, исследования показали, что данная тактика является, в определенном смысле, ошибочной. Пользователи вынуждены запоминать бессмысленные последовательности символов, тогда как применение мемориических фраз не менее эффективно. При использовании же случайным образом генерируемых паролей в некоторых случаях усилия, связанные с их генерацией и запоминанием, превышают полученную выгоду от дополнительной безопасности.



Янкин Ян, Алан Блэквел, Росс Андерсон и Алласдер Грант написали отличную статью под названием «Запоминаемость и безопасность паролей – некоторые эмпирические результаты», в которой они развенчивают хваленную надежность случайных паролей, а также приводят другие интересные факты, связанные с использованием паролей. Загрузить статью вы можете по адресу: [www.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf](http://www.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf).

## ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ

Не забывайте, что от пароля зависит устойчивость всего карточного домика безопасности (или, если вам угодно, его применение связано с эффектом домино, цепной реакцией, лазерным эффектом либо любой другой метафорой, которую вы считаете наиболее подходящей в данном случае). Если вы используете для всех случаев жизни один, пусть даже очень сложный пароль, то его раскрытие приведет к тому, что вы сможете попрощаться с конфиденциальностью всей вашей информации.

В то же время, чтобы свести к минимуму количество необходимых для запоминания паролей, можно, как принято в разведывательных управлениях, использовать разные пароли для разных сфер деятельности, требующих своего уровня секретности. Например, переписку с вашим юристом можно отнести к информации, требующей высокого уровня конфиденциальности, тогда как подключение к интернет-форумам не нуждается в таком уровне защиты. Применение в указанных примерах разных паролей позволит вам избежать угрозы для вашей конфиденциальной переписки в случае раскрытия пароля, используемого для подключения к интернет-форуму.

## ЗАЩИТА ОТ ПРИЕМОВ СОЦИОТЕХНИКИ

Как мы уже говорили, хороший шпион старается использовать для взлома систем не только все уязвимые места в техническом плане, но и человеческий фактор. Нередко легче выяснить пароль, используя приемы социотехники, основанные на поведенческих стереотипах человека. Поэтому ваша политика безопасности паролей должна включать следующие правила для защиты от приемов социотехники:

- Не сообщать пароль по телефону.
- Не пересылать пароль по электронной почте.
- Не сообщать пароль вашим коллегам или менеджеру.
- Не произносить пароль вслух при других людях.
- Не описывать содержание пароля, например «имя моей жены».
- Не указывать свой пароль в анкетах или формах.
- Не сообщать пароль членам семьи.
- Не использовать легко разгадываемые подсказки для паролей в приложениях или на веб-сайтах, предоставляющих альтернативный способ доступа в случае вашей забывчивости. Простые подсказки сужают область поиска для потенциального шпиона, намеренного взломать вашу учетную запись.
- Не использовать один и тот же пароль для подключения к веб-сайту и для шифрования конфиденциальной информации, к примеру.

## РЕГУЛЯРНАЯ СМЕНА ПАРОЛЕЙ

Чем дольше вы используете пароль, тем выше шансы, что кто-то случайно или сознательно раскроет его. Менять свой пароль необходимо регулярно, по крайней мере, раз в три–шесть месяцев. (Одна американская пословица говорит, что пароль нужно менять так же часто, как зубную щетку, а стоматологи рекомендуют делать это раз в три–четыре месяца).

Подходите к смене пароля творчески, старайтесь не использовать повторно старые пароли. Многие пользователи попадают в эту ловушку и постоянно используют два–три пароля, меняя их по очереди, когда приходит время. Учтите, что при этом вы сильно рискуете.

## Списки паролей

Современная жизнь полна сложностей. Вам приходится запоминать пароли для входа в систему, пароли для проверки почты, пароли для подключения к платным веб-сайтам, пин-коды для банкоматов, дни рождения и годовщины знаменательных событий (из которых наиболее критичной для вашего здоровья является дата свадьбы). Поэтому неудивительно, что люди стараются использовать простые для запоминания (и для раскрытия) пароли.

Простейшее решение в данном случае сводится к хранению зашифрованного списка всех ваших паролей. Список паролей, вместе с информацией о том, для каких целей применяется тот или иной пароль, можно сохранить в текстовом файле, зашифрованном при помощи некоторого стойкого алгоритма шифрования, такого как AES, BlowFish или IDEA. Если вы вдруг забыли пароль, просто расшифруйте файл и найдите нужную вам информацию. При необходимости смены пароля расшифруйте файл, отредактируйте его и заново зашифруйте. Если вы страдаете паранойей (независимо от того, имеются ли для этого основания), вы можете скрыть список паролей внутри другого файла с помощью одной из стеганографических утилит, описанных в разделе «Контрмеры» пятой главы.

Вы помните поговорку о том, что нельзя класть все деньги в один банк? Тогда, если вы не хотите, чтобы вся эта информация попала в руки шпиона:

- убедитесь, что используемый вами алгоритм шифрования достаточно надежен и заслуживает доверия;
- используйте сложный пароль;
- убедитесь в невозможности утечки данных в виде простого текста из приложения или операционной системы.

Один из способов проверки отсутствия утечек информации заключается в использовании после шифрования документа редактора шестнадцатеричных кодов для поиска на жестком диске уникальной строки символов, которая существует только в защищенном документе (например, одного из ваших паролей). Если такая строка будет найдена, следовательно, либо утечку информации допускает приложение, записывая информацию во временные файлы, о которых вам ничего не известно,

либо операционная система сохраняет данные в файле подкачки. В таком случае подумайте над созданием загрузочного диска DOS с простым текстовым редактором и версией утилиты шифрования для командной строки. В дальнейшем используйте эту дискету для просмотра и редактирования списка паролей.

Еще одна альтернатива – использование коммерческих или свободно распространяемых программ для управления паролями. Эти программы позволяют хранить в зашифрованной базе данных пароли и другую конфиденциальную информацию. (Бесплатные менеджеры паролей под Windows вы можете найти в сети Интернет по следующей ссылке: [www.webattack.com/Freeware/security/fwpass.shtml](http://www.webattack.com/Freeware/security/fwpass.shtml).) Хотя пользоваться подобными менеджерами паролей чрезвычайно легко и удобно, учтите, что при этом вам, опять-таки, придется довериться знаниям и навыкам неизвестного программиста.

## Альтернативы паролю

Как вы понимаете, пароль представляет собой всего лишь метод аутентификации, то есть способ различения одного компьютерного пользователя от другого. Поскольку простые текстовые пароли достаточно легко отгадать, а убедить людей использовать надежные пароли трудно, существуют другие методы аутентификации, обеспечивающие более высокий уровень безопасности. Далее мы вкратце рассмотрим несколько альтернативных устройств аутентификации, которые уже применяются на практике или могут найти применение в ближайшем будущем.

### БИОМЕТРИЯ

Многие альтернативные устройства аутентификации основаны на принципах биометрии. Вместо традиционной системы с паролем, для доступа к которой вам нужно сообщить нечто, известное только вам (пароль), биометрические устройства считывают уникальные физические характеристики человека.

В настоящее время вокруг биометрии сложилось несколько превратное мнение как исключительно о средстве борьбы с терроризмом. Когда дело доходит до широкого применения, биометрические системы продолжают демонстрировать свое несовершенство; понадобится устранить еще немало ошибок, прежде чем эти системы можно будет внедрять повсеместно. Точность биометрических систем характеризуется двумя параметрами:

- **FFR (False Rejection Rate)** – процент ошибочных отказов, когда система отказывает в доступе авторизованному пользователю;
- **FAR (False Acceptance Rate)** – процент ошибочных допусков, когда доступ к системе ошибочно предоставляется неавторизованным пользователям.

Необходимо знать оба параметра системы (FRR и FAR), особенно если они были получены в результате лабораторных тестов либо скрупулезного анализа результатов ежедневного использования. Кроме того, намереваясь приобрести ту или иную биометрическую систему, вы должны вначале выяснить ее уязвимые места:

- **Атака путем повторной передачи корректной информации.** Аппаратные компоненты биометрической системы должны передавать информацию на обработку программным компонентам для аутентификации пользователя. Если эти передаваемые данные в определенный момент времени перехватить, то в будущем можно попытаться повторно симулировать их передачу от аппаратных компонентов, чтобы получить доступ к системе. К примеру, при использовании сканера для проверки отпечатков пальцев, подключенного через порт USB, последовательность передаваемых во время верификации данных может быть перехвачена, и позднее повторно передана тому же порту.
- **Фальсификация.** Поскольку принцип работы биометрических устройств идентификации сводится к распознаванию некоторых физических характеристик человека, можно попытаться создать точную копию характеристики. Например, чтобы обмануть систему распознавания по голосу, достаточно воспроизвести речь этого человека, записанную на пленку.
- **Манипуляции с базой данных.** Биометрическая информация должна храниться в некоторой базе данных, чтобы поступившие данные можно было сравнивать с некоторым образцом в процессе аутентификации пользователя. Поэтому, проникнув в базу данных, шпион может добавить характеристики пользователя, ранее не имевшего права на доступ к системе.
- **Инженерный анализ.** Любое устройство биометрической аутентификации состоит из аппаратной и программной части, которые взаимодействуют с операционной системой или приложениями. Можно проанализировать программный код приложения, чтобы в дальнейшем создать программную «заплату», позволяющую всегда идентифицировать пользователя как легального, даже если на самом деле его данные вообще отсутствуют в системе. Ведь в течение многих лет компьютерные пираты успешно игнорировали, например, схемы защиты программного обеспечения от копирования, изменяя значения шестнадцатеричных кодов на ассемблере в операторах условного выбора либо заменяя фрагменты кода холостыми командами (NOP). И если подростки в состоянии дизассемблировать приложение и убрать нетривиальные средства защиты программы от копирования, то, очевидно, что защита системы биометрической аутентификации также может быть взломана.

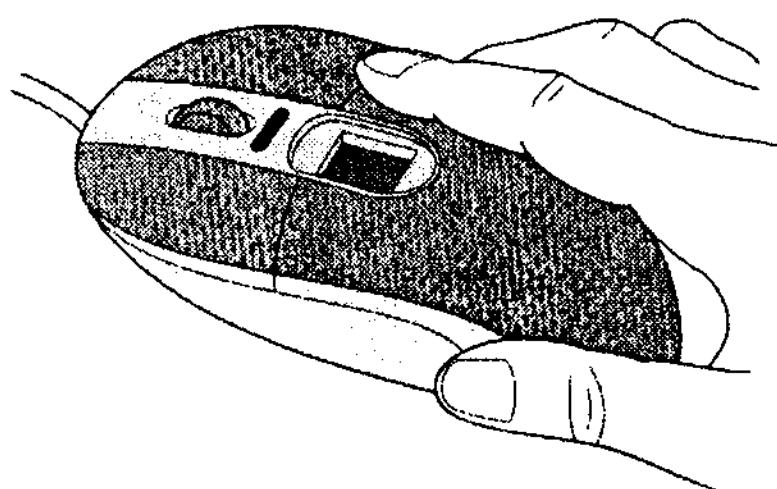
Учтите, что с ростом популярности и распространением биометрических устройств в них могут обнаружиться и стать известными широкой общественности новые уязвимые места и способы их использования. Нельзя полагаться исключительно на биометрию, как и на любую другую технологию, для защиты конфиденциальных данных. Необходимо, чтобы биометрические устройства включались в состав интегрированных многоуровневых систем защиты информации.



Немецкий компьютерный журнал c't опубликовал в ноябре 2002 года статью, содержащую результаты тестирования 11 биометрических устройств. Во всех случаях система защиты была успешно взломана при помощи ряда простых атак. Англоязычную версию статьи вы можете прочесть по адресу <http://heise.de/ct/english/02/11/114/>.

**СКАНЕРЫ ОТПЕЧАТКОВ ПАЛЬЦЕВ.** На сегодняшний день к наиболее распространенным биометрическим устройствам относятся именно сканеры отпечатков пальцев. Модели, ориентированные на массовый рынок, розничная цена которых колеблется в пределах \$100...\$150, выполняют распознавание рельефа кожи на пальцах при помощи внешних аппаратных сканеров, которые могут быть встроены в клавиатуру или мышь (как показано на рис. 6.3). Вначале сканируется отпечаток пальцев авторизованного пользователя, который затем сохраняется в базе данных (в виде 256-байтного «файла деталей» – изображения, преобразованного в серию точек, в отличие от цифрового изображения отпечатков пальцев, которое обычно делается полицией). Затем, когда возникает необходимость идентифицировать пользователя, система повторно сканирует его отпечатки пальцев и осуществляет поиск совпадения в базе данных. Если такой отпечаток пальцев найден в базе, вы получаете доступ к компьютеру или данным. Если нет – что ж, значит, вам не повезло.

К сожалению, системы распознавания отпечатков пальцев далеки от совершенства: на точность распознавания может влиять естественное шелушение кожного покрова, царапины, рубцы, пот и грязь. Вдобавок, если ваш противник имеет доступ к вашему пальцу (его отпечаткам) или их точной копии, существует немалая вероятность того, что эта система защиты может быть обманута.



**Рис. 6.3.** Сканер для отпечатков пальцев, встроенный в мышь

## Тактика: как все испортить

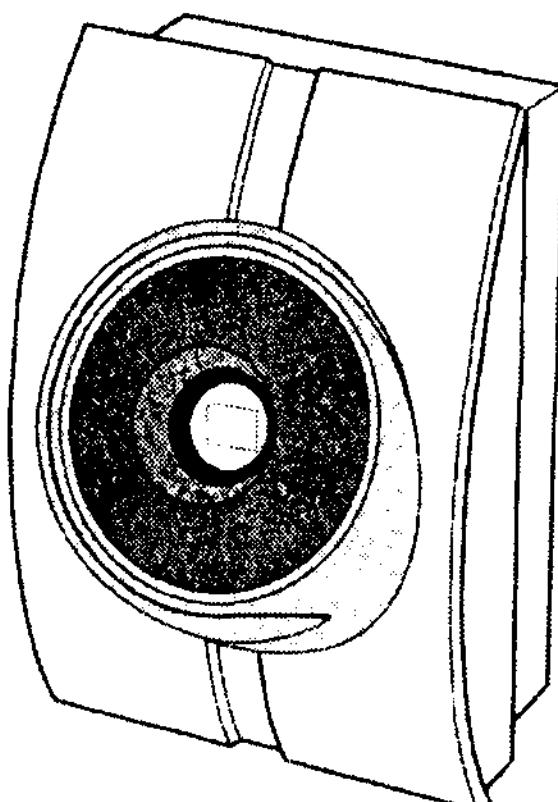
В мае 2002 года Цутому Матцумото, исследователь из Национального университета в Иокогаме, провел презентацию (а позднее опубликовал статью) об уязвимых местах сканеров для отпечатков пальцев. Потратив \$10 долларов на пищевые продукты, которые можно найти на кухне любой домохозяйки, ему удалось сделать из них фальшивые желатиновые отпечатки пальцев, при помощи которых были обмануты большинство моделей сканеров.

Матцумото сделал пластиковые слепки для пальцев некоторых добровольцев, которые затем были заполнены желатином (из тех же самых материалов изготавливаются мишки Гамми). Восстановленные таким образом отпечатки оказались достаточно надежными для того, чтобы обмануть сканер в 80% случаев. Матцумото также попытался воспользоваться скрытыми отпечатками пальцев, оставленными на стекле, и не меньше преуспел в этом деле, сделав фальшивые отпечатки, которые помогли одурачить большинство сканеров.

Производители сканеров для отпечатков пальцев поспешили опротестовать работу Матцумото, заявив, что подобный успех возможен только в лабораторных условиях. Однако дело было сделано – большинство экспертов по безопасности сомнением покачали головами и решили, что проведенные исследования являются веской причиной для того, чтобы не полагаться исключительно на биометрические сканеры отпечатков пальцев, как на единственный метод защиты конфиденциальной информации.

Презентацию Матцумото в формате PowerPoint, включая цветные фотографии и инструкции по созданию ваших собственных искусственных отпечатков пальцев, вы можете загрузить по адресу [www.itu.int/itudoctitu-t/workshop/security/present/s5p4.pdf](http://www.itu.int/itudoctitu-t/workshop/security/present/s5p4.pdf).

**СКАНЕРЫ СЕТЧАТКИ ГЛАЗА.** Широко рекламируемые в шпионских боевиках и телевизионных шоу сканеры сетчатки глаза делятся на две категории. К первой относятся собственно сканеры сетчатки стоимостью \$400...\$500, принцип работы которых заключается в направлении инфракрасного луча малой интенсивности непосредственно в зрачок для фотографирования узора, создаваемого сеткой кровеносных сосудов на глазном дне. Такие высокоточные устройства встречаются в организациях, требующих высокого уровня безопасности. Сканеры радужной оболочки, один из которых изображен на рис. 6.4, основаны на другой запатентованной технологии, отличающейся меньшей агрессивностью, чем сканирование сетчатки, поскольку подобные сканеры пассивно записывают картинку пятнышек и прожилок на поверхности радужки. К тому же



**Рис. 6.4.** Устройство, выполняющее сканирование радужной оболочки глаза, сохраняет рисунок радужки, когда вы смотрите в объектив. В отличие от сканеров сетчатки, оно не направляет световой луч непосредственно в ваш глаз

они имеют более низкую стоимость – от \$200 до \$300. Однако, в отличие от сканеров сетчатки глаза, показавших свою высокую надежность, сканеры радужной оболочки могут быть обмануты при помощи снимка глаза с очень высокой детализацией.

**ГОЛОСОВЫЕ СКАНЕРЫ.** Эти биометрические устройства проверяют характеристики человеческого голоса, такие как основной тон, тембр и характерные частоты. Поскольку практически все компьютеры имеют звуковые карты со входом для микрофона, реализовать данную технологию очень просто. Однако на точность их распознавания сильно влияет зашумленность помещения, качество микрофона или нормальное изменение характеристик голоса, вызванное, к примеру, простудой владельца. Стоимость голосовых сканеров на сегодняшний день колеблется в пределах \$150...\$200.



Если вы хотите больше узнать о биометрических системах аутентификации, посетите официальный сайт Биометрического консорциума ([www.biometrics.org](http://www.biometrics.org)) либо исследовательскую страницу по биометрии Мичиганского государственного университета (<http://biometrics.cse.msu.edu>).

## СМАРТ-КАРТЫ

Смарт-карты представляют собой обычные пластиковые карты размером с кредитную карточку, со встроенным микропроцессором. Название «смарт-карты» они получили за свою интеллектуальность\*, поскольку в

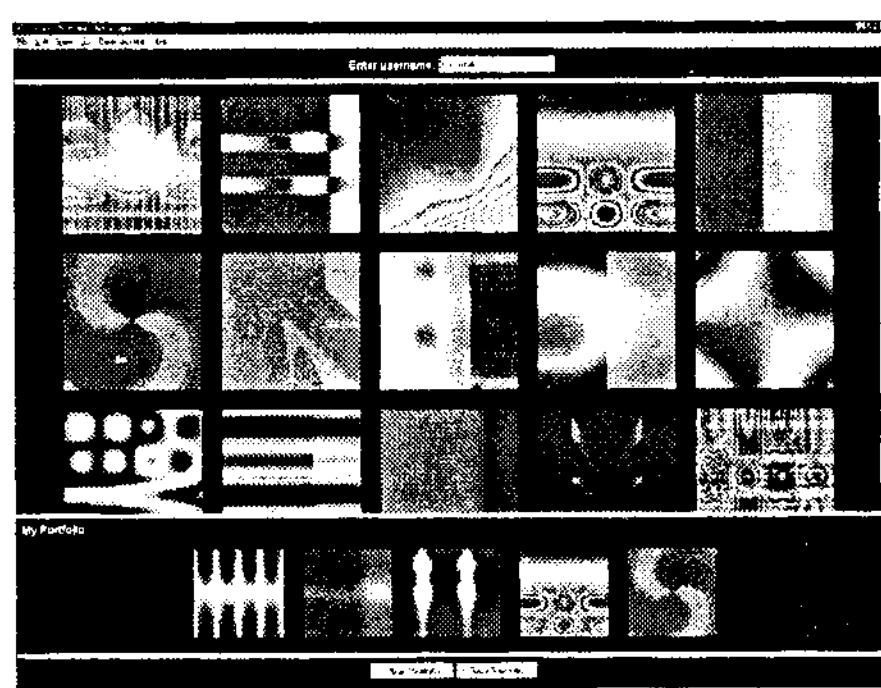
\* От англ. “smart” – «разумный». – Прим. ред.

них имеется собственный процессор, память и операционная система. В целях безопасности в этих картах применяют одновременно два принципа аутентификации: что-то, чем вы владеете, и нечто, что вам известно. Как только вы вставите карту во внешнее считывающее устройство (большинство современных смарт-карт могут подключаться непосредственно к вездесущим портам USB, избавляя вас от необходимости приобретать отдельное устройство считывания), она самостоятельно инициализируется, после чего пользователю предлагается ввести собственный идентификационный код (PIN) для доступа к системе или сети.

Несмотря на относительную надежность аутентификации с помощью смарт-карт, технически подкованные шпионы в состоянии обмануть их. Веб-сайт Бо Лавара целиком посвящен вопросам безопасности смарт-карт. Его адрес в сети Интернет: [www.geocities.com/ResearchTriangle/Lab/1578/smart.htm](http://www.geocities.com/ResearchTriangle/Lab/1578/smart.htm).

## РАСПОЗНАВАНИЕ СИМВОЛОВ

Еще один метод аутентификации, не связанный с биометрией, основан на распознавании символов либо изображений. Вместо диалогового окна ввода текстового пароля, перед вами на экране появляется серия картинок. Пользователь последовательно щелкает мышью по тем или иным изображениям. Исследования показали, что картинки запоминаются намного легче, чем, например, текстовые пароли, и, очевидно, являются менее восприимчивыми к атакам при помощи словаря (хотя количество исследовательских работ, проведенных в данной области, явно недостаточно, для того чтобы утверждать, что использование различных картинок равновероятно, или, наоборот, одни изображения могут использоваться людьми чаще, чем другие, что сродни применению ненадежного пароля). Рашина Дамия и Эдриан Перриг разработали экспериментальную систему под названием «Дежа Вю», показанную на рис. 6.5, который иллюстрирует данную концепцию аутентификации. За более подробной информацией обращайтесь на их сайт [www.sims.berkeley.edu/~rachna/dejavu/](http://www.sims.berkeley.edu/~rachna/dejavu/).



**Рис. 6.5.** Окно выбора картинки пользователя в системе аутентификации «Дежа Вю»

# Заключение

Информация и доказательства, которые кажутся вам защищенными, на деле не всегда оказываются таковыми. Нестойкие алгоритмы шифрования и ненадежные пароли – верная лазейка для шпиона, стремящегося взломать защищенные данные при помощи различных широко распространенных и простых в использовании утилит.

Если на вашей компьютерной системе хранятся конфиденциальные документы, не надейтесь на системы парольной защиты, встраиваемые во многие коммерческие продукты. Лучше использовать специальные приложения со стойкими алгоритмами шифрования. Кроме того, вы должны четко представлять себе риски, связанные с применением паролей, и соблюдать такую политику паролей, которая бы свела к минимуму угрозу атак из-за неправильно выбранных ненадежных паролей.

## Глава 7

# Копирование информации

«...Запиши это в свою тетрадь, мой друг, шпион Гаррет».

Indigo Girls, «Garamia», *Shaming the Sun*

Получив доступ к вашему компьютеру, шпион в первую очередь захочет скопировать с него наиболее важную информацию. Однако не думайте, что копирование информации – это простое занятие, не требующее детального обсуждения; на самом деле при этом необходимо учитывать многие аспекты и возможные альтернативы, в особенности когда речь заходит о компьютерном шпионаже.

Каждый носитель информации, будь то обычная или ZIP-дискета, CD-R и т. д., обладает своими преимуществами и недостатками в плане компьютерного шпионажа. Кроме того, вам стоит познакомиться с различными специальными внешними устройствами, подключаемыми к целевому компьютеру для дублирования информации. Большинство подобных устройств не являются чем-то из ряда вон выходящим, имеют небольшую стоимость и вполне могли бы пригодиться Джеймсу Бонду в его очередных приключениях.

В отличие от многих глав данной книги, содержащих раздел «Контрмеры» вслед за «Шпионской тактикой», в этой главе подобный раздел отсутствует. Дело в том, что если вы предварительно позаботитесь о соблюдении всех контрмер, описанных в предыдущих главах книги, включая ограничение физического доступа к компьютеру, шифрование, надежные пароли и т. д., шпион не сможет получить доступ к целевому компьютеру и просмотреть данные на нем, не говоря уже об их копировании.

А теперь, после краткого вступления, перейдем к рассмотрению способов копирования информации с точки зрения шпиона.

## Шпионская тактика

Перед тем как начать обсуждение носителей информации и высокотехнологичных приспособлений, рассмотрим четыре основных совета по копированию данных, о которых ни в коем случае нельзя забывать, когда вы начинаете работать с целевым компьютером:

- **Используйте имеющиеся ресурсы.** В первую очередь воспользуйтесь уже установленными устройствами для копирования информации.
- **Применяйте программы архивации.** Не забудьте взять с собой диск с архиваторами, на случай если данные не будут помещаться на носители.
- **Исследуйте другие источники информации.** Не зацикливатесь исключительно на жестком диске, как единственном источнике информации.
- **Досконально изучите процесс копирования информации.** Практикуйтесь в копировании информации заранее.

## Используйте доступные ресурсы

Китайский стратег Сунь-Цзы советовал всегда стараться использовать вражеские ресурсы в собственных целях, и когда речь идет о копировании информации, эта его рекомендация подходит как нельзя лучше. Целевой компьютер должен иметь, по крайней мере, дисковод для гибких дисков. Если вам повезет, на интересующем вас компьютере окажется привод ZIP или пишущий CD-ROM. Ну а если вы патологический везунчик, тогда на компьютере вполне может оказаться установленной программа резервного копирования важной информации.

Кроме тех случаев, когда вам нужен точный образ жесткого диска, используйте в целях копирования имеющееся аппаратное обеспечение. Вам всегда следует иметь с собой набор пустых дискет, CD-R, CD-RW и, возможно, ZIP- или Jaz-дискет, чтобы было, на что переписать нужную информацию, когда на месте нечего будет «позаимствовать».

## Применяйте программы архивации

Помимо пустых носителей, вы должны всегда иметь с собой диск с набором шпионских утилит и обычных архиваторов (таких как GZip, WinZip или WinRAR). Ведь нередко возникает необходимость уместить большое количество информации на носителях меньшего объема. При этом учите, что архивация данных требует времени, а в некоторых случаях бывает на счету каждая секунда.



Различные программы архивации демонстрируют различную эффективность по скорости и качеству сжатия. Вы можете прочесть результаты сравнения различных архиваторов на сайте Мартина Цачева, размещенном по адресу [martin.f2o.org/windows/archivers](http://martin.f2o.org/windows/archivers).

## Исследуйте другие источники информации

Помните, что жесткий диск компьютера не единственное место, на котором может находиться интересующая вас информация. Изучите расположенные на рабочем месте дискеты, компакт-диски, ленточные кассеты с архивной информацией; просмотрите содержимое ящиков стола и шкафа, картотеку. Вам придется скопировать информацию с этих носителей на месте либо забрать их с собой, если вы уверены в том, что пропажу не заметят. Если, к примеру, носитель информации помечен словом «архив», просмотрите содержимое жесткого диска компьютера, чтобы определить, с помощью какого программного обеспечения он был создан.

## Досконально изучите процесс копирования информации

Чем больше времени займет у вас копирование информации на месте операции, тем больше ваши шансы оказаться пойманным с поличным. Тот факт, что супершпион в популярном кинофильме умудряется скопировать сотню гигабайт информации на одну дискету в течение нескольких секунд, не означает, что то же самое удастся вам. Вы должны иметь представление о возможностях и ограничениях различных технологий копирования и носителей информации.

При копировании информации важно знать такую характеристику, как скорость передачи данных. Она определяет пиковую пропускную способность устройства: Мб/с означает количество мегабайт в секунду, Мбит/с – количество мегабит в секунду, а Кбит/с – количество килобит в секунду (три вышеперечисленных аббревиатуры будут использоваться в этой и следующих главах книги). Возможно, ваше время пребывания у компьютера ограничено жесткими рамками, но вам, так или иначе, придется смириться с максимальной скоростью копирования, которую может обеспечить используемое устройство. (Существуют и другие параметры, влияющие на скорость копирования, например пропускная способность системной шины компьютера или конкретной разновидности носителя, на котором записана информация, однако на них вы никак не сможете повлиять.)

Необходимо заранее попрактиковаться в копировании данных при помощи различных утилит копирования, используя разные носители, чтобы точнее оценить, сколько времени и усилий может занять копирование интересующей вас информации.

## Риски: низкие технологии, высокие ставки

В субботу, 14 декабря 2002 года, неизвестный вломился в офис корпорации TriWest Healthcare Alliance, Феникс, штат Аризона. Однако это не была простая кража со взломом. Вор в первую очередь пробрался в кабинет главного менеджера, похитил электронный ключ, а затем с его помощью проник в другие офисы компании. Внутри отсутствовали камеры слежения, однако по протоколу работы электронных дверей было установлено, что взломщик (или взломщики) дважды входил/и и выходил/и из офиса корпорации TriWest, расположенного в северо-западной промышленной зоне Феникса.

Кто бы это ни был, создалось впечатление, что злоумышленники хорошо знали, что делают. Они извлекли из серверов накопители на жестких дисках, на которых хранились данные по страховке и информация о предъявленных претензиях. Записи содержали личные сведения о более чем 550 000 получателей страховых пособий от военной организации медицинского обслуживания США TRICARE, действующей в 16 штатах. (Информация о том, являлись ли похищенные данные зашифрованными, отсутствует.)

ФБР и Отдел уголовных расследований Министерства обороны начали расследование кражи, а корпорация TriWest назначила вознаграждение в размере 100 000 долларов тому, кто сообщит следствию информацию, которая помогла бы в аресте преступников. Кроме того, всем получателям пособий были высланы письма с предупреждением о том, что их личные сведения были выкрадены. Министерство обороны, в свою очередь, затягивало пересмотр правил соблюдения безопасности по доступу к носителям информации для своих гражданских сотрудников. На данный момент не известен ни мотив преступления, ни подозреваемые, а все причастные к расследованию лица держат рот на замке (скорее всего, дело связано не только с нарушением уголовного кодекса, но и с угрозой национальной безопасности страны).

Даже если окажется, что эта кража никак не связана со шпионажем, ее можно приводить в качестве наглядного примера уязвимости высоких технологий к старомодному применению лома и отмычки. Если бы преступники поставили себе целью сделать атаку незаметной, они могли бы подменить жесткие диски на поврежденные диски того же типа. Системный администратор списал бы все на резкие скачки напряжения, приведшие к физической поломке головок жесткого диска, и просто заменил бы жесткие диски на новые, восстановив информацию с резервной копии. При «правильном» подходе компания могла бы вообще никогда не узнать о факте похищения информации.

# Необходимые носители информации

Помня приведенные выше советы, изучим некоторые широко используемые переносные носители информации, с помощью которых вы можете копировать данные (громоздкие, высокотехнологичные или экзотические носители информации выходят за рамки книги).

## Дискеты

Иногда шпионы принимают как само собой разумеющееся, что им удастся записать всю необходимую информацию на небольшую 3,5-дюймовую дискету и преспокойно вынести ее из здания в кармане рубашки. Однако так бывает не всегда.

В 1971 году компания IBM представила первый в мире «запоминающий диск». Первый гибкий диск (названный так именно потому, что его легко можно было согнуть, в отличие от жесткого) имел восемь дюймов в диаметре, предназначался только для чтения и мог хранить не более 100 Кб информации. Тем не менее это было революционное изобретение, поскольку диск был относительно небольшим и мобильным; вам больше не нужно было таскать стопки перфокарт либо магнитные ленты для переноса информации с одного компьютера на другой. Несколько лет спустя IBM презентовала версию диска, предназначенную как для чтения, так и для записи, на которой можно было разместить уже целых 250 Кб информации. Использованные в нем принципы записи до сих пор применяются в современных накопителях на гибких дисках.

С этого момента гибкие диски начали уменьшаться в размере и одновременно увеличиваться в объеме хранимой информации. Гибкий диск размером 5,25 дюйма появился в 1976 году, однако на нем, опять-таки, можно было хранить только 100 Кб данных. Но вскоре исследователи научились записывать информацию на обеих сторонах диска, что позволило резко увеличить емкость хранения – до 1,2 Мб.

Наконец, в 1981 году, компания Sony представила новый диск размером 3,5 дюйма, который, в конце концов, стал стандартом, пришедшим на смену 5,25-дюймовым дискетам. И теперь вы на каждом углу можете встретить небольшие, заключенные в пластиковую оболочку двусторонние диски двойной плотности, которые могут хранить 1,44 Мб информации и передавать данные на скорости 500 Кб/с, а их стоимость не превышает 20 центов за штуку.

Большинство людей полагают, что гибкие диски из-за их ограниченной емкости вскоре постигнет судьба динозавров. Это действительно так, если говорить о копировании больших объемов информации, однако гибкие диски по-прежнему могут быть полезны при дублировании небольших порций данных либо применения в других шпионских целях. Такие известные (а ныне осужденные) шпионы, как Роберт Хансен, Элдрик

Эймс или Анна Белен Монтес, использовали в своих целях обычные гибкие дискеты, получая на них инструкции от связных и передавая украденную информацию через тайники (предварительно оговоренные места, где шпионы оставляют информацию либо оборудование для связных и получают ее обратно, избегая таким образом личного контакта друг с другом).

## CD-R/CD-RW

Для многих пользователей компьютеров компакт-диски успели стать альтернативой вездесущим дискетам в качестве средства переноса информации. Приводы для записи компакт-дисков быстро превратились в стандартный компонент новых компьютерных систем, что стимулировалось популярностью загрузки и распространения музыки по сетям P2P. Основные характеристики данных носителей информации таковы:

- Один компакт-диск стандартного размера предназначен для хранения от 650 до 870 Мб данных. Диски CD-R позволяют выполнять однократную запись информации, тогда как на CD-RW вы можете перезаписывать информацию множество раз.
- CD-R- и CD-RW-диски недороги: в зависимости от качества их цена составляет около 50 центов за штуку и даже меньше.
- Когда говорят о скорости передачи данных, которая зависит от возможностей привода, обычно подразумевают скорость записи. Чем больше это число, тем выше скорость (запись данных на CD-R-диски выполняется с большей скоростью, чем запись на CD-RW). К примеру, уже довольно старый записывающий привод, пишущий на скорости 8x (что означает пропускную способность в 1200 Кб/с) способен сделать полную копию компакт диска за 10 минут, тогда как при наиболее распространенной скорости записи в 24x (около 3600 Кб/с) запись диска займет менее четырех минут. Приводы с максимальной на сегодняшний день скоростью записи в 52x уже вплотную приблизились к физическому потолку скорости записи.

В комплекте с большинством приводов для записи компакт-дисков поставляется программное обеспечение, позволяющее обращаться с CD-R как с обычными дискетами, так что вы можете копировать файлы непосредственно на них (например, популярный пакет от программы Roxio – DirectCD). Если для копирования информации вы используете пишущий привод для записи CD-R, убедитесь, что вы выбрали правильный стандарт для того, чтобы обеспечить чтение этого CD на любых компьютерах. Программное обеспечение, предназначенное для прямой записи на CD, не позволяет получать доступ к компакт-диску на других компьютерах, как это должно быть с компакт-дисками, предназначенными только для чтения. Если вы используете подобные программы, то, прежде чем записывать CD, необходимо задать такой формат записи, который бы гарантировал читабельность CD на других компьютерах (обычно это ISO 9660).

## Разоблачения: блуждающие диски

В документах ФБР по делу Роберта Хансена говорится, что он часто использовал обычные дискеты для передачи и получения информации от своих русских связных. В его ордере на арест прозвучало весьма любопытное упоминание о гибких дисках:

«4 апреля 1988 года КГБ получило конверт от «Б» с адресом получателя в Восточном округе Виргинии. Отправителем являлся некий Джим Бэйкер из Александрии, хотя на письме стоял почтовый штемпель Северной Виргинии с датой 31 марта 1988 года. В конверте содержалась записка от «Б»: «Используй РЕЖИМ 40 ДОРОЖЕК. Это письмо не является сигналом».

Термин «режим 40 дорожек» связан с техническим процессом переформатирования компьютерных дискет для скрытия данных, хранящихся на других дорожках дискеты. Если знающий человек не воспользуется специальными утилитами восстановления информации с дискеты, она будет казаться пустой.

Письменное указание, говорящее об использовании «режима 40 дорожек», звучит достаточно двусмысленно и, вероятно, подразумевает собою директиву «шифруй». Многие подробности деятельности Хансена остались неизвестны широкой общественности, однако эта ссылка на 40 дорожек может быть связана со следующими техническими нюансами:

- По умолчанию на 40 дорожек разбиваются односторонние дискеты размером в 5,25 дюйма, однако вам никто не мешает отформатировать двухсторонние дискеты в 5,25 дюйма, имеющие размер в 760 Кб или 1,2 Мб и обычно состоящие из 80 дорожек, так, чтобы в них использовались только 40 дорожек. С помощью этой маленькой хитрости вы можете спрятать информацию, размещенную на другой стороне диска.
- Загрузочный вирус под названием Joshi создавал 41-ю дорожку, которая на дискетах формата 5,25 дюйма, размером в 320 Кб должна быть 40-й и на которой хранилось тело вируса. Хансен вполне мог прятать информацию на этой дополнительной дорожке. (Вирус Joshi был впервые обнаружен в 1990 году, два года спустя после отправки зашифрованного сообщения Хансена.)

- Старые накопители Tandy TRS-80 использовали дискеты, разбитые на 35 дорожек, однако поклонники этого привода вскоре обнаружили, что эти дискеты вполне можно отформатировать на нестандартные 40 треков. В 1988 году технология TRS уже считалась устаревшей, однако иногда применение «старых» технологий может сослужить вам хорошую службу, особенно если противник полагает, что вы используете самые современные технические средства.

Как бы там ни было, до тех пор, пока нам не станет доступной вся информация по делу Хансена, остается только гадать, что могло означать упоминание о режиме 40 дорожек.

## Шпионский инструментарий: USB и IEEE 1394

Мечта шпионов о высокоскоростных устройствах копирования информации становится реальностью с появлением USB (универсальной последовательной шины) и стандарта IEEE 1394. В современных операционных системах, поддерживающих технологию plug and play, вам нужно только подключить переносимый носитель информации, например жесткий диск либо пишущий CD-привод, к USB-порту компьютера и приступить к копированию информации. Однако перед тем как вы отправитесь в магазин за необходимым оборудованием, мы расскажем вам краткую предысторию возникновения этих стандартов.

Стандарт USB, предназначенный для подключения периферийных устройств, впервые был представлен в 1997 году. Однако широкое распространение он получил только с выходом Microsoft Windows 98 в июне 1998 года. Оригинальный стандарт USB 1.0/1.1 поддерживал сравнительно низкую пропускную способность в 12 Мб/с (мегабит в секунду, не путайте с мегабайтами в секунду – Мб/с). Компьютеры с поддержкой USB 2.0 начали появляться на рынке только летом 2002 года, но в ближайшие несколько лет стандарт USB 2.0 будет реализован во всех новых компьютерах. Версия USB 2.0 поддерживает скорость передачи данных на уровне 480 Мб/с, и хотя сейчас появляется все больше скоростных устройств передачи данных, поддерживающих стандарт USB 2.0, которые обладают обратной совместимостью с более ранним стандартом USB 1.1, однако будьте готовы к тому, что на сегодняшний день большая часть используемой техники в состоянии работать только со стандартом USB 1.1.

Конкурент USB – технология IEEE 1394 (обычно называемая FireWire – под этим названием ее продает компания Apple, либо i.Link – зарегистрированная торговая марка Sony). Технология IEEE 1394 появилась еще в 1986 году, однако в качестве стандарта она была принята Институтом инженеров по электротехнике и электронике (IEEE – Institute of Electrical and Electronics Engineers) только в 1995 году. Компания Apple использовала этот стандарт в качестве высокоскоростного способа переноса цифровых аудио- и видеоданных между компьютерами Macintosh и другими устройствами. Устройства стандарта IEEE 1394 могут передавать данные на скорости 400 Мб/с. Стандарт IEEE 1394b, появившийся в начале 2003 года в ответ на внедрение USB 2.0, позволяет передавать информацию на вдвое большей скорости – 800 Мб/с.

Хотя компания Microsoft включила поддержку стандарта IEEE 1394 в свои операционные системы, вероятность того, что интересующий вас компьютер будет иметь порт USB, намного выше. Отличный информационный ресурс по теме USB-устройств, включая жесткие диски и приводы для записи компакт-дисков, – сайт EverythingUSB [www.everythingusb.com](http://www.everythingusb.com).

## DVD

DVD-диски (расшифровка аббревиатуры со временем претерпела изменения: вначале DVD расшифровывали как цифровой видеодиск, поскольку он использовался как носитель для видеофильмов, теперь же DVD называют цифровым универсальным диском) являются следующим поколением оптических накопителей. По сути, DVD можно считать скоростным CD, на котором к тому же можно уместить целых 4,7 Гб информации. Благодаря снижению цен на пишущие приводы (сейчас такое устройство можно приобрести менее чем за \$200. – *Прим. перев.*) и устоявшимся стандартам, DVD приобретают все большую популярность, постепенно вытесняя с рынка CD-приводы.

- На сегодняшний день между двумя группами компаний ведется борьба за то, какой стандарт записи DVD-дисков считать основным – DVD-R/DVD-RW или же DVD+R/DVD+RW. Некоторые производители, такие как Sony, отказались принять чью-либо сторону, поэтому их DVD-приводы поддерживают оба набора стандартов.
- Данные, записываемые на DVD со скоростью 1x, передаются со скоростью 11 Мб/с, что почти в девять раз больше скорости 1x для компакт-диска. Существующие на рынке устройства позволяют записывать DVDR на скорости до 4x, и DVD-RW на скорости до 2x. (Кроме того, приводы для записи DVD-дисков с тем же успехом могут читать и записывать диски CD-R/CD-RW).

- В зависимости от заказываемой партии, стоимость болванок DVD-R может составлять от \$1,5 до \$3,5 за штуку, тогда как стоимость DVD-RW колеблется в пределах от \$2,5 до \$4,5. С увеличением спроса и массовости продукта на рынке следует ожидать дальнейшего снижения цен.

И хотя компьютеры с пишущими CD-приводами встречаются намного чаще, чем с пишущими DVD-приводами, вам лучше все-таки иметь про запас чистый DVD-диск, просто на всякий случай.

## ZIP-диски

До того, как пишущие CD-приводы приобрели большую популярность и упали в цене, светлое будущее пророчилось дискам ZIP от компании Iomega ([www.iomega.com](http://www.iomega.com)), которые даже претендовали на роль нового стандарта после обычных дисков. Первые диски ZIP, представленные еще в 1994 году, позволяли хранить до 100 Мб данных и выглядели как утолщенные дисковые стандартного размера. Последние модели дисков ZIP позволяют хранить до 750 Мб информации, а дисковые формата Jaz – до 2 Гб данных.

Внешние ZIP-устройства, подключаемые к порту LTP, имеют чрезвычайно низкую скорость передачи данных (от 300 до 800 Кб/с) по сравнению с IDE-версиями (работающими на скорости 1,4...2,4 Мб/с). Несмотря на то, что ZIP- и Jaz-приводы последних моделей позволяют передавать информацию на высоких скоростях, высокая стоимость носителей (от \$7 до \$10 за диск) и появление недорогих пишущих CD-приводов и дисков привели к резкому падению популярности этих устройств. Тем не менее вы все еще можете встретить приводы ZIP на старых компьютерах (эти приводы были весьма популярны в компаниях, занимающихся графикой и дизайном).

## Устройства внешней памяти

Если вам не требуется копировать большие объемы информации, наилучший выбор – это устройства внешней флэш-памяти. Их легко спрятать благодаря их небольшому размеру, и они удобны в обращении, так как для хранения данных во флэш-памяти не требуется внешний источник энергии, поскольку она является энергонезависимой.

Вам потребуется только вставить карту флэш-памяти в устройство считывания, подключив его, например, к разъему PC-card ноутбука (несколько моделей ноутбуков имеют отдельные слоты, предназначенные непосредственно для подключения карт памяти) либо к настольному компьютеру, и начать копирование нужных файлов.

Поскольку на сегодняшний день отсутствует единый стандарт флэш-памяти для различных устройств (цифровых фотовидеокамер, карманных компьютеров и аудиоплееров), на рынке представлены следующие типы флэш-памяти:

- **CompactFlash (CF).** Первое устройство хранения флэш-памяти, представленное компанией SanDisk в 1994 году (и по сей день остается одним из самых популярных).
- **MemoryStick.** Разработанное компанией Sony устройство хранения информации, появившееся в 1998 году.
- **Multimedia Memory Card (MMC).** Небольшая карта памяти размером с почтовую марку.
- **Secure Digital.** Карты памяти со встроенной защитой от случайной перезаписи.
- **SmartMedia.** Устройства памяти, которые меньше и легче, чем модули CompactFlash.

Карты памяти CompactFlash лучше всего подходят для решения шпионских задач, поскольку они позволяют хранить большие объемы информации (в марте 2003 года компания SanDisk представила новые накопители объемом в 4 Гб, продажа которых началась летом 2003 при розничной цене в \$999), чем другие аналогичные устройства, и имеют больший срок службы. Новые высокоскоростные накопители информации Ultra CF поддерживают передачу данных на скорости 2,8 Мб/с, что почти вдвое больше, чем стандартные CompactFlash. Следовательные цены на 128-Мб модули флэш-памяти лежат в пределах \$30...\$40 и при этом продолжают снижаться.



Если в ходе операций по тайному проникновению вы начали сталкиваться с картами флэш-памяти, содержимое которых требовалось скопировать на жесткий диск, подумайте о приобретении карманного устройства для считывания и записи флэш-карт компании Imation ([www.imation.com](http://www.imation.com)) FlashGo!. Портативное USB-устройство поддерживает форматы CompactFlash (типа 1 и 2), SmartMedia, Multimedia Memory Card и MemoryStick, а его стоимость составляет всего \$55. Последовательность операций при этом простейшая: вначале необходимо вставить карту памяти в устройство, затем подключить его к USB-порту и начать копирование файлов.

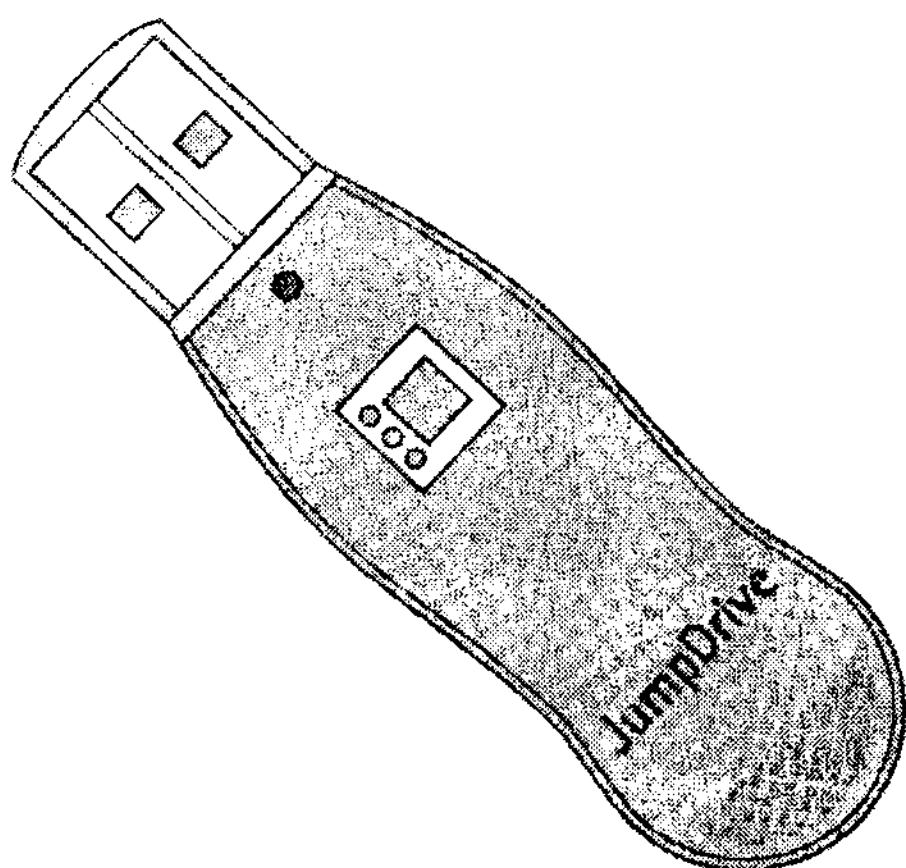
Еще одна новинка в области внешних устройств хранения информации на основе флэш-памяти – USB Flash Drive. Это миниатюрное устройство (оно незначительно превышает в размере ваш большой палец), которое подключается непосредственно к USB-порту, как будто материализовалось из фильмов о Джеймсе Бонде (рис. 7.1). В Windows Me, 2000, XP вам достаточно просто подключить устройство к порту и приступить к копированию файлов (для предыдущих версий Windows необходимо иметь с собой диск с драйверами).

Выпускаемые флэш-модули нередко имеют красочную расцветку, а некоторые модели вообще выглядят как обычный маркер или брелок для ключей. Благодаря своему виду и относительной новизне на рынке,

устройства могут быть вообще не замечены в случае вашей поимки. (Если вы человек творческий и умеете обращаться с миниатюрными устройствами, вы можете вынуть устройство флэш-памяти из корпуса и поместить его, к примеру, в толстый маркер, чтобы полностью сыграть роль шпиона.)

На подобных устройствах может храниться от 8 до 512 Мб информации, а их цена, зависящая в первую очередь от емкости, может колебаться от \$40 до \$260. Стандартная скорость передачи данных составляет около 1 Мб/с, в то же время некоторые новые модели с поддержкой USB 2.0 позволяют записывать данные со скоростью до 4,5 Мб/с.

Чтобы ознакомиться с полным перечнем существующих на рынке накопителей флэш-памяти, посетите веб-страницу в сети Интернет по адресу [www.everythingusb.com/hardware/Storage/USB\\_Flash\\_Drives.htm](http://www.everythingusb.com/hardware/Storage/USB_Flash_Drives.htm).



**Рис. 7.1.** Устройство считывания и записи флэш-памяти JumpDrive 2.0 Pro компании Lexar ([www.lexarmedia.com](http://www.lexarmedia.com)) объемом 256 Мб, поддерживающее скорость передачи данных 4,8 Мб/с. Чтобы приступить к работе с устройством, его необходимо подключить к USB-порту

## Жесткие диски

Первый жесткий диск появился еще в 1957 году в составе мэйнфрейма IBM (RAMAC 350). Он состоял из пятидесяти 24-дюймовых дисков, суммарная емкость которых составляла 5 Мб. Стоимость аренды этого жесткого диска равнялась \$35 000 в год. К концу же 2003 года широкое распространение получили жесткие диски объемом более 100 Гб, цена которых опустилась ниже порога в \$1 за 1 Гб.

## Шпионский инструментарий: нашествие MP3-плееров

В феврале 2002 года издание *Wired News* опубликовало статью об инциденте, произошедшем в компании CompUSA в Далласе, штат Техас. Тинэйджер, слушавший плеер iPod производства компании Apple (вспомните широкую рекламную кампанию плеера Sony WalkMan, с поддержкой файлов формата MP3, оцифрованных с аудиокомпакт-диска или загруженных из сети Интернет), был пойман с поличным в тот момент, когда он подключился к одному из компьютеров Mac в магазине. Заказчик застал подростка за копированием новой версии Microsoft Office для OS X на свой плеер iPod ([www.apple.com/ipod](http://www.apple.com/ipod)). Подключившись через порт FireWire, он скопировал все инсталляционные файлы (объемом в 200 Мб) на свой MP3-плеер менее чем за одну минуту.

Хотя в данном случае речь шла всего лишь о вопиющем случае компьютерного пиратства в сочетании с воровством, этот факт говорит о том, что данный плеер (комплектуемый памятью в 5, 10 и даже 20 Гб), который, если верить рекламе, позволяет скопировать объем данных, эквивалентный размеру компакт-диска за 15 секунд, вполне может использоваться в шпионских целях для копирования информации с компьютеров Mac или любых других персональных ЭВМ, с поддержкой интерфейса FireWire.

Существуют и другие продукты, которые умеют работать с любыми персональными компьютерами, например Creative Labs Nomad Jukebox Zen ([www.nomadworld.com/products/Jukebox\\_Zen/](http://www.nomadworld.com/products/Jukebox_Zen/)). Новейшие MP3-плееры, совместимые с операционной системой Windows, которые имеют функцию подключения к USB, отлично подходят на роль шпионского инструментария, а плееры Zen даже имеют встроенный разъем для микрофона, позволяющего записывать аудиоинформацию в цифровом виде.

Таким образом, MP3-плееры, которые можно подключить к USB-порту и которые поддерживают копирование файлов на плеер, идеально подойдут шпионам, чтобы выйти сухими из воды в случае поимки. «Кто, я? Да я просто убираю офис, слушая свою любимую музыку».

Создание дубликатов жесткого диска нашло широкое применение в ходе судебных расследований. Иногда необходимость дублирования содержимого одного жесткого диска на другой возникает и у шпионов, которым необходимо скопировать информацию на месте. Для этого нужно вскрыть компьютер, подключить пустой жесткий диск как подчиненный (slave), а затем загрузить компьютер с дискеты и запустить утилиту для

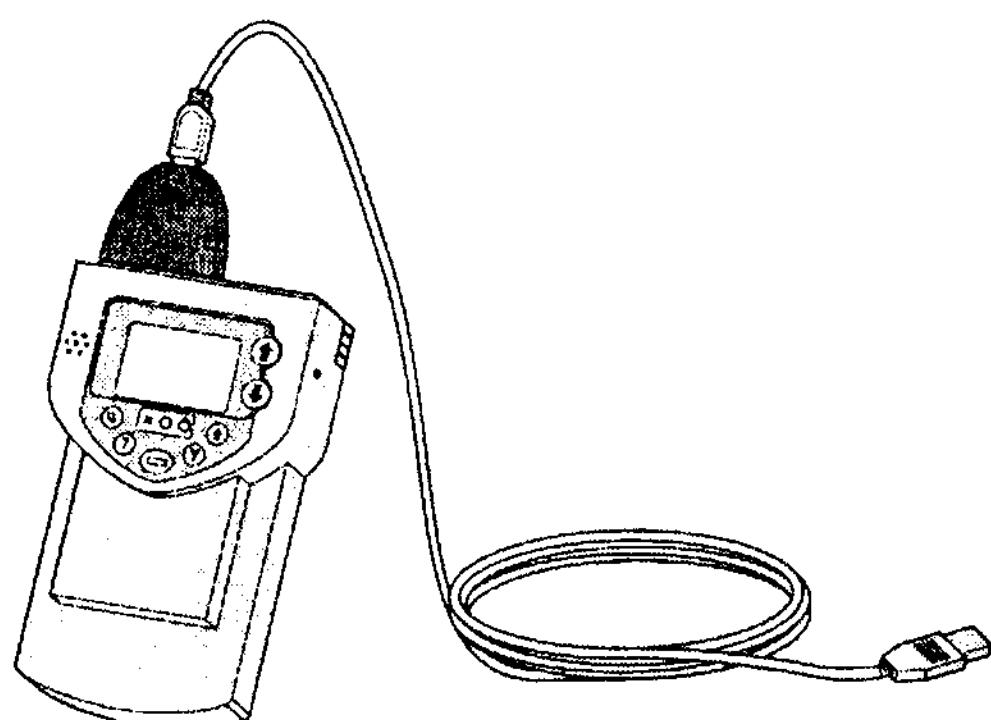
дублирования жестких дисков – при этом вам не придется волноваться по поводу входного пароля Windows. После завершения работы, верните компьютер в исходное состояние и отправляйтесь изучать дубликат жесткого диска в безопасное место.



Программное обеспечение, используемое судебными экспертами для дублирования содержимого жестких дисков, было рассмотрено в главе 5.

## Шпионский инструментарий: устройство для дублирования жестких дисков

Один из любимых инструментов ФБР (а также других правительственные служб, правоохранительных органов и разведывательных управлений) – устройство под названием Logicube SF-5000 (рис. 7.2). Чтобы скопировать содержимое одного жесткого диска на другой, вам понадобится только подключить диск-источник и пустой диск к этому устройству и запустить процесс копирования. Эти устройства активно используются ФБР в течение последних нескольких лет благодаря их скорости, мобильности и легкости применения. (Этот модуль отлично зарекомендовал себя при работе с IDE-устройствами, но он демонстрирует низкую скорость при работе со SCSI-накопителями.) Базовая цена этого устройства составляет \$1199 (стоимость полного набора составляет \$2249), а получить о нем более подробную информацию вы можете по адресу [www.logicube.com](http://www.logicube.com).



**Рис. 7.2.** Устройство для дублирования содержимого жестких дисков Logicube SF-5000 с разъемом USB для подключения к компьютеру; любимый инструмент агентов ФБР и других госслужб

К альтернативным устройствам для копирования содержимого жестких дисков, весьма популярным среди представителей правоохранительных органов (и других менее законных профессий), относятся:

- **Corporate Systems Portable Pro Drive.** Хотя устройство Logicube показало наилучшие скоростные характеристики при работе с IDE-устройствами, модуль от Corporate Systems хорошо зарекомендовал себя для ноутбуков. Не слишком компактный, поставляемый в огромном чемодане, он пользуется спросом среди компьютерных экспертов за счет своей привлекательной цены в \$995. Если вы хотите больше узнать об этом устройстве, посетите сайт компании Corporate Systems в Интернете по адресу [www.corpsys.com](http://www.corpsys.com).
- **Intelligent Computer Solutions Image Masster Solo-2.** Прибор под названием Image Masster Solo-2 представляет собой небольшое устройство, весьма напоминающее только что рассмотренный Logicube. Опыт применения устройства в полевых условиях показывает, что Solo-2 хорошо справляется с проблемой плохих секторов, что является главным препятствием для многих других устройств дублирования информации. Базовая цена модуля – \$1495. За дополнительной информацией обращайтесь на сайт [www.ics-iq.com](http://www.ics-iq.com).

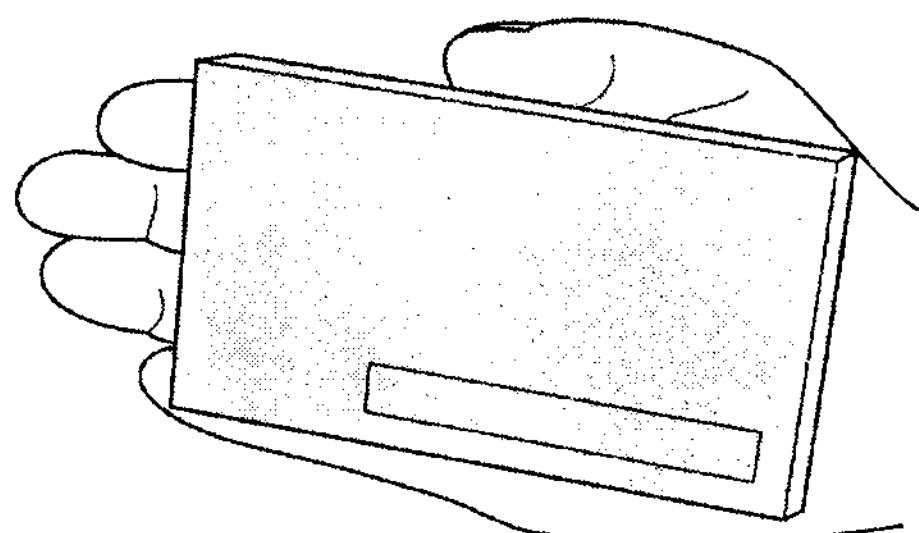
Хотя вышеперечисленные устройства отлично подходят для дублирования содержимого жестких дисков в полевых условиях, достичь подобных результатов вы сможете и с помощью обычного ноутбука и соответствующего программного обеспечения – Norton Ghost или утилиты dd в Linux.

Скорость передачи данных у традиционных жестких дисков, особенно у моделей со скоростью вращения шпинделя 7200 об/мин с включенным кэшированием данных, может достигать 100 Мб/с. Тем не менее при расчете времени, необходимого на выполнение операции, надо учитывать не только чистое время копирования данных, но и время, требуемое для вскрытия системного блока компьютера, установки вашего жесткого диска, а после завершения копирования – время на приведение компьютера в его исходное состояние. Если же вы стеснены во времени выполнения операции, вариант с использованием внутреннего жесткого диска вам не подойдет. В данной ситуации для скрытного копирования информации прекрасной альтернативой являются переносные внешние жесткие диски USB и диски Microdrive.

## Жесткие диски USB

Внешние жесткие диски, подключаемые к порту USB (или IEEE 1394), – отличный инструмент для копирования данных. Вместо того чтобы разбирать целевой компьютер и устанавливать в него второй жесткий диск, вам достаточно подключить внешний жесткий диск к USB-порту и начать копирование информации (хотя при этом скорость передачи данных окажется ниже, чем у IDE-устройства, из-за ограниченной максимальной пропускной способности универсальной последовательной шины USB). На рынке представлены два вида таких накопителей:

- **Стандартные.** Хотя эти жесткие диски достаточно мобильны для того, чтобы использовать их в целях шпионажа, они все равно не поместятся в карман (особенно с блоком питания переменного тока и шнуром). Стандартные внешние жесткие диски имеют объем от 20 Гб до 200 Гб, а цена их варьируется в пределах от \$100 до \$250.
- **Компактные.** Эти небольшие внешние носители легко помещаются в карман рубашки, позволяя хранить от 5 до 60 Гб данных (рис. 7.3). Их стоимость составляет от \$175 до \$400, а поскольку питаются они от шины USB, то и дополнительный внешний источник питания им не нужен.



**Рис. 7.3.** Внешний компактный жесткий диск Pockey DataStore ([www.rocketec.net](http://www.rocketec.net)), который помещается в карман и весит не более 5,5 унций\* отлично подходит для скрытого копирования больших объемов информации

\* Около 157 г. – Прим. перев.

## ДИСКИ MICRODRIVE

Если вам предстоит копировать информацию с ноутбука либо настольного компьютера, имеющего устройство чтения PC Card, подумайте над использованием дисков Microdrive. Microdrive представляет собой PC Card со встроенным однодюймовым жестким диском, на который можно записать 340 Мб, 500 Мб, 1 Гб или 4 Гб информации (в зависимости от конкретной модели). Эти диски могут подключаться к любым разъемам, совместимым с CompactFlash CF+ Type II или PC Card, и передавать данные на скорости 40...60 Мб/с. Диск объемом в 1 Гб на сегодняшний день стоит менее \$350. В конце 2002 года компания Hitachi приобрела заводы по выпуску жестких дисков у компании IBM и теперь является основным производителем и продавцом Microdrive. Если вы хотите больше узнать об этих продуктах, посетите веб-сайт [www.hgst.com/products/microdrive/index.html](http://www.hgst.com/products/microdrive/index.html).

## Системы резервного копирования на магнитной ленте

Системы резервного копирования пользуются популярностью во многих корпорациях, однако, несмотря на существование на рынке портативных вариантов исполнения таких устройств, они плохо подходят для целей шпионажа (разве что для резервирования данных в судебной лаборатории). Системы резервного копирования на магнитную ленту чрезвычайно медленны по сравнению с другими устройствами хранения и требуют частой замены кассеты с лентой. Поэтому, обнаружив на целевом компьютере установленную систему резервного копирования, лучше воспользуйтесь другими носителями для копирования файлов. Если вы обнаружили готовые ленты с резервными копиями информации и решили прихватить их с собой, обратите внимание на то, какое аппаратное и программное обеспечение использовалось для их создания, дабы в последствии не мучиться в догадках, пытаясь восстановить данные на своем рабочем месте.

## Альтернативные методы копирования данных

Не фиксируйте ваше внимание исключительно на использовании гибких дисков, CD, жестких дисков и внешних накопителей для копирования данных. Хороший шпион всегда ищет лучшее решение для каждого конкретного случая, и сейчас мы перечислим несколько альтернативных способов копирования, которые вам стоит рассмотреть.

## Передача данных по сети

Если целевой компьютер подключен к сети (например, Интернет), вы можете передавать данные на другой компьютер по сети вместо того, чтобы записывать информацию на локальный носитель. При этом необходимо учитывать следующие нюансы:

- Скорость передачи данных в этом случае полностью зависит от пропускной способности сетевого подключения. Чем меньше пропускная способность сети, тем больше вам придется ожидать загрузки информации.
- Все операции по передаче сетевых пакетов обычно заносятся в журнал (который впоследствии может быть просмотрен), поэтому в данном случае могут остаться следы ваших действий. По крайней мере, убедитесь, что сетевой IP-адрес, на который отсылаются данные, не выведет на вас.

Если обстоятельства складываются в пользу копирования информации по сети, вам доступны три способа решения поставленной задачи:

- **FTP, Telnet и SSH.** Если вы имеете доступ к учетной записи, поддерживающей протоколы FTP, Telnet и SSH, вы можете воспользоваться ею, чтобы скопировать локальные файлы на удаленный компьютер. (Вам необходимо иметь при себе соответствующие приложения на диске с утилитами.)
- **Электронная почта.** Если вы обладаете доступом к почтовому клиенту на целевом компьютере, вы можете просто переслать письмо с вложением на ваш ящик электронной почты. Этот способ подходит для отправки небольших по объему данных, поскольку при попытке передачи солидных объемов информации, вы можете запросто превысить лимит вашего почтового ящика.
- **NetCat.** Программа NetCat, сравниваемая по разнообразию возможностей со швейцарским складным ножом, представляет собой утилиту командной строки, которую обязан иметь в своем арсенале каждый шпион. Эта программа, разработанная Хоббитом (Hobbit) еще в 1995 году, позволяет сканировать порты, осуществлять копирование файлов, удаленно запускать команды и выполнять другие виды сетевых операций. Чтобы скопировать файлы с одного компьютера на другой, убедитесь, что программа NetCat запущена на получателе, затем запустите ее на отправителе, задайте IP-адрес и порт компьютера-получателя и приступайте собственно к копированию файлов. Различные версии свободно распространяемой утилиты под Unix и Windows вы можете найти в сети Интернет по адресу [www.ats-take.com/research/tools/network\\_utilities/](http://www.ats-take.com/research/tools/network_utilities/). (Существует также модифицированная версия NetCat под названием

Cryptcat, которая позволяет выполнять шифрование данных с помощью алгоритма Twofish; ее вы можете загрузить с веб-страницы [www.farm9.org/Cryptcat/GetCryptcat.php](http://www.farm9.org/Cryptcat/GetCryptcat.php).)

## Цифровые камеры

Любой компьютерный шпион обязан включить в свой арсенал цифровую камеру. Фото- и видеокамеры необходимы для фотосъемки или видеозаписи конфиденциальной информации, которая представлена в нецифровом формате и потому не может быть скопирована иным способом. Кроме того, камера обязательно понадобится вам для фотографирования обстановки в помещении, чтобы впоследствии вы могли расставить все вещи по своим местам.

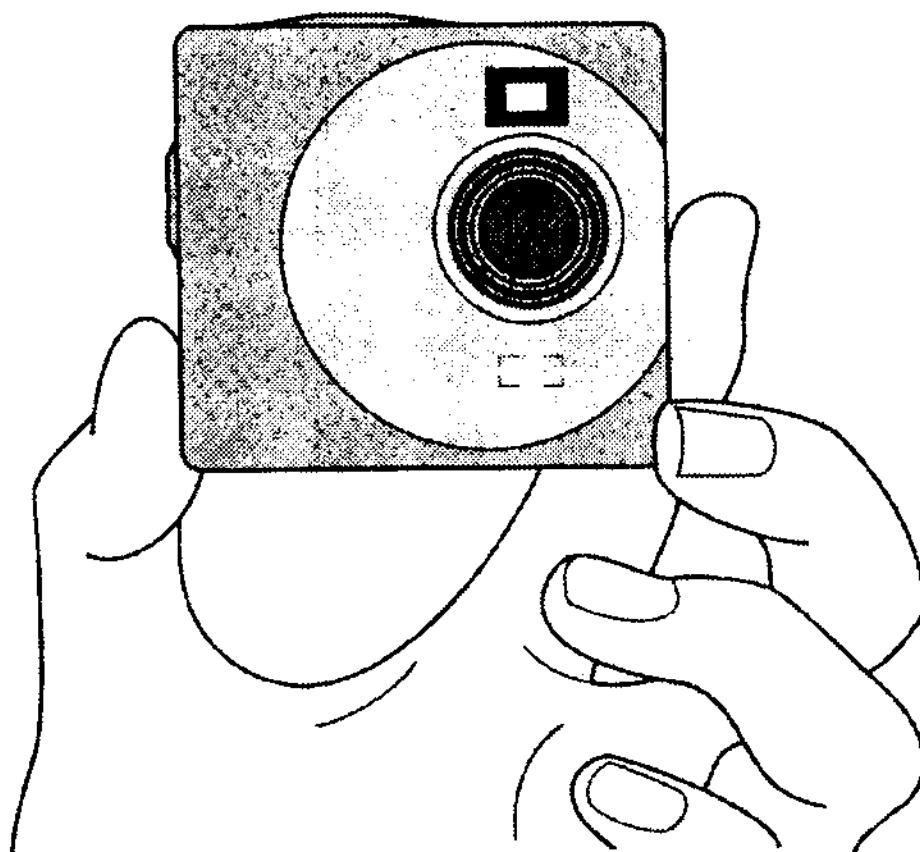
Идеальная шпионская камера для этих случаев – микрофотоаппарат Minox (более подробную информацию по нему вы можете получить на веб-сайте [www.minox-web.de](http://www.minox-web.de)). Крохотная 56-граммовая камера, делающая снимки на микропленку в формате 8×11 мм, используется многими разведывательными управлениями еще с 30-х годов прошлого века и по-прежнему не теряет своей популярности.

Фотоаппарат Minox является классикой жанра, но цифровая фототехника, за счет своей универсальности, на сегодняшний день намного лучше подходит для целей шпионажа. Конечно, вы можете использовать и традиционные полноформатные фотоаппараты, однако рекомендуем вам не обойти своим вниманием постоянно расширяющийся ассортимент миниатюрных камер, которые, несмотря на некоторые ограничения по качеству картинки и функциональности, выигрывают за счет своего размера. Такие цифровые фотоаппараты, как SiPix StyleCam Snap ([www.sipixdigital.com](http://www.sipixdigital.com); см. рис. 7.4) и Creative Labs Cardcam ([www.americas.creative.com](http://www.americas.creative.com)), легко умещаются на ладони, их легко спрятать, и при всем при этом их стоимость составляет около \$40 и \$80 соответственно. Конечно, у них отсутствуют LCD-дисплеи, вспышка, функции увеличения, да и фотографируют они с меньшей разрешающей способностью, чем более дорогие фотокамеры, но тем не менее им можно найти применение во многих шпионских задачах.

## Заключение

Существует множество способов копирования информации с целевого компьютера, причем одни способы являются более быстрыми, а другие более незаметными. Планируя операцию по копированию интересующей вас информации, вы в первую очередь должны продумать, сколько времени вы можете посвятить этому процессу. Исходя из временных ограничений, вы можете определить подходящие для данного случая носители информации и оценить, какой объем информации вы можете

успеть скопировать. Перед началом копирования данных в полевых условиях, будь то создание образа диска в экспертной лаборатории либо тайное копирование стратегического бизнес-плана конкурентов, попрактикуйтесь в использовании выбранных вами носителей и устройств хранения информации. Знакомство с процессом копирования информации на тот или иной носитель позволит вам узнать о возможных проблемах в процессе копирования и правильно оценить продолжительность операции.



**Рис. 7.4.** Недорогая цифровая фотокамера SiPix StyleCam Snap весом около 50 граммов, которую очень легко спрятать.

С другой стороны, обеспечение физической безопасности имеет ключевое значение для защиты от противозаконного копирования информации. Очевидно, что чем сложнее будет шпиону добраться до компьютера, тем выше ваши шансы на сохранность конфиденциальной информации. Если вы на стороне «хороших парней», то время работает на вас. Поскольку объем информации, который может скопировать злоумышленник, напрямую зависит от имеющегося в его распоряжении времени, то чем меньшими будут промежутки времени, в течение которых техника находится без присмотра, тем меньше успеет навредить вам шпион. Сигнализация, видеокамеры наблюдения и регулярно патрулирующие здание охранники уменьшают шансы злоумышленников на успех. Разумеется, время, необходимое на выполнение копирования, является дополнительной контрмерой, однако учтите, что для копирования нескольких наиболее важных документов с конфиденциальной информацией понадобятся считанные секунды. В этом случае на первый план выходит шифрование информации. Даже если потенциальному шпиону удастся скопировать данные, используемый вами стойкий алгоритм шифрования (и строгое соблюдение политики паролей) не позволят шпиону получить доступ к конфиденциальной информации.

## Глава 8

# Мониторинг клавиатуры

«Я никогда не печатаю на пишущей машинке, мой друг».

The Posies, «Farewell, Typewriter», Success

## Что такое keylogger

Keylogger, или средство мониторинга клавиатуры, – это такое программное или аппаратное обеспечение, которое позволяет запоминать последовательность нажатия клавиш. С его помощью, анализируя последовательность нажатия клавиш, можно узнать пароль, найти доказательства незаконной деятельности и получить конфиденциальную информацию, которую ее владельцы предпочли бы спрятать подальше от чужих глаз. Идея осуществления записи последовательности нажатых клавиш далеко не нова и, наверное, впервые была реализована на практике вскоре после того, как E. Remington & Sons продали в 1874 году первую пишущую машинку. Можно привести немало примеров известных в истории наблюдений за клавиатурой пишущих машинок и компьютеров:

- Для получения оттиска на бумаге в пишущих машинках используется красящая лента, и на ней остаются следы от всех напечатанных символов. Поэтому в начале XX века представители правоохранительных органов нередко занимались поиском в мусорных корзинах использованных лент из пишущих машинок. Даже в 1990-х ФБР воспользовалась кусочками ленты в качестве ключевых доказательств виновности российского двойного агента Элдрика Эймса.
- На обложке книги бывшего агента ЦРУ Филиппа Эйджи «Взгляд изнутри: дневник ЦРУ» приведена фотография переносной пишущей машинки фирмы Royal, к которой был подключен «жучок». В 1970-х предполагаемый «друг», также работавший на ЦРУ, одолжил Ажи эту пишущую машинку, благодаря чему ЦРУ могло следить за написанием его изобличительной книги.
- Популярность электрических пишущих машинок сыграла на руку шпионам, предоставив в их распоряжение источник энергии для подключения устройств наблюдения. Хотя первые модели электрических пишущих машинок появились еще в 1902

году (их выпустила фирма Blickensderfer), коммерческая популярность пришла к ним только в 20-х годах XX века. Современная пишущая машинка IBM Selectric, впервые представленная в 1960-м, стала весьма привлекательной для шпионажа за счет своего повсеместного распространения. Шпион мог легко подменить одну пишущую машинку другой, со встроенным «жучком», и секретарша даже не заметила бы разницы. (Подслушивающее устройство могло состоять из микрофона, позволяющего по звуку определять нажатую клавишу, либо электроники, записывающей нажатие той или иной клавиши. Затем миниатюрный передатчик отсыпал информацию на расположенный неподалеку радиоприемник, на котором последовательность нажатия клавиш сохранялась для последующего анализа.)

- В 1984 году офицеры контрразведки США обнаружили в России 13 пишущих машинок IBM, на которых были установлены подслушивающие устройства. Эти пишущие машинки использовались в секретных отделах посольства Соединенных Штатов в Москве и американского консульства в Ленинграде. «Жучки» передавали информацию русским на протяжении многих лет.

Но возвратимся ко дню сегодняшнему. Хотя часть методов, которые использовались для наблюдения за клавиатурой пишущих машинок, пойдут и для мониторинга компьютерных клавиатур, появилось новое, намного более простое в использовании аппаратное и программное обеспечение, предназначенное именно для компьютерной техники. Фактически в последние несколько лет наблюдалось взрывообразное появление новых, свободно распространяемых и коммерческих программ для мониторинга клавиатуры (keylogger) в сети Интернет. (Многие коммерческие производители keylogger имеют целевые веб-сайты, посвященные исключительно своим продуктам.)

Начальники используют подобное программное и аппаратное обеспечение, чтобы следить за своими подчиненными; супруги – для наблюдения друг за другом; родители – для наблюдения за детьми; и даже ФБР использует keylogger-модули, чтобы следить за гангстерами. Если шпион имеет физический доступ к компьютеру, keylogger является идеальным инструментом для достижения его целей.

## Шпионская тактика

Готовы ли вы вновь примерить на себя личину шпиона? Отлично, тогда программа keylogger станет эффективным средством в вашем наборе инструментов. Использовать keylogger можно двумя способами:

- **Локально.** Если вы обладаете физическим доступом к целевому компьютеру, вы без труда сможете установить подслушивающее аппаратное или программное обеспечение. Предварительно убедитесь, что у вас будет достаточно времени для работы с

компьютером. Для установки программы keylogger вам может понадобиться до пяти минут, тогда как установка аппаратного модуля keylogger обычно занимает менее минуты.

- **Удаленно.** Если вы лишиены физического доступа к компьютеру, вы можете отослать на этот компьютер электронную почту с «тロянским конем», содержащим программу keylogger. Существует огромное количество приложений – троянских коней, в состав которых входят keylogger-программы, а также версии keylogger, специально написанные для проведения атак подобных видов.



Более подробно о троянских конях и других приложениях, предусматривающих возможность удаленного управления, вы узнаете из главы 9.

После того, как вы установили программу мониторинга клавиатуры, которая будет отслеживать и сохранять в файл последовательность нажатия клавиш, вам необходимо получить доступ к этой информации. Для этого, в зависимости от вида используемого вами модуля keylogger, вам понадобится либо физический доступ к компьютеру, либо при использовании «продвинутых» программ мониторинга клавиатуры результаты могут отсылаться вам по почте. Некоторые keylogger-программы позволяют открывать порты на целевой машине, чтобы напрямую обращаться к компьютеру, если вы знаете его IP-адрес. Используя программу мониторинга клавиатуры, позволяющую удаленно получать собранную информацию, позаботьтесь о том, чтобы хорошо замести свои следы. Неразумно будет настроить отсылку протоколов работы keylogger на ваш персональный почтовый ящик либо обнаружить себя (через свой IP-адрес), удаленно подключившись к целевому компьютеру, чтобы извлечь файл, хранящий последовательность нажатых клавиш.

## Использование слабых мест

Любой компьютер, в котором для ввода информации используется клавиатура, уязвим для подобного рода атак. Программы keylogger разработаны практически для любых операционных систем, о которых вы только могли слышать. И точно так же, как пользователи используют клавиатуру для набора текстов, вы можете использовать программы мониторинга клавиатуры, чтобы шпионить за ними. (Перед тем как задавать вопрос по поводу программного обеспечения для распознавания голоса, воспользуйтесь традиционным микрофоном для записи голосовой информации. Об устройствах аудионаблюдения мы поговорим в главе 12.)

Итак, рассмотрим алгоритм работы аппаратных и программных средств мониторинга клавиатуры и обсудим их основные возможности.

## ПРОГРАММНЫЕ СРЕДСТВА KEYLOGGER

Программные средства keylogger реализуются элементарно – программист пишет код, перехватывающий нажатие любой клавиши и записывающий код этой клавиши в файл журнала. Для создания программ мониторинга клавиатуры используется три подхода:

- **Низкоуровневый.** Такие keylogger-программы пишутся на ассемблере. Принцип их работы основан на использовании ловушек (интерфейсов, позволяющих программисту добавлять пользовательский код) в обработчике прерываний нажатых клавиш (аппаратных сигналов, сообщающих о состоянии клавиатуры) и передаче событий для обработки пользовательским кодом. Потом код каждой нажатой клавиши записывается в журнал, после чего управление возвращается оригинальному обработчику.
- **Уровень API операционной системы.** Появление такой операционной системы, как Windows, значительно упростило разработку программ мониторинга клавиатуры. Современный программист, не нуждаясь в глубоких знаниях ассемблера и внутренней архитектуры системы, легко может написать программу-keylogger практически на любом языке программирования высокого уровня. (В сети Интернет вы можете найти немало текстов исходных кодов на Visual Basic, в частности одна из популярных коммерческих программ мониторинга клавиатуры написана на VB.) Программа, работающая в фоновом режиме, может регулярно проверять состояние отдельных клавиш при помощи вызова Windows API-функции GetAsyncKeyState или GetKeyState. При нажатии клавиши ее код будет сохранен в журнале. В таких программах может также вызываться, к примеру, Windows API-функция SetWindowsHookEx для перехвата системных сообщений и вызова специальных обработчиков клавиатуры.
- **Уровень драйверов устройств.** Программы-keylogger такого типа создаются в виде драйверов устройств и поэтому являются наиболее незаметными из всех, поскольку работают на уровне самой операционной системы Windows. Для операционных систем Windows 9x/Ме программы мониторинга клавиатуры создаются в виде драйверов виртуальных устройств (vxd). Для компьютеров под управлением операционных систем Windows 2000/XP keylogger-программы создаются в виде драйверов WDM (Windows Driver Model). Однако количество подобных программ мониторинга клавиатуры невелико, что обусловлено относительной сложностью написания драйверов по сравнению с использованием ловушек API.

Естественно, большинство шпионов не желают, чтобы их потенциальные жертвы знали о ведущемся за ними наблюдении с помощью программ мониторинга клавиатуры, однако есть keylogger-программы, которые легко обнаружить. В хорошей keylogger-программе используются различные приемы, для того чтобы скрыть от пользователя работу фонового процесса. Наиболее хитрыми и распространенными способами защиты от обнаружения являются:

- **Скрытие процесса от Диспетчера задач.** В Windows 9x/Me в библиотеке kernel32.dll существует специальная функция RegisterServiceProcess. Как следует из названия функции, она регистрирует процесс в качестве службы, что предохраняет процесс от автоматического закрытия при завершении сеанса работы пользователя и скрывает его от Диспетчера задач. Такая тактика широко применяется в keylogger-программах, предназначенных для работы под операционными системами Windows 9x/Me (из-за различий в архитектуре операционных систем, эти скрытые процессы видны в Windows NT/2000/XP). Те же программы мониторинга клавиатуры, которые были установлены в качестве драйверов устройств, не видны в Диспетчере задач и других программах просмотра процессов ни в одной ОС).
- **Использование ложного имени процесса.** Очевидно, что, назвав процесс EvilKeylogger, вы привлечете к нему внимание пользователя в первую очередь. Скрытым процессам, как и файлам keylogger-программы, обычно присваиваются имена, не вызывающие подозрений.
- **Использование нейтральных имен файлов и ключей реестра.** Файлы keylogger-программы должны иметь малопонятные имена, которые бы усыпили бдительность пользователя, заставив его принять эти файлы как часть операционной системы. Некоторые программы мониторинга клавиатуры во избежание собственного обнаружения даже переименовывают файлы после своего запуска.
- **Скрытие файлов журнала.** Нередко к файлам журнала, хранящим последовательность нажатых клавиш, применяются определенные алгоритмы шифрования, защищающие информацию от случайного прочтения пользователем. Помимо шифрования журнала, используются приемы по присвоению файлам ложных расширений, например, текстовым файлам журнала может быть присвоено расширение .osx, заставляя пользователей думать, что перед ними пользовательский элемент управления OLE. Некоторые keylogger-программы также изменяют дату/время создания файлов, чтобы их нельзя было обнаружить среди свежих созданных/модифицированных файлов.

Насколько незаметная программа мониторинга клавиатуры нужна именно вам, следует решать, исходя из поставленных целей. Для опытного и подозрительного клиента необходимо найти как можно более незаметную версию keylogger-программы. Для членов семьи, не сведущих в вопросах компьютерной безопасности, наоборот, подойдет простейшая программка. Коммерческие программы мониторинга клавиатуры, как правило, являются менее заметными, чем их свободно распространяемые в Интернете аналоги.

## ДОСТУПНОСТЬ KEYLOGGER-ПРОГРАММЫ

Хотя программы мониторинга клавиатуры предназначены для выполнения тайных действий на компьютерной технике, их широкая доступность не является секретом. Эти шпионские инструменты подробно описываются во множестве печатных и электронных источников, а коммерческие версии активно борются за место на рынке. Чтобы загрузить программу мониторинга клавиатуры, достаточно щелчка мышки. Поиск по ключевому слову keylogger на поисковом сервере Google возвращает ссылки на более чем 210 тысяч страниц, включая четыре спонсорских ссылки на коммерческие продукты. В конце 2002 года на некоторых шпионских веб-сайтах было перечислено более 250 коммерческих и свободно распространяемых программ для мониторинга клавиатуры. В рекламе коммерческой утилиты SpyCop, предназначеннай для обнаружения установленных в системе keylogger-программ, анонсировано распознавание более 300 различных программ мониторинга клавиатуры. Подобно вирусам, новые программы мониторинга клавиатуры появляются чуть ли не каждый день, не в последнюю очередь благодаря общедоступности исходного кода и разработке новых методов скрытой установки программ, не позволяющих жертве обнаружить их присутствие.

## НЕ ТОЛЬКО КЛАВИАТУРА – KEYLOGGER С РАСШИРЕННЫМИ ВОЗМОЖНОСТЯМИ

Первые программы мониторинга клавиатуры решали задачи, соответствующие названию, – они сохраняли последовательность нажатия клавиш, и ничего более. Современные версии таких программ, в особенности коммерческих, позволяют выполнять целый ряд других шпионских функций помимо простого сохранения в файл последовательности нажатых клавиш. Программы мониторинга клавиатуры, помимо своей основной задачи, могут выполнять следующие функции:

- **Запись содержимого экрана.** Некоторые программы в целях обеспечения безопасности используют так называемую виртуальную клавиатуру для защиты от программ мониторинга клавиатуры (изображение клавиатуры появляется на экране монитора – а для набора текста необходимо воспользоваться мышью). Но даже такую защиту позволяют преодолеть специальные keylogger-программы, умеющие периодически снимать копии экрана.

## Тактика: не только пароли

При использовании keylogger-программы не сосредотачивайте свое внимание исключительно на поиске паролей, коммерческих тайн либо доказательств аморальных действий. Информация, полученная в результате работы keylogger в сочетании с приемами социотехники, может применяться для получения доступа к другой информации. К примеру, вы перехватили содержимое послания электронной почты от вице-президента Фрэнка Джордана к инженеру Карле Найт. Они обсуждали возможные характеристики готовящегося к выпуску нового пылесоса ХР-9000. Что нам это дает? Зная имя инженера и некоторые подробности дела, мы можем вызвать этого инженера и, заявив, что мы от Фрэнка Джордана, выяснить дополнительную информацию по товару ХР-9000.

- **Сохранение содержимого буфера обмена.** Любой текст, помещаемый в буфер обмена, записывается. Открыв текстовый файл, в котором хранится имя учетной записи и пароль, и скопировав эту информацию в поля ввода, можно обмануть простейший keylogger, поскольку в этом процессе символные клавиши не нажимаются. Если же программа мониторинга клавиатуры будет также следить за содержимым буфера обмена, интересующая шпиона информация все равно будет записана.
- **Запись содержимого текстовых окон.** Иногда возникает необходимость проследить не только за текстом, который набирает пользователь. Например, в случае обмена мгновенными сообщениями, вас наверняка заинтересует целостная картина переписки. Некоторые программы мониторинга позволяют целиком записывать содержимое текстовых окон.
- **Передача изображения с веб-камеры.** Если к вашему компьютеру подключена веб-камера, получаемый с нее видеосигнал может быть перехвачен и сохранен. В результате некто за тысячи километров от вас сможет без вашего ведома наблюдать за вами или за тем, куда указывает ваша веб-камера.
- **Запись в журнал файловой активности.** Каждый раз при копировании, переименовании, переносе либо удалении файла программа будет записывать информацию о ваших действиях в журнал. На практике эта функция весьма полезна для сбора доказательств.
- **Сохранение списка посещенных веб-страниц.** Вместо поиска интернет-адресов среди тысяч нажатых символов, некоторые keylogger-программы позволяют сразу сохранять запрошенные URL в виде списка веб-сайтов.

- **Генерация отчетов.** Большинство коммерческих keylogger-программ позволяют сохранять все найденные доказательства в удобном для чтения формате, который впоследствии легко можно импортировать в таблицу или базу данных.
- **Удаленный доступ к информации.** Некоторые программы мониторинга клавиатуры могут отсылать собранную информацию по электронной почте на заданный шпионом почтовый ящик, другие же позволяют получать непосредственный доступ к компьютеру по локальной сети или через Интернет.

### Разоблачения: Никодермо Скарфо-младший

В январе 1999 года в Нью-Джерси агенты ФБР тайно проникли в деловой офис Никодермо Скарфо, сына гангстера Скарфо по кличке Маленький Никки, отбывающего наказание в тюрьме в Филадельфии. Вооружившись ордером на обыск для копирования информации с компьютера, федеральные агенты нашли зашифрованную информацию в одном из файлов под названием Factors, для защиты которого была использована популярная утилита PGP.

Суд США выдал ФБР другой ордер для тайной установки keylogger-программы на компьютер подозреваемого, чтобы выведать пароль для расшифровки файла, в котором, по подозрениям ФБР, содержалась информация о кредитах и закладах. Агенты ФБР повторно заинтересовались коммерческой деятельностью Скарфо в мае 1999-го и установили keylogger-программу на его компьютер. Эта программа, проработав в течение 14 дней, успешно записала используемый Скарфо пароль. Проблема возникла из-за того, что этот пароль не подходил к тому файлу, который агенты ФБР переписали ранее, однако агенты нашли новую версию файла, действительно зашифрованную с помощью этого пароля, получив таким образом доступ к нужным им доказательствам. Дело Скарфо было передано в суд, но на этом история не закончилась.

Адвокат защиты Скарфо потребовал сообщить подробности использования keylogger программы. ФБР же отказалось от комментариев, аргументируя это угрозой национальной безопасности. Неожиданно это дело привлекло к себе общенаученное внимание в контексте возникшего вопроса нарушения прав на неприкосновенность частной жизни и полномочий правоохранительных органов на использование секретных шпионских технологий. В данном случае судья встал на сторону правительства, заявив, что данная технология не может быть разглашена широкой общественности, а сам Скарфо был признан виновным весной 2002 года.

В конце концов, ФБР письменно обнародовало некоторую информацию по используемой keylogger-программе, употребив термин KLS (Key Logger System – Система протоколирования клавиатуры).

- Система KLS была разработана в ФБР и представляла собой пример скоординированной работы нескольких компонентов (программного и аппаратного обеспечения, а также аппаратно реализованного программного обеспечения).
- Система KLS не выполняла запись последовательности нажатия клавиш во время использования модема (Скарфо пользовался услугами America Online). Это связано с тем, что при использовании модема компьютер приравнивается к электронному средству связи, что требует наличия дополнительного ордера на прослушивание линий связи.
- Похоже, что ФБР обошла это ограничение, анализируя содержимое окон активных процессов и записывая нажатия клавиш только в тех программах, которые не взаимодействовали с модемом. Создается впечатление, что система KLS в фоновом режиме осуществляла поиск активного окна PGP и только тогда начинала записывать последовательность нажатия клавиш.
- Для анализа собранной системой KLS информации федеральным агентам нужен был физический доступ к компьютеру, и с этой целью ФБР провело пять тайных проникновений в офис Скарфо. Во время четвертого рейда состояние компьютера было описано как «неработающий или отсутствующий». (Это любопытное заявление породило подозрение: а не ноутбук ли Скарфо был под наблюдением? Дело в том, что Скарфо брал ноутбук с собой на празднование Хэллоуина в 1999 году, проведя в ресторане как раз ту ночь, когда в его офис вновь было совершено проникновение. В одном из телефонных разговоров, записанных еще в начале расследования по делу Скарфо, им была произнесена следующая речь: «У меня в руках чудовище. В нем есть встроенный DVD, 128 мегабайт памяти, Pentium III, 450..., 19-дюймовый монитор и звук Digital Surround».)

Немало слухов ходило вокруг системы KLS, однако до сегодняшнего дня никакой конкретной информации о том, что собой представляет эта система, так и не стало известно широкой общественности.

На случай, если когда-нибудь дело дойдет до выхода шпионской версии игры Trivial Pursuit\*, постарайтесь запомнить, что паролем Скарфо в PGP был «nds09813-050» – номер, под которым содержался отец Скарфо в федеральной тюрьме.

\*

Или в русском варианте «Счастливый случай». – Прим. перев.

Когда дело доходит до выбора keylogger-программы с расширенными возможностями, прежде всего вам следует определить, какие действия пользователя на компьютере вы хотите отслеживать. Не покупайтесь на яркую рекламу «суперпрограммы», если от keylogger-программы вам нужна только запись последовательности нажатия клавиш. В большинстве случаев вы не воспользуетесь дополнительными возможностями такой программы, поэтому лучше сразу выбирать утилиты, не перегруженные ненужными расширениями.

## АППАРАТНЫЕ KEYLOGGER-МОДУЛИ И ПРИНЦИПЫ ИХ РАБОТЫ

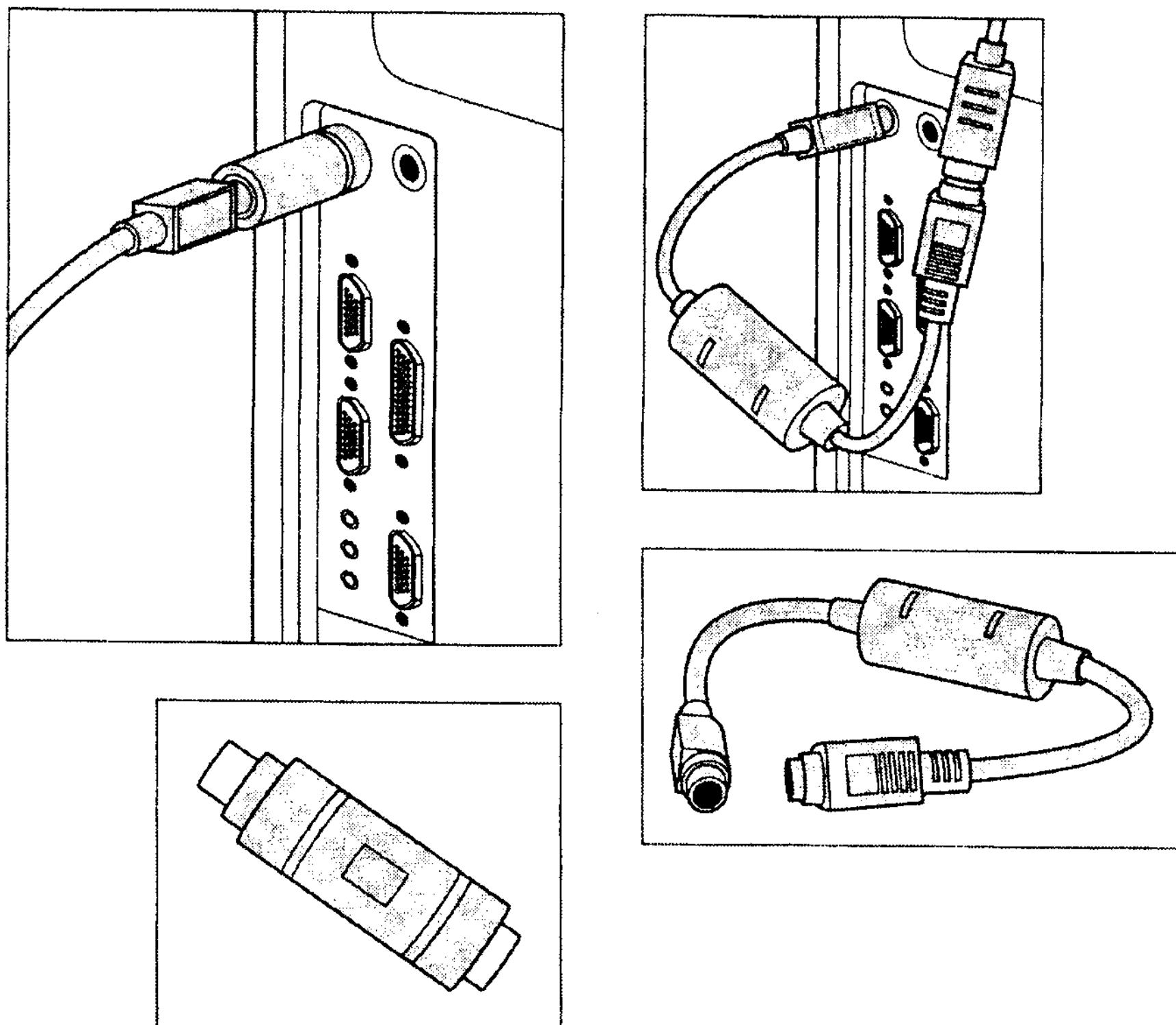
Помимо программных существуют также аппаратные средства мониторинга клавиатуры. Такие устройства состоят из электронной микросхемы, в которую записываются нажатия клавиш по мере передачи сигнала от клавиатуры к ее контроллеру (два подобных устройства изображены на рис. 8.1). Чтобы воспользоваться данным устройством, его необходимо подключить в качестве переходника. Все действия осуществляются самим устройством, и для его работы не требуется дополнительная установка какого-либо программного обеспечения (обычно подобные устройства легко обнаружить, поскольку они явным образом подключены к порту компьютера).

Существует две разновидности коммерческих аппаратных средств мониторинга клавиатуры:

- **Внешние.** Внешние keylogger-модули подключаются к компьютерному порту, к которому подключается сама клавиатура. В этом случае кабель клавиатуры вставляется в keylogger. Подобный keylogger выглядит как дополнительный переходник или кабель с согласующим электронным фильтром (см. рис. 8.1).
- **Внутренние.** Внутренние keylogger-модули обычно встраивают-ся в саму клавиатуру. Обнаружить такое устройство очень сложно, если только вы специально не откроете клавиатуру, зная, что искать.

Аппаратные keylogger-модули, как правило, обладают встроенной памятью для записи последовательности нажатых клавиш. При переполнении памяти выполняется перезапись информации, начиная с наиболее старых данных.

Для управления аппаратным keylogger-модулем необходимо набрать пароль в окне любого текстового редактора. Поскольку микросхема осуществляет постоянную запись нажатий клавиш, после распознания пользовательского пароля среди последовательности символов, записанные данные передаются в текстовый процессор, в котором выводится текстовое меню. Выбрав в этом меню соответствующую опцию, вы сможете просмотреть записанные нажатия клавиш, сменить пароль, выполнить настройку модуля (рис. 8.2).



**Рис. 8.1.** Оборудование для мониторинга клавиатуры (KeyKatcher и KeyGhost). Если вы заметите, что к порту клавиатуры вашего компьютера подключены похожие устройства, не сомневайтесь: за вами следят

Для просмотра зарегистрированных данных не нужен доступ к компьютеру подозреваемого. Просто отключите устройство от компьютера, за которым велось наблюдение, а затем подключите его к своему компьютеру в безопасном месте, чтобы изучить собранную информацию.

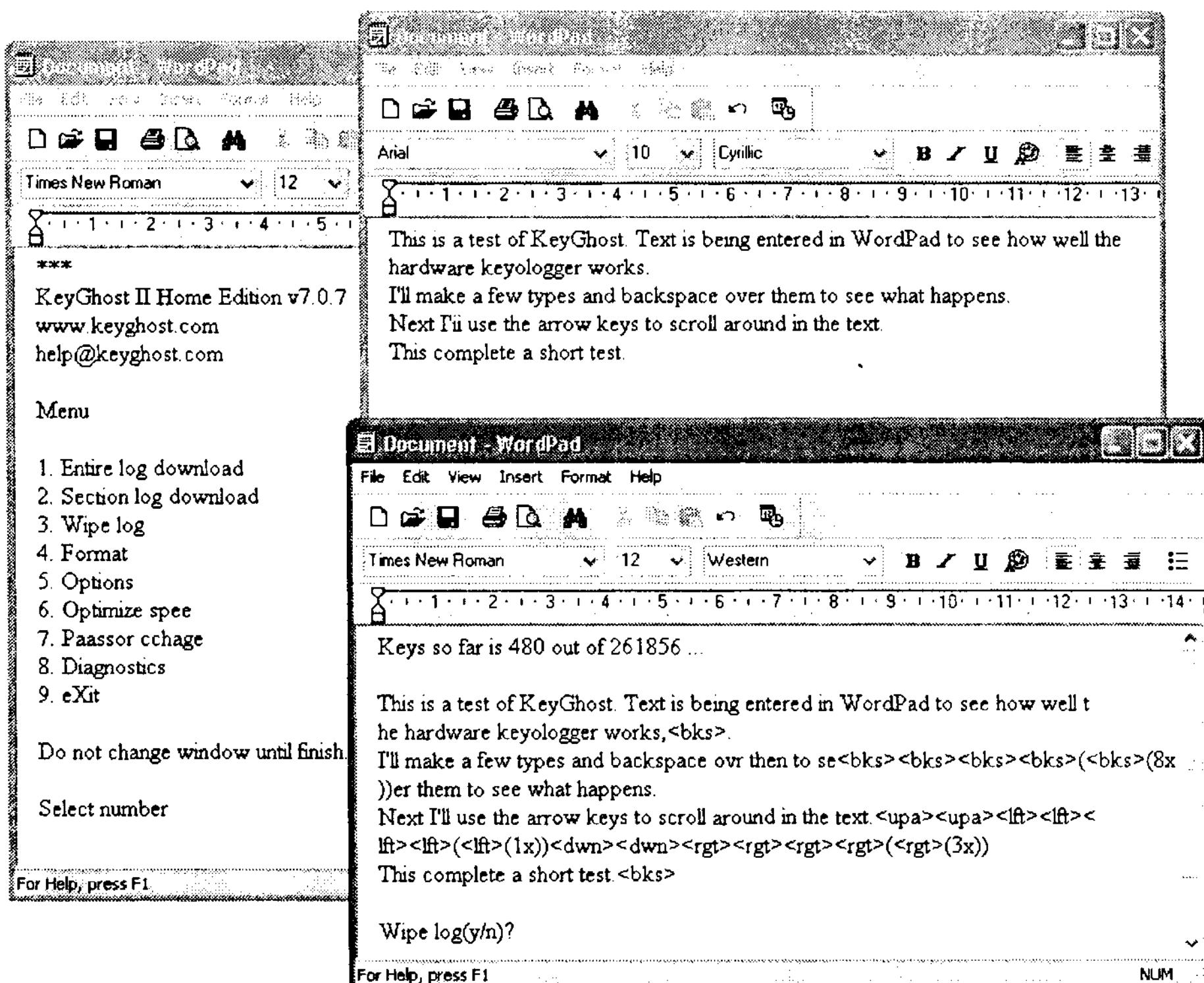
## «ЗА» И «ПРОТИВ» ИСПОЛЬЗОВАНИЯ АППАРАТНЫХ KEYLOGGER

У любых средств мониторинга клавиатуры, аппаратных или программных, имеются свои преимущества и недостатки. Поэтому, прежде чем принять решение, какое средство лучше использовать, вы должны выяснить сильные и слабые стороны каждого типа устройств.

**ПРЕИМУЩЕСТВА АППАРАТНЫХ СРЕДСТВ МОНИТОРИНГА КЛАВИАТУРЫ.** Аппаратные средства мониторинга клавиатуры обладают целым рядом преимуществ по сравнению со своими программными аналогами:

- Их невозможно обнаружить при помощи программного обеспечения. Стандартные приемы по обнаружению программных

keylogger-модулей не подходят для аппаратных средств мониторинга клавиатуры, поскольку в систему не устанавливаются файлы, не выполняются дополнительные процессы на уровне операционной системы и не сохраняются файлы журнала.



**Рис. 8.2.** Слева меню для обработки данных, полученных в результате работы устройства KeyGhost, которое отображается в текстовом редакторе. В верхнем окне показан текст, набранный пользователем в редакторе, а в нижнем окне – данные, записанные аппаратным keylogger-модулем, включая нажатие клавиши Backspace и стрелок

- **Аппаратные средства мониторинга клавиатуры легко и быстро устанавливаются.** Вам нужно вставить keylogger-модуль в порт клавиатуры, а затем подключить к нему саму клавиатуру. Вам даже не понадобится включать компьютер, для того чтобы установить keylogger, что весьма удобно, если опытный пользователь защитил свой компьютер при помощи трудно угадываемого пароля в BIOS.
- **Аппаратные keylogger-модули не привязаны к виду операционной системы на платформах фирмы Intel.** То есть ваше устройство будет работать и под DOS, и под Windows 9x/Me/

2k/XP, Linux, и под любой другой системой, которая может быть запущена на вашем персональном компьютере. Подобные устройства позволяют даже записывать клавиши, нажимаемые при входе в BIOS Setup.

- Аппаратным keylogger-модулям не нужны дополнительные источники питания, им достаточно питания от порта клавиатуры.

**НЕДОСТАТКИ АППАРАТНЫХ СРЕДСТВ МОНИТОРИНГА КЛАВИАТУРЫ.** Хотя применение аппаратных keylogger-модулей выглядит весьма привлекательно, с их использованием связаны некоторые ограничения:

- Вам необходим физический доступ к компьютеру. Установка некоторых программных средств мониторинга клавиатуры при удаленной атаке представляет собой меньший риск обнаружения.
- Аппаратные keylogger-модули стоят в 2...6 раз дороже своих программных аналогов. Тем не менее их нельзя отнести к предметам роскоши, поскольку стоимость большинства устройств не превышает \$300.
- Возможности аппаратных keylogger-модулей ограничены записью нажатий клавиш, в отличие от некоторых усовершенствованных программных средств мониторинга клавиатуры, с помощью которых вы можете записывать даже движения мыши и нажатия ее кнопок, а также другую подобную информацию.
- Если не принимать в расчет аппаратных keylogger-устройств, встраиваемых внутрь клавиатуры, такие модули более заметны, чем их программные собратья. Сообразительный пользователь может задуматься, почему это вдруг к порту клавиатуры подключен какой-то дополнительный переходник. Хотя обычно аппаратные keylogger-модули исполняются в виде стандартного фильтра или переходника, они сразу же возбудят подозрения пользователя, знающего, что искать.
- Вы не сможете автоматически отсылать собранную с помощью аппаратных средств мониторинга клавиатуры информацию, например, по сети. Для этого вам придется, опять-таки, написать специальную программу, которая бы взаимодействовала с аппаратным keylogger-модулем и могла считывать данные из памяти keylogger, а затем тайно отправлять их адресату.
- Имеющиеся на сегодняшний день аппаратные средства мониторинга клавиатуры не позволяют работать с ноутбуками. Согласитесь, это существенный недостаток, если вашими основными объектами шпионажа в первую очередь являются путешествующие бизнесмены.

- Ни одно из представленных в данный момент на рынке средств мониторинга клавиатуры не позволяет работать с клавиатурами USB. Существующие устройства подходят только для клавиатур PS/2 или AT. Можно предположить, что правительство и хорошо финансируемые шпионские организации имеют доступ к keylogger-модулям для клавиатур USB, однако пока такие устройства недоступны широкой публике. Скорее всего, следует ожидать появления коммерческих средств мониторинга USB-клавиатур на рынке в ближайшие годы.

## Средства мониторинга клавиатуры

Теперь, когда вы имеете базовые знания о keylogger-модулях, давайте рассмотрим примеры конкретных программных и аппаратных средств мониторинга клавиатуры, используемых в целях компьютерного шпионажа. В принципе средства мониторинга клавиатуры – небольшая расходная статья для людей, занимающихся компьютерным шпионажем. Вам наверняка захочется приобрести несколько типов keylogger-модулей для решения своих специфических задач.



Более длинный перечень коммерческих, свободно распространяемых и условно бесплатных программных «keylogger» вы можете найти на официальном веб-сайте данной книги: [www.wiley.com/combooks/mcnamara](http://www.wiley.com/combooks/mcnamara).

### ПРОГРАММНЫЕ KEYLOGGER-МОДУЛИ

На просторах сети Интернет можно найти столько различных программ мониторинга клавиатуры, что, вероятно, понадобится отдельная книга, только чтобы их всех описать (причем такая книга покажется довольно скучной для всех, кроме профессиональных шпионов). В данном параграфе мы расскажем вам о наиболее известных и популярных keylogger-программах. В ассортименте крупных производителей программ мониторинга клавиатуры обычно имеются различные версии наблюдательного ПО: от утилит с ограниченными возможностями, предназначенных для домашнего использования, до профессиональных версий, позволяющих выполнять, к примеру, удаленную отправку данных. Для большинства коммерческих программ доступны бесплатные оценочные версии, с помощью которых можно убедиться, соответствует ли программа вашим нуждам (воспользовавшись описанными ниже контрмерами, вы можете проверить, сумеет ли потенциальная жертва обнаружить ведущееся за ней наблюдение).

**Spector Professional Edition.** Эта программа от компании SpectorSoft находится на первом месте по популярности среди программных keylogger-модулей (что любопытно, программный код данной утилиты частично основан на коде известного троянского коня Netbus). Программа позволяет записывать последовательность нажатия клавиш, электронную

переписку, мгновенные сообщения, а также тайно отправлять отчеты по электронной почте каждые полчаса. Некоторые пользователи жалуются на то, что копия зашифрованных данных отсылается на сайт компании SpectorSoft. Представители компании объясняют это необходимостью работы их системы предупреждения по электронной почте, однако такая пересылка данных третьей стороне вполне может смутить шпионов-параноиков. Стоимость обеих программ (Spector Professional Edition и eBlaster) составляет \$99, а найти их вы сможете на сайте компании [www.spectorsoft.com](http://www.spectorsoft.com).

**Invisible Keylogger Stealth (IKS).** Как следует из названия продукта (программа-невидимка для мониторинга клавиатуры), IKS является одной из наиболее скрытных коммерческих keylogger-утилит. Данная программа реализована в виде драйвера устройства, причем для различных версий операционной системы Windows доступны различные версии keylogger. В отличие от некоторых других keylogger-программ, реализованных по принципу «все в одном флаконе», программа IKS предназначена исключительно для мониторинга клавиатуры. Для просмотра файлов журнала и тайной отправки результатов мониторинга по почте существуют отдельные утилиты. IKS относится к немногим keylogger-модулям, позволяющим осуществлять запись нажатых клавиш в диалоговом окне входа Windows 2000/XP, вызываемом по нажатию клавиш Ctrl+Alt+Del. Кроме того, компания-производитель предлагает пользователям самостоятельно скомпилировать немного модифицированные версии данного продукта, чтобы обмануть программы обнаружения keylogger-модулей, которые ищут файлы определенного размера или двоичную строку сигнатуры, характерную только для файлов IKS. Версия IKS под Windows 2000/XP стоит \$99, а заказать ее вы можете на сайте [www.amecis-co.com](http://www.amecis-co.com). Приведем некоторые ссылки на независимые детальные обзоры по программам мониторинга клавиатуры:

- В июле 2001 Национальный консорциум по юридической информации и статистике ([www.search.org](http://www.search.org)) опубликовал обзор коммерческих программ мониторинга клавиатуры, предназначенный в помощь должностным лицам, осуществляющим надзор за условно осужденными, чтобы те могли выбрать оптимальную утилиту для наблюдения за своими подопечными. PDF-версия документа ранее находилась на веб-сайте организации, однако теперь почему-то недоступна (добавьте еще одно «за» к своей теории заговоров). Список наиболее популярных утилит вы можете сформировать самостоятельно в виде HTML-страницы, сохранив результаты запроса «Desktop Monitoring and Surveillance Software» («Наблюдательное ПО») на каком-нибудь поисковом сервере.
- Журнал *PC Magazine* опубликовал обзор коммерческих программ мониторинга клавиатуры в июле 2002 года, сейчас найти его вы можете на официальном сайте журнала [www.pcmag.com/article2/0,4149,272723,00.asp](http://www.pcmag.com/article2/0,4149,272723,00.asp).

**WINWHATWHERE INVESTIGATOR.** Программа Investigator, начавшая свое существование под названием WinWhatWhere в 1993 году, предназначалась для управления проектами. В ее задачи входил учет времени использования того или иного программного продукта. К 1998 году, в связи с возросшим интересом к компьютерному наблюдению, функциональная направленность программы была изменена. Теперь Investigator представляет собой полнофункциональный пакет для мониторинга клавиатуры, изображения на экране, веб-камер и работы приложений. Одна из очень удобных особенностей программы заключается в возможности ее автоматической deinсталляции по истечении заданного периода времени. Основной недостаток программы Investigator – ее огромный размер (она написана на Visual Basic). Поэтому удаленное распространение программы возможно только в том случае, если вы придумаете способ убеждения потенциальных жертв в необходимости открытия вложений объемом 3 Мб в письмах. Заказать Investigator вы сможете на сайте компании [www.winwhatwhere.com](http://www.winwhatwhere.com) всего за \$100.

## АППАРАТНЫЕ СРЕДСТВА МОНИТОРИНГА КЛАВИАТУРЫ

В отличие от нескольких сотен программных keylogger-утилит, доступных в сети Интернет, продажей аппаратных устройств мониторинга клавиатуры занимается всего несколько компаний. Среди них вы можете найти следующие (см. врезку на с. 289).

**KEYHOST.** Новозеландская компания Interface Security является одним из пионеров и новаторов в сфере выпуска аппаратных средств мониторинга клавиатуры. Выпущенный ею продукт под названием KeyGhost выглядит как обычный согласующий фильтр. Шнур клавиатуры подключается к одной стороне фальшивого фильтра, который своей другой стороной подключается непосредственно к PS/2- либо AT-порту клавиатуры. Запись последовательности нажатия клавиш начинается сразу после подключения устройства к компьютеру. Набрав в текстовом редакторе пароль для данного keylogger-модуля, вы можете настроить само устройство. Поскольку KeyGhost регистрирует все без исключения нажатия клавиш, то при встрече в последовательности искомой комбинации символов, являющейся паролем, он отсылает в текстовый процессор текстовое меню, позволяющее загрузить или очистить текущий журнал, изменить пароль или выполнить другие операции.

Поскольку интерфейс клавиатуры не предназначен для высокоскоростного обмена данными, выгрузка информации с аппаратного keylogger-модуля представляет собой довольно длительный процесс (передача может осуществляться со скоростью порядка 150 символов в секунду). Проработав в течение длительного времени и записав, скажем, около полумиллиона нажатий, keylogger потребует около часа для выгрузки такого количества информации. Производитель KeyGhost предлагает решение проблемы в виде приобретения дополнительного адаптера для

ускоренной выгрузки данных, который одной стороной подключается к keylogger, а другой – к последовательному порту компьютера. Это позволяет достичь приемлемой скорости в 56 Кбит/с\*.

## Разоблачения: из России с любовью

В ходе операции ФБР с подставной компанией Invita (о которой мы рассказывали в главе 1), завершившейся арестом двух российских взломщиков, правительство использовало для сбора улик коммерческую программу мониторинга клавиатуры WinWhatWhere Investigator. Хотя письменные показания специального агента ФБР Майкла Шулера изначально не подлежали огласке, в конце концов, их содержание распространилось по сети Интернет. Эти показания придают операции весьма пикантную окраску.

ФБР установила программу WinWhatWhere на два компьютера. Горшков, один из подозреваемых, использовал прослушиваемый компьютер IBM Thinkpad для подключения с помощью службы telnet к удаленному компьютеру freebsd.tech.net.ru. Он не подозревал, что используемое им имя учетной записи (kvakin) и пароль (cfvlevfg) были записаны при помощи keylogger. После ареста Горшкова Шулер несколько раз безуспешно пытался подключиться к компьютеру подозреваемого (похоже на то, что он использовал имя вместо IP-адреса). Затем он посетил веб-сайт [www.samspade.org](http://www.samspade.org) и выяснил с помощью whois, что компьютер freebsd являлся частью сети, связанной с tech.net.ru. С помощь службы telnet Шулер подключился к нужному ему компьютеру и затем использовал программу CuteFTP для загрузки содержимого жесткого диска.

За помощью в проведении операции по удаленной загрузке файлов Шулер обратился к эксперту по вопросам безопасности. (Из письменных показаний можно сделать вывод, что Шулер не имел опыта работы с операционными системами Linux.) Привлеченный Шулером эксперт сделал оценку свободного дискового пространства на целевом компьютере, а затем заархивировал содержимое при помощи tar и загрузил его по FTP в офис ФБР в Сиэтле.

Заметка для будущих шпионов: никогда не доверяйте чужим компьютерам либо сетям, демонстрируя свои знания в вопросах безопасности, иначе вы можете попасться, как те двое русских, которые полагали, что их проверяют для приема на высокооплачиваемую работу.

\* В настоящее время существуют также USB-адAPTERЫ для ускоренной выгрузки. – Прим. ред.

Стоимость KeyGhost колеблется от \$89 за устройство для домашнего использования, позволяющее хранить около 128 Кб информации, до \$199 за профессиональную модель с объемом памяти в 2 Мб и встроенным шифрованием данных. В ассортименте компании Interface Security также имеются клавиатуры со встроенными устройствами мониторинга. Ознакомиться с ассортиментом и заказать понравившиеся вам товары вы сможете в сети Интернет по адресу [www.keyghost.com](http://www.keyghost.com).

**KEYCATCHER.** Разработчики KeyKatcher любят называть свой продукт «магнитофоном для клавиатуры». Это устройство отличается по своему виду от того же KeyGhost или KeyLogger. KeyKatcher выглядит не как кусок кабеля, а как небольшой переходник, подключаемый к порту клавиатуры компьютера. Сама клавиатура затем подключается к этому переходнику. В комплект KeyKatcher входит специальная спрессованная под нагревом трубка, которая может быть надета на шнур клавиатуры и переходник, делая данное устройство менее заметным по сравнению с аналогами.

KeyKatcher функционирует подобно другим аппаратным средствам мониторинга клавиатуры – для вывода меню, ввода пароля и загрузки журнала он также использует текстовые редакторы. Но модулю KeyKatcher недостает памяти – он может хранить не более 64 Кб данных (хотя меньшее количество памяти позволяет уменьшить размер устройства). Таким образом, данный товар подходит для кратковременного мониторинга активности пользователя либо для тех случаев, когда известно, что пользователь мало работает с клавиатурой. KeyKatcher уникален тем, что каждый экземпляр устройства имеет свой серийный номер, присвоенный производителем, что позволяет легко выяснить владельца данного устройства.

Базовая модель KeyKatcher с 8 Кб памяти стоит \$45, 32 Кб и 64 Кб версии доступны по цене \$59 и \$79 соответственно. За более подробной информацией обратитесь к сайту производителя [www.keykatcher.com](http://www.keykatcher.com).

**HARDWARE KEYLOGGER.** Помимо программы мониторинга клавиатуры под названием IKS, компания Amecisco также занимается выпуском аппаратных средств мониторинга Hardware KeyLogger. Подобно KeyGhost, их keylogger, под недвусмысленным названием, выполнен в виде кабеля, подключаемого между шнуром клавиатуры и компьютерным портом. Последовательность нажатых клавиш хранится в энергонезависимом ЗУ, размер которого, в зависимости от модели, варьируется в пределах от 512 Кб до 2 Мб. Командное меню отображается в текстовом процессоре после ввода пароля.

Однако наиболее интересным продуктом компании Amecisco можно считать их Hardware KeyLogger Keyboard Edition. Компания Amecisco приобретает клавиатуры различных производителей и устанавливает внутрь самой клавиатуры микросхему для записи последовательности нажатых клавиш. В ассортименте компании имеются клавиатуры многих известных марок со встроенными устройствами мониторинга. Прием

с подменой клавиатуры отлично подойдет для новых компьютеров, однако этот вариант не подходит для старых клавиатур, покрытых слоем грязи и потемневших от времени. В такой ситуации вы даже можете заказать немного подержанную клавиатуру со встроенным «жучком», которая будет не так бросаться в глаза.

Стоимость KeyLogger составляет от \$99 за устройство с 512 Кб памяти до \$199 за версию с 2 Мб памяти. Модели Keypad Edition продаются по цене от \$129 до \$299. Детальная информация по предлагаемой продукции размещена на официальном сайте компании [www.amecisco.com](http://www.amecisco.com).

**СПЕЦИАЛЬНОЕ АППАРАТНОЕ ОБЕСПЕЧЕНИЕ.** Для выполнения большинства задач отлично подойдут обычные серийные устройства мониторинга клавиатуры, особенно модели, встраиваемые в клавиатуру, но иногда, когда вам предстоит работа над серьезным объектом, возникает необходимость в таком устройстве, которое действительно не смог бы обнаружить даже опытный хакер. Если вы располагаете достаточными государственными или корпоративными ресурсами, рассмотрите возможность создания аппаратного обеспечения на заказ. Специально разработанное keylogger-устройство может быть помещено внутрь клавиатуры, системного блока, ноутбука и иметь достаточно малый размер, чтобы не вызывать подозрений. Возможно также использование подобного устройства мониторинга клавиатуры в сочетании с программным обеспечением, позволяющим осуществлять передачу собранной информации по сети или через Интернет. Такое оборудование, конечно, обойдется вам недешево, но ваши затраты с лихвой окупятся за счет его высокой эффективности в шпионских операциях с большими ставками.

## Контрмеры

Наилучшая контрмера против шпионов, использующих keylogger, – это обеспечение физической безопасности рабочего места. Адекватные меры физической защиты уменьшают шансы злоумышленников на тайную установку шпионской аппаратуры на ваш компьютер. (Конечно, существует опасность удаленной установки программ мониторинга клавиатуры, однако, если придерживаться общих правил безопасности при работе с электронной почтой и сетью, этот риск можно свести к минимуму.)



Подробно меры по обеспечению физической безопасности обсуждались в главе 3.

Любые ухищрения, связанные с тайной установкой аппаратного или программного обеспечения для мониторинга клавиатуры, так или иначе, себя проявляют. Обнаружив, что вы являетесь объектом наблюдения, вы можете применить соответствующие контрмеры, действенные против большинства известных средств мониторинга клавиатуры.

## Инструментарий шпиона: Magic Lantern

В 2001 году начала всплывать информация о проекте ФБР, названном Magic Lantern (волшебный фонарь). Эта используемая правоохранительными органами программа мониторинга клавиатуры может устанавливаться на системе пользователя, открывшего вложение электронной почты, которое содержит «тロjanского коня». К сожалению, средства массовой информации несколько перекрутили факты, обозвав данную программу вирусом; с этого момента события вышли из-под контроля. Предполагается, что компания Network Associates сообщила ФБР о своих гарантиях того, что их антивирусное программное обеспечение McAfee не будет обнаруживать Magic Lantern, дабы не препятствовать проведению расследований. (В то же время такие производители антивирусного программного обеспечения, как Symantec и Sophos, поспешили заявить, что они не станут предоставлять льготы программе Magic Lantern и оставят в своих продуктах функции обнаружения и удаления данного «тロjана», как и любой другой недружественной программы.) Это вызвало всплеск возмущений со стороны адвокатов по защите прав на электронную интеллектуальную собственность, в результате чего компания Network Associates вынуждена была убрать всякие упоминания о Magic Lantern из своих заявлений. Некоторые аналитики по вопросам безопасности рассматривали пресс-релиз по этому поводу как «открытую дверь» для участия компании Network Associates в других правительственные проектах, необязательно связанных с Magic Lantern. Поклонники теории заговоров начали распускать слухи о компании Network Associates, которая в то же время начала продажу коммерческих версий утилиты шифрования PGP, по поводу наличия в этих версиях запасной лазейки, сделанной по запросу правительственных служб.

Тема проекта Magic Lantern оказалась настолько животрепещущей, что по ее поводу даже стали шутить. К примеру, в одном из онлайновых обсуждений участник цинично пошутил по поводу наблюдательной программы: «Программа работает только в том случае, если: а) ФБР ворвется к вам домой и установит Outlook; б) вы всегда открываете сообщения электронной почты с вложениями, в теме которых значится 'Белоснежка и 7 агентов ФБР'; в) вы всегда запускаете вложения с названиями вроде ФБРЛЮБИТВАС.VBS».

Хотя разговоры по поводу данного проекта не утихали довольно долго, никаких достоверных подробностей по нему не известно. ФБР признает, что Magic Lantern являлся «инструментальным средством», входящим в набор программных инструментов для ведения расследований под кодовым названием Cyber Knight (кибер-рыцарь).

## Просмотр установленных программ

В Панели управления Windows найдите значок «Установка и удаление программ» и просмотрите список всех установленных на вашем компьютере программ, обращая особое внимание на те программы, которые вы не устанавливали самостоятельно либо предназначение которых вам неизвестно. Как это ни удивительно, столь простая мера позволяет обнаружить некоторые виды коммерческих keylogger-программ.

## Анализ автоматически загружаемых программ

Очевидно, что для решения своих задач keylogger-программа вначале должна быть запущена. Обычно программа инсталляции помещает инструкции по автоматической загрузке keylogger-утилиты в одно из следующих мест:

- файл autoexec.bat,
- папку Автозагрузка,
- системный реестр.

Как правило, программы мониторинга клавиатуры записывают информацию о себе и инструкции в системный реестр, поскольку большинство пользователей вообще никогда туда не заглядывают. Чтобы выяснить, какие программы назначены для автозагрузки, воспользуйтесь стандартной утилитой RegEdit и просмотрите значения следующих ключей:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce  
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```

Но прежде чем приступить к просмотру и изменению ключей реестра, загрузите компьютер в «безопасном режиме» (Safe Mode). Это необходимо потому, что некоторые программы мониторинга клавиатуры изменяют значения ключей Run после своей загрузки, чтобы скрыть следы своего присутствия. В безопасном же режиме автозагрузка программ отключена, и вы можете просматривать неизмененные значения ключей реестра, например, путь для запуска keylogger.

В состав операционной системы Windows 9x/Me/NT/2000/XP также входит стандартная утилита настройки системы msconfig.exe. Эта программа позволяет модифицировать содержимое файлов autoexec.bat, Win.ini и списка программ автозагрузки. Данная утилита хорошо подходит для обнаружения keylogger-модулей, автоматически запускаемых при загрузке операционной системы.

## Контрмеры: дезинформация

Что делать, если вы обнаружили установленный на своей системе keylogger-модуль? Конечно, вы можете немедленно отключить либо удалить его, но, с другой стороны, подумайте над возможностью использования программы в качестве средства дезинформации установившего программу шпиона. Пролистайте главу 1 данной книги и вспомните обсуждавшиеся в ней вопросы: подумайте, кто за вами может шпионить и что его может заинтересовать. Вам необходимо проанализировать, к какому типу keylogger-модулей относится данное программное или аппаратное средство. Если вы обнаружили файл журнала, проверьте дату создания файла, чтобы оценить, как давно за вами ведется наблюдение (не забывайте, однако, что дата создания файла легко может быть фальсифицирована). После приблизительного подсчета времени работы keylogger-программы попытайтесь оценить возможный ущерб от последствий его применения. Над чем вы в это время работали? Как часто вы посещали различные веб-сайты либо использовали программные продукты, требующие ввода пароля?

Если вы хотите дезинформировать потенциального шпиона, вам придется перенести свою работу на другой безопасный компьютер, а скомпрометированный компьютер использовать как часть своей стратегии по введению злоумышленника в заблуждение. Конечно, вы можете продолжать работать и на том компьютере, за которым ведется наблюдение, однако в этом случае вам придется проявить большую осторожность, дабы не допустить утечки конфиденциальной информации.

Какие сведения необходимо включить в кампанию по дезинформации? Подойдут документы и переговоры, маскирующие ваши реальные действия, информация, противоречащая ранее собранным при помощи keylogger данным, упоминание имен людей, которые могут быть причастны к данному факту шпионажа. Классический пример – «подсадная утка», в результате применения которой ваш противник начинает думать, что люди в вашей организации, которым он доверял, на самом деле работают на вас. К примеру, если вы подозреваете, что информация о предстоящем слиянии компании стала известна конкурентам, вы можете фальсифицировать серию документов и электронных писем, свидетельствующих о расторжении предварительной договоренности и поиске другой компании для приобретения.

Учтите, что, если вам предстоит бороться с умудренным опытом противником, ваши действия по дезинформации могут вызвать подозрение, поэтому в любом случае вы должны быть готовы к пересмотру своих планов. Длительность операции по дезинформации зависит от целей, которые вы ставите перед собой, и количества ресурсов, которые вы готовы выделить на решение данного вопроса.

Если у вас возникли подозрения, что кто-то сумел получить физический доступ к вашему компьютеру, вы можете установить наблюдение, чтобы выяснить, кто подключил к вашему компьютеру «жучка». Наблюдение может быть организовано как с помощью дорогой видеокамеры, так и с помощью простой веб-камеры в сочетании с программным обеспечением для обнаружения движения.

## Анализ активных процессов

Произведя поиск подозрительных файлов в списке автоматически загружаемых программ, далее необходимо проверить, не является ли keylogger активным в данный момент времени, то есть не запущен ли он в качестве процесса.

### ДИСПЕТЧЕР ЗАДАЧ

Диспетчер задач позволяет просматривать активные программы и процессы. Запустить его можно следующими способами:

- В Windows 3.x, 9x и Me нажмите Ctrl+Alt+Del.
- В Windows 2000, NT и XP щелкните правой кнопкой мыши по пустому пространству панели задач и выберите в контекстном меню пункт Диспетчер задач (с тем же успехом, вы можете воспользоваться сочетанием клавиш Ctrl+Alt+Del).

Учтите, что в предыдущих версиях Windows 3.x, 9x и Me Диспетчер задач выводил весьма ограниченные сведения о системе, поэтому в этих версиях умело написанные программы мониторинга клавиатуры могли быть вообще не видны в списке программ. В Windows 2000, NT и XP можно просмотреть все процессы в системе, что позволяет обнаружить программный keylogger, если только он не был написан в виде драйвера.

### PROCESS EXPLORER

Великолепной альтернативой Диспетчеру задач является свободно распространяемая утилита Process Explorer от компании Sysinternals. Process Explorer позволяет получать массу дополнительной информации, помимо стандартных сведений, выводимых в Диспетчере задач, и при этом он работает со всеми версиями ОС Windows, начиная с Windows 95. Эта программа идеально подходит для обнаружения скрытых программ

мониторинга клавиатуры, поскольку в ней выводится путь запуска того или иного файла. Загрузить Process Explorer можно с официального сайта компании [www.sysinternals.com](http://www.sysinternals.com).

Исследуя запущенные системой процессы, вы, скорее всего, наткнетесь на несколько неизвестных вам названий. Не надо сразу думать, что перед вами keylogger. Возможно, вы имеете дело с обычной программой или службой, но чтобы убедиться в этом, вам придется провести некоторое расследование.

Чтобы корректно идентифицировать неизвестный процесс, обратитесь к следующим источникам информации:

- Введите имя процесса или связанное с ним имя файла в поисковом сервере, задав поиск в сети Интернет и группах новостей. Как правило, по указанным ссылкам вы сможете найти информацию об определенном процессе.
- Посетите сайт [www.answersthatwork.com/Tasklist\\_pages/tasklist.htm](http://www.answersthatwork.com/Tasklist_pages/tasklist.htm). Здесь вы сможете найти регулярно обновляемую информацию по процессам ОС Windows и программам сторонних разработчиков, которые вы часто можете увидеть в списке активных процессов.

## MSINFO32

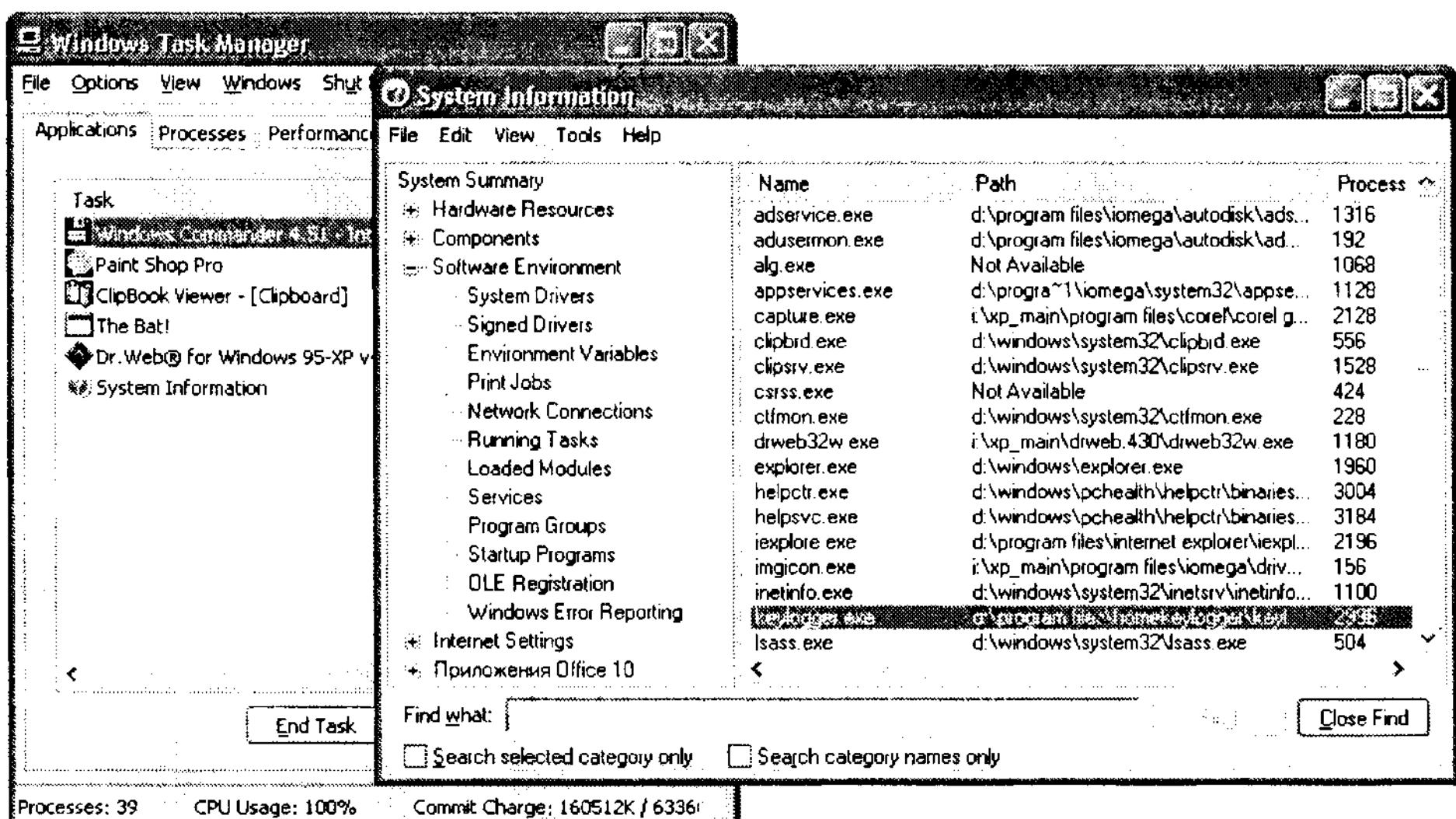
Еще одна очень полезная утилита для поиска keylogger и других скрытых программ называется MSinfo32. Она выводит сведения об установленном аппаратном и программном обеспечении, загруженных драйверах, список активных процессов, включая перечень автоматически загружаемых программ (рис. 8.3). Это мощная утилита, которая используется реже, чем это стоило бы делать. Чтобы запустить программу, вам необходимо:

1. В меню Пуск выбрать пункт Выполнить.
2. Ввести имя MSinfo32.
3. Нажать OK.

Сведения, которые могут помочь вам распознать установленный keylogger, находятся в папке Software Environment («Программная среда»).

## Отслеживание процессов, ведущих запись в файл

Практически все программы мониторинга клавиатуры записывают последовательность нажатых клавиш в файл. Эта важная особенность таких программ также помогает в их обнаружении. Осуществляя мониторинг постоянно открытых файлов, в которые ведется запись информации, вы можете обнаружить активный keylogger.

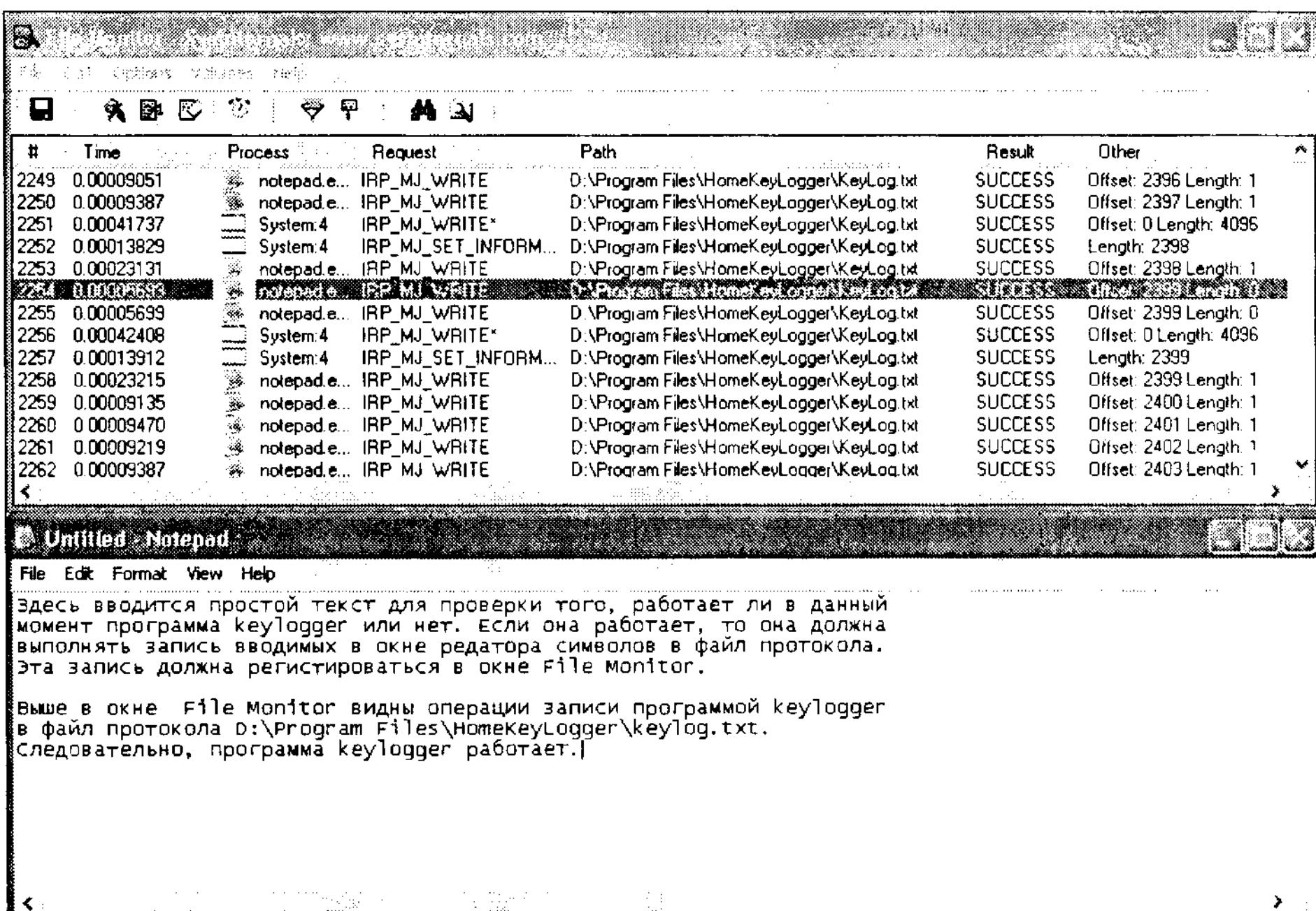


**Рис. 8.3.** Программа keylog.exe не видна в Диспетчере задач в Windows XP, зато ее можно увидеть в списке активных процессов в утилите MSinfo32

Программа File Monitor или Filemon позволяет вести наблюдение за файловыми операциями в режиме реального времени. Каждый раз, когда происходит обращение к файлу – его открытие или закрытие, запрос атрибутов, чтение или запись, Filemon выводит дату и время обращения, а также имя процесса, инициировавшего обращение к файлу. Это чрезвычайно мощная утилита для обнаружения программ мониторинга клавиатуры, поскольку она позволяет одновременно получать информацию и об имени процесса, и об имени используемого им файла (рис. 8.4).

Чтобы воспользоваться этой свободно распространяемой утилитой, вам понадобится вначале загрузить ее с сайта [www.sysinternals.com](http://www.sysinternals.com), а затем запустить, следуя инструкциям по установке. (При работе в операционных системах Windows NT/2000/XP вам необходимо обладать полномочиями администратора для корректной работы утилиты.) Выполните следующую последовательность действий:

1. Закройте все активные программы.
2. Запустите Filemon.
3. Выберите значок Filter на панели инструментов (либо нажмите сочетание клавиш Ctrl+L).
4. Установите флажок Log Writes. В результате на экране постоянно будут отображаться только последние несколько операций.
5. Нажмите кнопку Apply.



**Рис. 8.4.** Программа Filemon в действии – она обнаруживает запись в некоторый файл во время ввода информации в Блокноте

6. Выберите значок Capture (с изображением увеличительного стекла) на панели инструментов (либо выберите пункт Capture из меню Options или нажмите сочетание клавиш Ctrl+E).

После запуска программы FileMon откройте какой-либо текстовый редактор и начните набирать в нем текст. Поскольку программы мониторинга клавиатуры обычно записывают последовательность нажатия клавиш в буфер, перед тем как перенести информацию в файл журнала, вам может понадобиться ввести достаточный объем текста (в зависимости от размера буфера), прежде чем keylogger обратится к файлу журнала.

Если вы обнаружите постоянные обращения к определенному файлу, в то время как система и другие приложения бездействуют, проверьте, не является ли он файлом протокола keylogger.

## Удаление исполняемых библиотек VB

Немалая толика свободно распространяемых и коммерческих программ мониторинга клавиатуры написаны на Visual Basic и, как следствие, требуют для своей работы наличия в системе соответствующих библиотек. Если никакие нужные вам программы не используют эти файлы, вы можете спокойно удалить их, чтобы не допустить запуска keylogger, написанных на VB. В зависимости от используемой версии Visual Basic, эти

библиотеки могут называться vbrun100.exe, vbrun200.exe, vbrun300.exe, vb4run.exe, MSVBVM50.exe или vbrun60sp5.exe. Задайте поиск файлов и папок на локальных дисках. Чтобы в системе не могли работать программы на Visual Basic, вам достаточно переименовать эти файлы, а затем выполнить перезагрузку компьютера. Очевидно, что подобный способ не поможет вам в борьбе с keylogger-программами, написанными на других языках программирования.

## Поиск уникальной строки

Наберите в текстовом процессоре некоторую уникальную строку символов; затем скопируйте часть строки в буфер обмена и воспользуйтесь пунктом Поиск файлов и папок меню Пуск для поиска файлов, содержащих данную строку. Этот прием работает в тех случаях, когда установленный в системе keylogger не шифрует содержимое файла протокола.

## Использование персональных брандмауэров

На сетевом компьютере возможна ситуация, когда установленный в системе keylogger не выполняет запись информации на диск, а сразу отсылает данные через Интернет. В этом случае программа FileMon не поможет вам в обнаружении keylogger-программы, поскольку никаких обращений к файлам происходит не будет.

Установка персонального брандмауэра (такого, как ZoneAlarm, который проверяет правомочность сетевого обращения со стороны каждой программы) может помешать работе подобных программ мониторинга клавиатуры.

Тем не менее, если шпион обладает физическим доступом к вашему компьютеру, ему ничто не помешает изменить настройки брандмауэра таким образом, чтобы keylogger-программа имела права на доступ в Интернет. По этой причине советуем вам периодически проверять настройки брандмауэра, чтобы убедиться, что ни одна из неизвестных вам программ не получила доступ к Интернету без вашего разрешения.

## Использование программ проверки целостности файлов и реестра

В результате установки программы мониторинга клавиатуры в системе остаются некоторые следы этого процесса. Как раз для выявления изменений в системе (добавления файлов или модификации ключей реестра Windows) и предназначены программы проверки целостности файлов и реестра. С их помощью вы можете собрать ценную информацию и выявить тайно установленные программы мониторинга клавиатуры.

## Тактика: обход защиты брандмауэра

Одно из потенциальных уязвимых мест персонального брандмауэра заключается в возможности использования заслуживающего доверия приложения для скрытой отправки информации через Интернет со стороны установленной злоумышленником программы. К примеру, большинство пользователей доверяют Internet Explorer, однако, если воспользоваться уязвимыми межстами самого Internet Explorer, можно организовать через него передачу данных на веб-сайт шпиона, которую большинство персональных брандмауэров даже не заметят.

Джейсон, член немецкой группы German Rat Coding Team, разработал keylogger под названием God (Бог), в котором использовался вышеупомянутый недостаток Explorer. Вначале шпион размещал на своем веб-сайте сценарий php, выполняющий установку программы мониторинга клавиатуры на целевом компьютере. Затем эта программа записывала последовательность нажатия клавиш и отсыпала ее на веб-сервер, запуская php-сценарий в Internet Explorer. Поскольку большинство людей настраивают свои брандмауэры таким образом, чтобы те позволяли Internet Explorer без подтверждения подключаться к сети Интернет, такой keylogger было невозможно обнаружить.

Если вас заинтересовала информация по проекту God, посетите веб-сайт [www.ratct.net](http://www.ratct.net). Только перед этим вам придется подучить немецкий.



Подробное обсуждение программ проверки целостности файлов и программ мониторинга реестра ожидает вас в разделе «Контрмеры» главы 9.

## Использование ПО для обнаружения keylogger

Вместо ручного поиска тайно установленных keylogger-программ при помощи одного из вышеперечисленных методов, можно прибегнуть к услугам существующих на рынке программных продуктов, позволяющих автоматически обнаруживать установленные программы мониторинга клавиатуры. Однако при использовании ПО для автоматического обнаружения keylogger, вместо того чтобы вручную анализировать активные процессы и файловые операции записи, вам необходимо учсть ряд моментов:

- ПО для обнаружения программ мониторинга клавиатуры позволяет выявлять только известные программные типы keylogger; соответственно недавно появившиеся либо неизвестные keylogger-программы обнаружены не будут.

- Как и для антивирусного программного обеспечения, производители часто выпускают обновления к базе данных известных keylogger-программ. Поэтому, если вы используете такое ПО, не забывайте о его своевременном обновлении.
- ПО для обнаружения keylogger-программ может приводить к «ложным срабатываниям» (когда программа заявляет о найденной программе мониторинга клавиатуры, которая на самом деле таковой не является). Если программа приняла решение о существовании в системе keylogger-программы на основе подозрительного имени файла, попробуйте задать поиск в Интернете имени этого файла на случай, если такое имя может относиться к другой программе.

Некоторые популярные программы мониторинга клавиатуры перечислены в следующих параграфах.

## SPYCOP

Авторы программы SpyCop утверждают, что с ее помощью вы можете обнаруживать более 300 различных keylogger-программ. В случае обнаружения программы мониторинга клавиатуры, SpyCop предлагает пользователю переименовать файл, присвоив ему расширение .spy (что, как правило, не дает запустить keylogger, однако может вызывать другие проблемы). Помимо анализа файлов на предмет наличия доказательств либо обнаружения keylogger, в SpyCop организована функция, находящаяся на данный момент в стадии бета-тестирования, с помощью которой вы можете осуществлять мониторинг активных процессов для обнаружения действующего keylogger. Демонстрационную версию программы SpyCop вы можете загрузить с сайта [www.spycop.com](http://www.spycop.com), правда, представлена она здесь в несколько ущербном виде (в ней во время сканирования пропускаются случайные файлы). Стоимость полной версии, которую можно заказать онлайн на том же сайте, составляет \$69,95.

## WHO'S WATCHING ME

Еще одной программой, специально предназначеннной для обнаружения keylogger, является программа Who's Watching Me (Кто следит за мной). Эта программа может загружаться автоматически при запуске операционной системы либо по расписанию. Who's Watching Me сообщает пользователю об обнаружении работающей программы мониторинга клавиатуры, однако бороться с подобными программами она не умеет. Утилита Who's Watching Me распространяется с 90-дневным сроком опробования (стоимость регистрации составляет \$24,95), загрузить ее можно с сайта [www.trapware.com](http://www.trapware.com).

## PEST PATROL

PestPatrol представляет собой многоцелевую программу, предназначенную для поиска и обнаружения keylogger-программ, «тロянских коней», «червей» и рекламного шпионского ПО. Утилита выполняет сканирование файлов и процессов, предоставляя детальную информацию по найденным шпионским программам. Стоимость PestPatrol составляет \$29,95, оценочная версия с ограниченной функциональностью доступна на сайте [www.pestpatrol.com](http://www.pestpatrol.com).

### Контрмеры. Шпионские игры: keylogger против ПО для обнаружения

В марте 2002 года спекуляции вокруг темы «keylogger» достигли своего апогея. MSNBC сообщила о том, что коммерческие компании WinWhatWhere и SpectroSoft, специализирующиеся на производстве программ мониторинга клавиатуры, включили в свои продукты код, не позволяющий обнаруживать их keylogger-программы при помощи популярной утилиты Who's Watching Me.

Ричард Итон, президент компании WinWhatWhere, заявил: «Если кто-то зарабатывает деньги на том, что разрушает написанное мною ПО, то я просто вынужден предпринять соответствующие контрмеры».

Вес Остин, разработчик программы Who's Watching Me, в ответ сказал: «Мы только сообщаем людям о существовании наблюдательной программы. Зачем мешать работе программы Who's Watching Me, если ваш продукт используется в законных целях, и вы не пытаетесь что-либо скрыть... Ведь нам с вами известно, для чего чаще всего используются подобные программные продукты».

Однако казавшаяся неизбежной война производителей противоположного по своей функциональности ПО (по принципу «око за око, зуб за зуб») не вспыхнула, угаснув вскоре после того, как информация об этом достигла прессы. Немного погодя компания WinWhatWhere объявила, что больше не будет вносить в файлы программы Who's Watching Me исправления, которые бы мешали обнаружению их keylogger-программ.

## SPYBOT SEARCH & DESTROY

Spybot Search & Destroy – популярная бесплатно распространяемая утилита, автором которой является Патрик Колла. Эта программа позволяет обнаруживать и удалять keylogger-программы, троянских коней, рекламное ПО, собирающее информацию о пользователях, и другой недружественный программный код. В этой программе реализовано множество

полезных функций, включая онлайнное обновление баз, удаление следов использования программы и мультиязычный интерфейс. Загрузить программу вы можете с веб-сайта <http://beam.to/spybotsd>.

## Использование программ перехвата сетевых пакетов

Если у вас возникли подозрения в том, что keylogger тайно отправляет информацию по электронной почте, воспользуйтесь программой перехвата сетевых пакетов, такой как Ethereal, для наблюдения за сетевым трафиком. Обратите внимание на передачу данных по почтовым протоколам и помните о том, что, скорее всего, данные окажутся зашифрованными, поэтому вы вряд ли сможете прочесть содержимое. (Однако поскольку в большинстве keylogger-программ используются ненадежные алгоритмы шифрования, то при наличии опыта в сфере криптографии, вы можете попытаться взломать зашифрованную информацию за короткое время.)



Более подробно о программах перехвата сетевых пакетов мы расскажем вам в главе 10.

## Обнаружение аппаратных keylogger-модулей

Очевидно, что никакой из вышеперечисленных способов обнаружения программных keylogger-модулей не подходит для выявления аппаратных средств мониторинга клавиатуры. В зависимости от используемого типа аппаратного keylogger-модуля, их либо очень легко, либо практически невозможно обнаружить.

### KEYLOGGER, ИСПОЛНЕННЫЙ В ВИДЕ КАБЕЛЯ

Выявить keylogger, выполненный в виде кабеля или соединителя, очень легко. Достаточно взглянуть на порт подключения клавиатуры к компьютеру и проверить, как подключена ваша клавиатура. Если между кабелем клавиатуры и портом компьютера находится дополнительный кабель или переходник, вам следует проявить осторожность.

### KEYLOGGER, ВСТРОЕННЫЙ В КЛАВИАТУРУ

Обнаружить подмену клавиатуры другим экземпляром, который оснащен встроенным keylogger-модулем, на порядок сложнее, чем обычный аппаратный keylogger, выполненный в виде соединителя. Помочь вам в этом сможет только ваша наблюдательность и следующие контрмеры:

- **Если клавиатура выглядит как-то «не так».** Если вдруг вам показалось, что ваша клавиатура выглядит необычно, – у вас есть все основания для подозрений. Возможно, у нее несколько изменился цвет, клавиатура стала как будто чище, либо же при нажатии клавиш пальцы испытывают иные ощущения.

- **Использование эталонной клавиатуры.** Одна из давних технических контрмер, применявшаяся, к примеру, при поиске «жучков» в телефонах, сводилась к сравнению этого телефона с эталонным аппаратом. Технические специалисты тщательно сравнивали два телефона, пытаясь выявить различия между ними. То же самое можно проделать и с клавиатурами. Микросхемы для мониторинга клавиатуры обычно достаточно заметны.
- **Нанесение отметин.** Еще одна сигнальная контрмера заключается в нанесении на клавиатуру характерных царапин в разных местах и под разными углами. Затем вы должны записать расположение отметин либо сделать цифровую фотографию клавиатуры. Если кто-либо захочет подменить клавиатуру, чтобы начать шпионить за вами, вряд ли он сможет в точности воссоздать все характерные особенности клавиатуры – если только ваш противник не является чрезвычайно скрупулезным и опытным аналитиком.

В случае возникновения подозрений в том, что к вашему компьютеру была подключена клавиатура со встроенным «жучком», лучше не рискуйте и приобретите в магазине новую клавиатуру. Кроме того, вы можете воспользоваться программами с «виртуальной клавиатурой», предназначенней для работы пользователей с физическими недостатками либо для ввода секретной информации (паролей). Поскольку аппаратные средства мониторинга клавиатуры взаимодействуют непосредственно с самой клавиатурой, то метод ввода информации при помощи экранной клавиатуры позволяет избежать наблюдения со стороны подобных устройств. Однако такой подход может не сработать в случае использования злоумышленником программных средств мониторинга клавиатуры, поскольку многие из них позволяют, например, записывать копию экранного изображения. Кроме того, опытный шпион обычно прибегает к параллельному использованию программных и аппаратных средств мониторинга клавиатуры, чтобы увеличить свои шансы на успех. Старая поговорка разведчиков: обнаружив один «жучок», ищи второй – справедлива и по сей день.

Учтите, что использование ноутбуков либо USB-клавиатур намного снижает вероятность быть подслушанным с помощью аппаратных keylogger-модулей, если только против вас не брошены все силы полиции либо иностранной разведки.

## Использование паролей для работы с аппаратными keylogger-модулями

В большинстве коммерческих аппаратных и программных средств мониторинга клавиатуры используется пароль либо определенная последовательность нажатия клавиш для выполнения функций обслуживания keylogger-модуля. Если шпион по ошибке оставил настройки по умолчанию, которые обычно описаны на веб-сайте производителя, то доступ к программе или устройству сможете получить и вы.

Существует весьма эффективная техника обнаружения установленного keylogger с помощью сценария либо программы для атаки «в лоб», которая почему-то применяется нечасто. Многие коммерческие keylogger-модули имеют функцию вызова панели управления keylogger при нажатии некоторого заданного пользователем сочетания клавиш. Простейший сценарий для подбора искомого сочетания Ctrl с двумя другими клавишами может быть написан на Visual Basic, Perl, как, впрочем, и на любом другом языке программирования.

## Контрмеры: опломбирование системного блока

Если у вашего противника бездонный бюджет и он хочет быть уверенным в том, что его не обнаружат, шпион может установить устройство мониторинга клавиатуры внутрь системного блока. Обнаружить подобное устройство сложно, поскольку вам (как, впрочем, и злоумышленнику) придется вскрывать системный блок, зная при этом, как это устройство должно выглядеть. При проведении правительственной шпионской операции спецслужбы могут даже заказать разработку и изготовление специального контроллера клавиатуры, на вид неотличимого от настоящего, но при этом обладающего встроенной функциональностью keylogger. (Пожалуйста, вспомните главу 1 и наш разговор о вероятной и возможной угрозе применительно к вашей ситуации.)

Одна из контрмер, позволяющая определить, подвергался ли системный блок вскрытию, заключается в использовании пломб (наклеек, без повреждения которых вскрыть компьютер невозможно). Открытие системного блока либо попытки снятия этих наклеек приводят к их повреждению. Разумеется, решительный противник может найти способы незаметного удаления и последующего восстановления пломб, однако это затруднит и задержит его.

Для людей экономных мы приведем современную интерпретацию старого шпионского метода. Снимите крышку с вашего системного блока, возьмите в руку пару своих волосинок (или позаимствуйте у кого-нибудь еще, если у вас их слишком мало, чтобы тратить по пустякам) и зажмите их между корпусом и крышкой системного блока, когда будете ставить крышку на место. Если кто-то попытается открыть системный блок, он вряд ли обратит внимание на пару волосинок, выпавших при снятии крышки. Вы же, заметив, что волосинки отсутствуют, будете иметь повод задуматься. (Подобный способ подходит для лиц, страдающих обоснованной паранойей, имеющих слишком много свободного времени либо слишком часто смотревших сериал «Миссия невыполнима».)

Так как аппаратные keylogger-модули используют введенный в текстовом редакторе пароль для отображения меню команд, вы можете написать сценарий для перебора всех возможных вариантов нажатия клавиш, после чего будет выполняться проверка, не были ли выведены в текстовом редакторе какие-либо иные данные, кроме введенного текста. Конечно, если длина пароля составляет более 7 символов, то для этого понадобится много времени.

## Использование Linux

В отличие от множества keylogger-утилит, написанных для ОС Windows, для операционной системы Linux количество таковых исчисляется единицами. Хотя установить keylogger на компьютер под управлением Linux можно путем подмены ядра системы на целевом компьютере, необходимыми для этого знаниями располагает далеко не каждый среднестатистический шпион. Тем не менее нам известны, по крайней мере, два программных keylogger-модуля, написанных специально для Linux, которые распространяются вместе с исходными кодами, включая один, описанный в популярном электронном журнале Phrack\*. Обе программы очень просты и по возможностям намного уступают коммерческим программам мониторинга клавиатуры под Windows. Однако вслед за растущей популярностью системы Linux, особенно среди настольных систем, после появления вирусов для этой операционной системы в ближайшее время можно ожидать разработки новых наблюдательных программ или же переделки существующих программ для Windows под платформу Linux.

## Просмотр журнала системных ошибок

Как и в работе любого другого программного обеспечения, в работе программ мониторинга клавиатуры иногда возникают сбои, приводящие к появлению странных сообщений об ошибках. Пользователи Windows, привыкшие к таким ошибкам, часто просто игнорируют подобные сообщения, но некоторые плохо написанные keylogger-программы могут вызывать постоянно повторяющиеся ошибки. И если вы допускаете, что можете стать жертвой шпионов, то потратьте время на просмотр журнала системных сбоев, вызванных ошибками программного обеспечения, на предмет выявления необычных сообщений.

## Удаление программ мониторинга клавиатуры

После обнаружения программы мониторинга клавиатуры, установленной на своей системе, пользователь должен принять решение, то ли ему прибегнуть к кампании по дезинформации противника, то ли просто удалить эту программу. Поскольку коммерческие программы мониторинга клавиатуры обычно копируют в системные папки множество своих файлов,

\* См. №59. – Прим. ред.

удалить их полностью трудно. Первое, что вам необходимо сделать, это определить тип keylogger-программы, установленной в системе. Для этого, воспользовавшись найденными доказательствами присутствия вредительского программного кода в системе (например, именами файлов либо ключами реестра), задайте поиск информации в сети Интернет. Если этот keylogger относится к коммерческим программным продуктам, советуем вам посетить веб-сайт производителя. Большинство производителей размещают на своих официальных веб-страницах информацию о том, как деинсталлировать keylogger-программу и другие сведения, помогающие в точности идентифицировать тип и версию используемого ПО.

## Контрмеры: устройство CompuSafe

Корейская компания Safe Technology Co. Ltd создала устройство под названием CompuSafe, предназначенное для безопасного ввода с клавиатуры. Это устройство необходимо подключить к порту клавиатуры, а затем вставить шнур от клавиатуры в разъем устройства. Аппаратное обеспечение позволяет зашифровывать информацию, взаимодействуя с программным драйвером. В результате получается зашифрованный текст, который не в состоянии разобрать keylogger-программа (по крайней мере, такая утилита, которая не умеет записывать копии экрана).

Сотрудники веб-сайта ExtremeTech протестировали устройство и обнаружили, что нажатия клавиш продолжают записываться в незашифрованном виде при взаимодействии с программой WinWhatWhere Investigator. Устройство работает даже с неизвестными ей keylogger-программами, однако при этом наблюдается чрезвычайное замедление скорости ввода с клавиатуры.

Хотя сама идея казалась многообещающей, ее воплощение, как всегда, несколько подкачало. Подробности вы можете прочесть на сайте [www.extremetech.com/article2/0\\_3973\\_472055\\_00.asp](http://www.extremetech.com/article2/0_3973_472055_00.asp).

Если вам не удается деинсталлировать keylogger-программу либо вы подозреваете о присутствии в системе иного наблюдательного ПО, сохраните резервную копию данных, с которыми вы работаете, на чистый носитель, после чего выполните низкоуровневое форматирование жесткого диска и переустановку системы с заслуживающего доверия источника (желательно оригинального носителя производителя ПО). Такой способ потребует времени, однако только так вы гарантированно избавитесь от всех недружественных программ.

# Заключение

Аппаратные и программные средства мониторинга клавиатуры – наиболее распространенный и коварный инструмент из шпионского набора. Тем не менее большинство коммерческих программных и аппаратных keylogger-модулей относительно легко обнаружить и блокировать после того, как вам стало известно о существующей угрозе.

- Если вы не обладаете глубокими техническими познаниями, воспользуйтесь утилитами для автоматического обнаружения keylogger-модулей, при этом не забывая постоянно обновлять базы данных к ним.
- Если у вас все-таки присутствуют технические наклонности, найдите время, чтобы внимательно проанализировать список активных процессов, файловую активность, а также список программ и драйверов, назначенных для автозагрузки.
- Осмотрите системный блок и клавиатуру – вдруг кто-то подключил к вашему компьютеру аппаратные средства мониторинга клавиатуры.

Выполняя простые вышеперечисленные меры, вы сможете значительно снизить риск подслушивания со стороны средств мониторинга клавиатуры (keylogger), если только вы не оказались жертвой широкомасштабной шпионской операции.

## Глава 9

# «Троянские кони»

«Я въезжаю в ваш город на большом черном троянском коне».

The Cure, «Club America», *Wild Mood Swings*

Шпионаж нередко называют второй из древнейших профессий, поэтому, прежде чем мы начнем говорить о современных троянских конях в контексте компьютерного шпионажа, освежим в памяти греческую мифологию, дабы создать декорации для последующего повествования.

В незапамятные времена, а именно в XII веке до нашей эры, Парис, сын короля Трои, похитил Елену, жену короля Спарты Менелая, которая считалась тогда самой прекрасной женщиной в мире. Менелаю и его брату, могущественному греческому королю Агамемнону, не понравилась выходка Париса, и они решили напасть на Трою. К несчастью для Менелая, легендарная Троя была слишком хорошо укреплена, и поэтому им не удалось отобрать Елену даже после десяти лет войны.

В конце концов, греки сообразили, что для того, чтобы выиграть войну, им необходимо прибегнуть к хитрости. Для этого они решили построить большого деревянного коня, внутри которого были спрятаны люди, в качестве подарка от якобы признавших себя побежденными греков, вернувшихся на свои корабли для отплытия в Грецию.

Троянцы приняли этот «подарок» за предложение мира, втащив коня на территорию укрепленного города и затеяв грандиозное празднование своей победы. Как вы, должно быть, догадались, это оказалось большой ошибкой с их стороны, поскольку ночью, когда большинство жителей города забылись во сне после празднества, греки тайком выбрались из деревянного коня, убили охрану и открыли ворота города, чтобы впустить греческую армию, которая вновь высадилась на берег под покровом темноты. Город пал, армия Трои была разбита, а Елена возвращена законному мужу.

Сегодня троянскими конями называют безобидные с виду компьютерные файлы и электронные послания, которые не всегда являются тем, чем кажутся. Приложения, называемые троянскими конями, позволяют получать удаленный доступ к компьютеру через Интернет, – с их помощью шпион может, к примеру, просматривать содержимое файлов на жестком диске компьютера жертвы. Данная глава будет посвящена принципам работы троянских коней. Мы рассмотрим, каким образом они устанавливаются в системе, какие из них лучше подходят для использования в целях шпионажа и (что, вероятно, важнее всего) как с ними бороться.

# Шпионская тактика

В этом параграфе мы, как всегда, предложим вам представить себя в роли шпиона: продажного журналиста, работающего на одну бульварную газетенку. Итак, вы являлись восходящей звездой уважаемой городской газеты, только недавно закончив колумбийский университет по специальности «журналистика». Однако в погоне за Пулитцеровской премией вы решили приукрасить вашу серию разоблачительных репортажей, воспринятую весьма критично, и, в конце концов, были обвинены в клевете и уволены. Времена были тяжелые, и единственная работа, которую вы смогли найти, сводилась к копанию в «грязном белье» знаменитостей. Вы вертелись, как белка в колесе, стараясь наскрести денег для поездки в горячую точку на Ближний Восток, в Афганистан, чтобы восстановить свою репутацию в качестве внештатного корреспондента.

Вы избрали своей целью знаменитую певицу, репутацию которой многие папарацци пытались замарать уже не один год. Вокруг нее ходили разные слухи: наркотики, любовные связи на стороне, акты насилия, однако никому не удавалось подобраться достаточно близко, чтобы выяснить реальное положение вещей. Ваш работодатель предложил \$50 000 тому, кто сможет написать изобличительную статью о ней, предоставив документальные подтверждения своих слов. Вы давно мечтали о такой возможности, и вот, наконец, она представилась: заработав \$50 000, вы смогли бы купить себе билет назад, в мир серьезной журналистики.

В это время ваш младший брат, любитель проводить время в чатах, загружать из Интернета пиратские копии различных программ и распространяющую без соблюдения авторских прав музыку в формате mp3, постепенно начал превращаться в маленького «хакера» (приобретающего опыт использования программ для несанкционированного проникновения в чужие системы). До сих пор вы были далеки от этого, но однажды ваш брат поведал вам о возможностях троянских коней и похвастался, как ему удавалось удаленно проникать в чужие компьютеры под управлением Windows и находить файлы с номерами кредитных карточек и банковскими документами. И все это он делал, рассыпая «ламерам» (жаргонное слово, обозначающее неопытных пользователей или просто неудачников) почтовые сообщения, в которые были вложены троянские кони. И вдруг вас осенила одна идея – пару месяцев назад вам удалось выяснить адреса электронной почты певицы, которые не были известны широкой публике и использовались для частной переписки. Тогда вы не знали, что с ними делать, но теперь вам в голову пришла гениальная мысль, и вы начали расспрашивать брата обо всем, что ему известно о троянских конях.

## Использование уязвимых мест

Успешность атаки при помощи троянского коня зависит как от наличия слабых мест в компьютерной системе безопасности, так и от человеческих слабостей. Для удаленного запуска троянского коня вам необходимо

воспользоваться некоторыми приемами социотехники, чтобы, к примеру, убедить потенциальную жертву открыть то или иное вложение. Вам также должны предусмотреть приемы, позволяющие обмануть брандмауэры, антивирусные программы и программы защиты от троянских коней.

На первый взгляд это может показаться достаточно сложной задачей, однако на самом деле для эффективного использования троянского коня в качестве инструмента шпионажа существует немало средств. Можно легко атаковать при помощи троянского коня рядового пользователя, а при более тщательной подготовке и планировании – даже пользователя, сведущего в вопросах компьютерной безопасности.

## ЗНАКОМСТВО С «ТРОЯНСКИМИ КОНЫМИ»

В данном контексте термин «троянский конь» обозначает внешне безобидное приложение, внутри которого на самом деле спрятан враждебный программный код. Троянский конь может быть скрыт в игре, почтовом вложении или даже на веб-странице. После открытия или запуска пользователем такого приложения, троянский конь устанавливается на жесткий диск целевого компьютера и впоследствии запускается каждый раз при загрузке системы.

После того как троянский конь был установлен, он начинает решать задачи, для которых и был изначально создан. К примеру, сетевая версия троянского коня может провоцировать самопроизвольное выдвижение каретки CD-привода, проигрывание звуковых файлов, изменение рисунка на Рабочем столе и выполнение других «шуточных» действий, заставляющих человека усомниться в своей нормальности. Но поскольку наша книга не называется «Секреты компьютерных розыгрышей», мы перечислим только те распространенные возможности троянских коней, которые могут быть использованы в целях шпионажа:

- перехват аудиоинформации с микрофона;
- перехват данных, передаваемых веб-камерой;
- редактирование реестра;
- извлечение и модификация содержимого файлов автозагрузки, таких как autoexec.bat и win.ini;
- модификация существующих файлов;
- мониторинг клавиатуры;
- извлечение хешированных паролей;
- запуск приложений;
- запись моментальных снимков экрана в режиме реального времени;
- завершение запущенных процессов;
- самостоятельная deinсталляция (удаление следов присутствия);
- загрузка и выгрузка файлов по сети.

## Тактика: не доверяй никому?

Хотя троянские кони представляют опасность еще со времен Елены Прекрасной, первые сведения об угрозе с их стороны в современной интерпретации были сообщены в 1984 году Кеном Томпсоном, одним из первых разработчиков операционной системы UNIX.

Томпсон описал разновидность атаки, в ходе которой осуществлялась модификация исходного кода компилятора С таким образом, что при компиляции любого исходного кода для команды входа в систему компилятор проводил его семантический анализ, а затем добавлял несколько дополнительных строк кода, задающих запасной пароль для откомпилированной программы.

Любой человек, прибегнувший к помощи данного компилятора для создания команды входа в систему, делал систему беззащитной от хакеров, которым был известен запасной пароль. Причем анализ исходного кода программы ничего бы не дал, поскольку в нем действительно отсутствуют доказательства присутствия троянского коня.

Томпсон предположил, что добавление кода троянского коня в стандартный компилятор С, распространяемый вместе с дистрибутивом UNIX, привело бы к наличию запасного пароля во всех системах, перекомпилированных с его помощью. А мораль, которую хотел выразить Томпсон, такова: «Нельзя доверять программному коду, если только вы сами не написали его от начала до конца». (Текст оригинального документа, подготовленного для выступления на Turing Award Lecture 84, доступен на веб-сайте [www.acm.org/classics/sep95/](http://www.acm.org/classics/sep95/).)

Результаты исследования, проведенного Томпсоном, актуальны и по сей день. Свидетельством тому могут служить следующие события, произошедшие во второй половине 2002 года:

- В ноябре 2002 года некто провел сравнение последних версий исходных кодов libpcap и tcpdump с веб-узла [tcpdump.org](http://tcpdump.org) и обнаружил, что на зеркале сайта находятся версии, содержащие троянских коней.
- В период с 28 сентября по 6 октября троянский конь распространялся в исходном коде утилиты SendMail 8.12.6.
- В августе некто взломал защиту сайта [ftp.freBSD.org](http://ftp.freBSD.org) и поместил троянского коня в пакет исходных кодов для OpenSSH.

- В июне был взломан еще один сайт, посвященный компьютерной безопасности ([monkey.org](http://monkey.org)). Злоумышленники заменили исходные коды программ dsniff, fragroute и fragrouter на версии с вложенными троянскими конями.

Хотя некоторые поклонники Windows заявляют, что в этом и состоит недостаток программного обеспечения, распространяемого вместе с исходными кодами, однако не следует забывать, что в двоичный исполняемый файл также может быть помещен троянский конь; правда, для этого файл придется дизассемблировать, а затем перекомпилировать заново (эта тема будет обсуждаться в главе 13).

Как видите, приложение «троянский конь» представляет шпионам широкие возможности в плане удаленного доступа к вашей информации. После установки и запуска этого приложения на целевом компьютере вам понадобится только подключиться к Интернету и запустить у себя утилиту, способную на расстоянии контролировать работу троянского коня, и в результате вы сможете получать доступ к интересующему вас компьютеру из любой точки земного шара.

Обычно троянских коней делят на три группы:

- **Приложения, предназначенные для локального доступа к системе.** Первые компьютерные троянские кони использовались для проникновения в защищенные системы. К примеру, администратор Unix мог загрузить популярную игру, не подозревая, что в нее встроен троянский конь, который в первую очередь проверял, не обладает ли текущий пользователь администраторскими привилегиями, и если это так, то он тайно создавал дополнительный администраторский бюджет с известным паролем. В качестве примера такого троянского коня можно привести фальшивое окно входа в систему, которое сохраняет учетные записи пользователей и пароли в текстовый файл перед тем, как вызвать реальную службу входа в систему.
- **Приложения, предназначенные для вредительских действий.** Некоторые троянские кони были специально разработаны для совершения вредительских действий, например: разрушения системы, удаления файлов, форматирования жестких дисков и т. д. Фактически единственная область применения подобных троянских коней для шпиона – это уничтожение доказательств.
- **Приложения, предназначенные для удаленного доступа к системе.** Наиболее подходящими для целей шпионажа являются троянские кони именно из этой категории. Иногда таких троянских коней шутливо называют RATs, то есть «крысами» (этую английскую аббревиатуру расшифровывают как Remote Access Trojans или Remote Administration Tools – троянские кони с

удаленным доступом или средства удаленного администрирования). С помощью подобных троянских коней потенциальный шпион может удаленно наблюдать за целевым компьютером и управлять им по сети.

Важно отметить, что, в отличие от вирусов, программа-тロян не занимается самовоспроизведением. После установки программы в системе троянский конь не пытается создать свои копии и установить их на других компьютерах. Если программа все-таки занимается самовоспроизведением, то ее называют вирусом, или «червем». (Тем не менее многие вирусы распространяются по принципу троянского коня, например, в виде вложений электронной почты, тайно отправляемых ничего не подозревающему пользователю. Вирусы, используемые в целях шпионажа, обсуждаются в главе 13.)

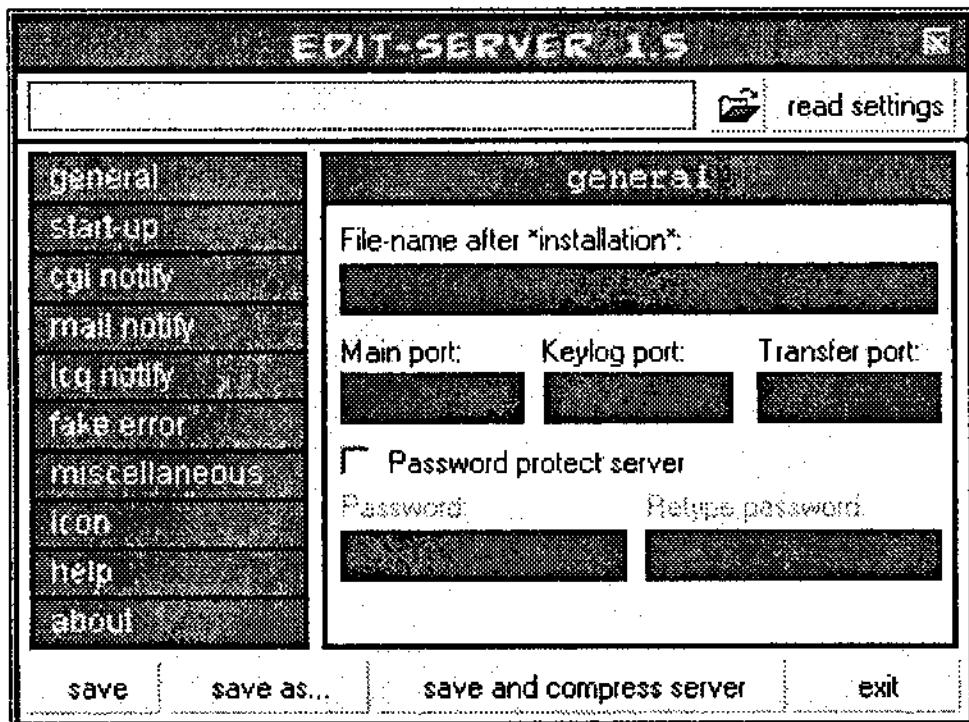
## АЛГОРИТМ РАБОТЫ ТРОЯНСКОГО КОНИ

Ваш маленький братец объясняет, что все троянские кони используют общий принцип работы. Ничего не подозревающий пользователь совершает некоторое действие, приводящее к сохранению троянского коня на жестком диске пользователя. К появлению троянского коня может привести открытие определенного почтового вложения, просмотр веб-страницы либо запуск загруженного приложения. После установки в системе троянского коня он либо немедленно запускается, либо ожидает следующей перезагрузки системы. При этом, как правило, модифицируются ключи реестра и другие файлы автозагрузки, благодаря чему впоследствии запуск троянского коня осуществляется при каждой загрузке Windows.

Такие троянские кони идеально подходят для выполнения многих шпионских задач, поэтому мы сосредоточим наше внимание на их принципах работы. Как правило, троянский конь состоит из трех частей: серверной, клиентской и редактора сервера:

- **Серверная часть.** Серверная часть представляет собой программный код, установленный на удаленном компьютере, представляющем интерес для шпиона. Различные серверные части обладают различной функциональностью, начиная от троянского приложения размером в несколько сотен килобайт, которое умеет делать практически все, что угодно, до небольших троянских коней, называемых «загрузчиками». Троянский конь-«загрузчик» размером около 20 Кб не вызовет такого подозрения, как серверная часть в 200 Кб и более. В соответствии со своим названием троянский «загрузчик» осуществляет загрузку основного серверного приложения с расширенными возможностями. Запущенный на целевом компьютере программный код серверной части открывает порт, за которым может осуществляться наблюдение и через который могут выполняться команды. Чем меньше вы будете выполнять действий, тем лучше: минимум шпионских потребностей – загрузка файлов с целевого компьютера и, возможно, мониторинг клавиатуры.

- **Клиентская часть.** Клиентское приложение предназначено для отправки команд на сервер и получения ответных данных. Вы задаете в клиенте IP-адрес целевого компьютера, и, если серверная часть в данный момент запущена, происходит установка соединения между компьютерами через определенный порт, по которому и осуществляется обмен пакетами TCP и UDP. Во многих троянских конях присутствует даже функция шифрования, помогающая скрыть реальное содержимое пересылаемых пакетов. Как правило, клиентская часть обладает дружественным пользователю интерфейсом, поэтому вам не придется разучивать замысловатые команды для работы с серверной частью.
- **Редактор сервера.** Последним компонентом приложения троянского коня с удаленным доступом является Редактор сервера (его вид показан на рис. 9.1). Эта утилита используется для настройки сервера перед его размещением на целевом компьютере. Большинство серверов обладают широкими возможностями в плане настройки, и вы сможете задать в них такие параметры, как, например, имя исполняемого файла серверной части, номер используемого порта, способ запуска сервера и пароль к нему, чтобы ограничить доступ.



**Рис. 9.1.** Редактор сервера для троянского коня NetDevil с широкими возможностями настройки

Перед тем как отправлять запросы на сервер, вы должны выяснить IP-адрес целевого компьютера. После запуска серверная часть троянского коня постоянно следит за состоянием определенного порта. Поэтому, чтобы инициировать общение с сервером, вам необходимо знать его IP-адрес. (Некоторые троянские приложения используют порт по умолчанию либо фиксированные порты для упрощения процесса идентификации. В процессе сканирования портов, обсуждению которого посвящена глава 10, взломщики обычно проверяют наиболее часто используемые порты, чтобы выявить уже установленных троянских коней (и не тратить

время на установку собственных). К примеру, если во время сканирования был обнаружен активный порт под номером 27374, то, скорее всего, на компьютере установлен троянский конь Sub7 Trojan, использующий по умолчанию именно этот порт.)



Михаэль Симовиц осуществляет поддержку сайта с информацией о существующих троянских конях, включая используемые ими порты и т. д.: чтобы ознакомиться со списком, посетите веб-сайт [www.simovits.com/nyheter9902.html](http://www.simovits.com/nyheter9902.html).

Существуют различные методики определения IP-адреса целевого компьютера. Серверные части некоторых троянских коней умеют делать это за вас, отсылая эти данные по электронной почте, через службу уведомлений мгновенных сообщений либо выполняемые на веб-страницах сценарии CGI.

## Риски: троянские кони международного значения?

2 февраля 2000 года, Государственный департамент Соединенных Штатов разослал срочную телеграмму в 170 своих посольств по всему миру с предупреждением о необходимости немедленного удаления со всех компьютеров в течение пяти дней пакета программного обеспечения, предназначенного для бюджетного планирования.

После ужесточения мер безопасности за несколько месяцев до этого (с последующим арестом одного российского дипломата, подозреваемого в государственном шпионаже) кое-кто занервничал по поводу программного пакета, разработанного компанией Synergy International Systems, который использовался для бюджетного и стратегического планирования.

Отдел дипломатической безопасности госдепартамента США выяснил, что работники компании Synergy, многие из которых являлись бывшими гражданами СССР, регулярно посещали офисы различных министерств для установки либо обслуживания программного обеспечения. Госдепартамент заключил эксклюзивный контракт на сумму в \$1 000 000 на разработку программного обеспечения, предназначенного для обработки не секретной, но достаточно конфиденциальной информации.

Разработка первых приложений началась в середине 90-х в посольстве США в Москве, и работникам посольства настолько понравился этот программный продукт, что, в конце концов, его начали использовать в посольствах Соединенных Штатов по всему миру. Эта программа стала предметом гордости армянского программиста Ашота Гованесяна, ставшего основателем компании Synergy.

Во внутренней докладной записке Государственного департамента, датированной 1 февраля 2000 года, было сказано, что целью настоящего расследования является «помощь в обнаружении и искоренении любого программного кода, который может содержать троянских коней, компьютерные вирусы либо другой враждебный программный код». ФБР и Управление национальной безопасности применили контрразведывательные меры и проанализировали несколько миллионов строк программного кода в поисках чего-то необычного. В результате расследования оказалось, что компания Synergy не сделала ничего предосудительного, и она по сей день занимается выпуском ответственных программных систем управления базами данных.

Похожая ситуация имела место в декабре 2002 года, когда ФБР проводило расследование по делу компании Ptech Incorporated, из штата Массачусетс, производителя корпоративного программного обеспечения. Инвестором компании являлся некий Ясин Аль-Кади, бизнесмен из Саудовской Аравии. Государственная разведка предположила, что этот бизнесмен мог заниматься финансированием террористических группировок, в том числе и Аль-Каиды. В средствах массовой информации прозвучала идея о том, что в программных продуктах, используемых правительством Соединенных Штатов и целой тысячей других коммерческих компаний, могли находиться троянские кони, написанные по заказу Бен Ладена.

Правительство признало полную непричастность Ptech к каким-либо противозаконным действиям, однако в январе 2003 года ранее процветавшая компания, имевшая в своем штате 65 сотрудников, сократила их количество до 10 и лишилась практически всяких перспектив для своего восстановления.

Серверная часть может быть написана практически на любом языке программирования, а поскольку для многих троянских коней в сети Интернет выложены исходные коды, то при желании, взяв за образец существующие приложения, вы можете заняться написанием собственного троянского коня. Самыми незаметными получаются троянские программы, написанные на С/C++ и ассемблере – по сравнению с программами, написанными на языках высокого уровня, таких как, например, Visual Basic (хотя среди разработчиков троянских коней огромной популярностью пользуется Delphi), для которых тем не менее также существуют способы оптимизации размеров исполняемых файлов.

## КАК ИЗБЕЖАТЬ ОБНАРУЖЕНИЯ ТРОЯНСКОГО КОНИ

Для того чтобы троянский конь смог успешно выполнить свою шпионскую миссию, он должен быть незамечен как для пользователя, вручную анализирующего состояние системы, так и для специальных

утилит, разработанных для обнаружения троянских коней (используемые для этого технологии и инструментарий описаны в разделе «Контрмеры» данной главы). Известны следующие способы распространения троянских коней, позволяющие отвлечь внимание пользователя:

- **Манипулирование доверием.** Если вы получаете письмо от известного вам человека, то вероятность того, что вы, не задумываясь, откроете его, выше, чем при получении послания от незнакомца. Эта особенность человеческой психики используется для маскировки отправителя письма под доверительный источник, тогда как на самом деле в письмо вложено тело троянского коня либо ссылки на веб-страницы, с которого этот троянский конь может быть установлен. (То есть такое письмо может служить всего лишь билетом на загрузку троянского коня с удаленного компьютера.)
- **Маскировка расширения файла.** Поскольку большинство пользователей достаточно умны, для того чтобы не открывать подозрительные вложения с расширением .exe, имя файла может быть замаскировано. Один из часто используемых способов – добавление в имя файла дополнительных пробелов, например: sexupixs.jpg-----.exe, где под символами «-» мы подразумеваем пробелы. Если имя файла достаточно длинное, чтобы целиком уместиться в строке почтового клиента, пользователь просто не увидит последнюю часть имени с расширением и будет полагать, что открывает простую картинку JPG. К сожалению, в популярных программах Microsoft Outlook и Outlook Express существует целый ряд уязвимых мест, которые позволяют передавать троянских коней под видом безобидных файлов.
- **Использование порта, не ассоцииированного ни с какими другими троянскими конями.** Многие троянские приложения применяют для обмена информацией между сервером и клиентом порт по умолчанию. В сети Интернет можно найти списки используемых троянами портов, и опытный пользователь может воспользоваться командой netstat -a и выяснить, не является ли один из перечисленных портов активным. Если применяемый вами троянский конь позволяет выбирать порт, назначьте ему уникальный номер, который не связан с известным троянским конем (при этом лучше выбирать порты с большим номером, поскольку это снижает вероятность конфликта с какой-то из стандартных служб – системные службы обычно используют порты с малыми номерами).
- **Маскировка в списке задач.** Многие троянские кони, подобно программам мониторинга клавиатуры, могут не отображаться в списке активных задач, как мы обсуждали в главе 8. В Windows 2000/XP добиться невидимости сложнее, поэтому вам

придется дать процессу не вызывающее подозрений имя, чтобы его можно было принять за часть операционной системы. Когда потенциальная жертва взглянет на список активных процессов либо просмотрит список автозагрузки в соответствующей папке и ключах реестра, она должна принять троянского коня за обычную службу. К примеру, название троянского процесса Explorer.exe не вызовет подозрений, поскольку всем известен стандартный процесс explorer.exe (название которого состоит из символов нижнего регистра).

Чтобы обмануть автоматические средства обнаружения троянских коней, необходима дополнительная смекалка и определенные технические знания. Вот перед вами некоторые популярные подходы:

- **Разработка новой серверной части.** Многие разработчики троянских приложений выкладывают в Интернете исходные коды своих творений. Поэтому, обладая некоторыми навыками программирования, вы можете видоизменить существующие программы либо составить из кусков различных программ своего собственного троянского коня. Уникальный троянский конь может быть пропущен антивирусным программным обеспечением либо специальными утилитами для защиты от троянских коней. Главное – предварительно проверить, обнаруживается ли ваш самодельный троянский конь с помощью последних популярных утилит обнаружения.
- **Модификация существующей серверной части.** Антивирусные программы и утилиты, специально предназначенные для обнаружения троянских коней, обычно осуществляют поиск уникальной последовательности байт или проверку значений контрольной суммы в файлах, которые могут являться троянскими конями. Воспользовавшись hex-редактором для модификации байтов, не влияющих на выполнение задач, вы осложните таким программам задачу обнаружения модифицированной серверной части.
- **Архивация серверной части.** Запустив утилиту архивации для создания самораспаковывающегося архива, вы уменьшите исходный размер файла и усложните для специальных программ обнаружение троянского коня по размеру файла или известной последовательности байт.
- **Привязка серверной части к другому приложению.** Существуют специальные утилиты-«переплетчики» (binders), которые позволяют объединять в одном исполняемом файле несколько приложений. При запуске такого файла происходит выполнение всех связанных приложений. При помощи подобной утилиты вы легко можете привязать троянского коня к заслуживающему доверия приложению.

## Инструментарий шпиона: архиваторы, переплетчики, сбрасыватели

Если вы займетесь в Интернете поиском информации по троянским коням и родственным темам, чаще всего вы будете сталкиваться с тремя терминами: архиваторы,\* «переплетчики» (binders) и так называемые сбрасыватели (dropper). Это важные утилиты в арсенале пользователя троянских коней, о которых вы обязательно должны знать.

Архиваторами называют программы, позволяющие уменьшать размер файлов путем их сжатия (удаления избыточной информации). Файлы приложений, сжатые при помощи архиватора исполняемых файлов, могут распаковываться автоматически (в отличие от файлов популярного формата архивирования ZIP). Архиваторы чрезвычайно популярны среди пользователей и разработчиков троянских коней, поскольку они позволяют уменьшать размеры исполняемых файлов и осложняют их обнаружение со стороны специальных программ, осуществляющих поиск уникальной последовательности байт. Наибольшей популярностью пользуется архиватор UPX (Ultimate Packager for Executables), который доступен на сайте <http://upx.sourceforge.net>. Тем не менее популярные архиваторы имеют свой уникальный формат, который легко обнаружить при помощи программного обеспечения, предназначенного для поиска троянских коней.

Переплетчиками (binder) называют приложения, позволяющие связывать несколько программ и помещать их в один исполняемый файл. При запуске исполняемого файла происходит выполнение всех заключенных в нем приложений. Одним из недостатков данной технологии является то, что большинству антивирусных приложений и утилит обнаружения троянских коней известны заголовки популярных переплетчиков, по которым они выявляют такие файлы. Ссылки на популярные переплетчики вы можете найти на веб-сайте [www.tlsecurity.net/exebinder.htm](http://www.tlsecurity.net/exebinder.htm).

\* Хороший обзор переплетчиков можно найти по адресу [http://assiste.free.fr/p/internet\\_les\\_listes/liste\\_binder.php](http://assiste.free.fr/p/internet_les_listes/liste_binder.php) (увы, на французском) и в статье Эда Скудиса на сайте InformIT [http://www.informit.com/isapi/product\\_id~%7B05BA703C-7AE7-4E8B-9DAB-612A5967FF34%7D/element\\_id~%7B2BCFFD79-7D0B-4ADC-AEB2-028C0A07F928%7D/st~%7BEEA4B8BA-4464-4E41-BE37-B668A7ACCF61%7D/content/articlex.asp](http://www.informit.com/isapi/product_id~%7B05BA703C-7AE7-4E8B-9DAB-612A5967FF34%7D/element_id~%7B2BCFFD79-7D0B-4ADC-AEB2-028C0A07F928%7D/st~%7BEEA4B8BA-4464-4E41-BE37-B668A7ACCF61%7D/content/articlex.asp). – Прим. ред.

Сбрасывателями (dropper) называют приложения, содержащие программный код, позволяющий неявно устанавливать и запускать на выполнение троянского коня. Классический пример сбрасывателя – игра Whack-A-Mole, распространившаяся по Интернету в 1998 году. Эта игра на самом деле являлась носителем троянского коня NetBus. Широкий ассортимент сбрасывателей вместе с исходными кодами вы можете найти на сайте [www.megasecurity.org/Droppers.html](http://www.megasecurity.org/Droppers.html).

## СКРЫТАЯ УСТАНОВКА ТРОЯНСКОГО КОНИ

До тех пор, пока вы не установите троянского коня на целевом компьютере, он представляет собой лишь бесполезный набор байтов. Для установки серверной части приложения вы можете воспользоваться двумя способами: удаленным – по сети либо интерактивным – локальным, если вы обладаете физическим доступом к компьютеру.

**СЕТЕВАЯ ИНСТАЛЛЯЦИЯ.** Как и во многих других видах компьютерного шпионажа, при правильном подходе наиболее эффективным и безопасным для вас способом будет удаленная сетевая атака. Однако, поскольку сетевые атаки – явление весьма распространенное, вы можете столкнуться с серьезными защитными мерами, уменьшающими ваши шансы на успех. Успех или неудача распространения троянского коня по сети зависит от сложности вашей цели (которую вы должны были определить к этому моменту).

Если вы полагаете, что интересующий вас объект имеет уязвимые места в сетевой защите, попробуйте воспользоваться следующими способами для скрытого распространения троянских коней:

- **В почтовых вложениях.** Самый популярный способ распространения троянских коней (а именно их серверной части) – через вложения сообщений электронной почты. Когда пользователь открывает вложение (или, в некоторых случаях, просто просматривает содержимое сообщения при помощи Outlook или Outlook Express), происходит инсталляция троянского коня. (Поскольку вам известны почтовые адреса вашей примадонны, такой способ кажется вам заслуживающим внимания.)
- **Через службу мгновенных сообщений.** Троянский конь может быть выслан на целевой компьютер в процессе обмена файлами через службу мгновенных сообщений. Служба мгновенных сообщений идеально подходит для вычисления IP-адреса целевого компьютера. К примеру, если вы общаетесь с кем-то через службу обмена мгновенными сообщениями AOL, то, введя в командной строке команду netstat -n и посмотрев адрес, указанный напротив порта 5190 (стандартного порта службы мгновенных сообщений), вы узнаете IP-адрес искомого абонента.

- **Путем загрузки файлов.** Довольно старый способ установки серверной части троянского приложения сводится к тому, чтобы заставить вашу потенциальную жертву загрузить откуда-нибудь исполняемый файл либо файл с данными (содержащий макро-команды), когда объект даже не подозревает о существовании вложенного троянского коня.
- **Через веб-страницы.** Из-за ошибок в предыдущих версиях Internet Explorer при посещении некоторых разработанных злоумышленниками веб-сайтов во время просмотра могла произойти скрытая установка троянского коня. (Те же самые ошибки, связанные с поддержкой просмотра сообщений в формате HTML, характерны и для Outlook/Outlook Express.) Хотя компания Microsoft постоянно выпускает «заплаты» для всех обнаруживаемых брешей в защите системы, данный подход демонстрирует свою эффективность борьбы с несознательными пользователями, несвоевременно обновляющими браузеры или почтовые клиенты.

Львиная доля успеха по доставке троянского коня к месту назначения зависит от вашей изобретательности. Ваша цель – заставить интересующий вас объект открыть вложение электронной почты, посетить нужный веб-сайт или же выполнить некоторые другие действия для установки и запуска серверной части троянского коня. Быстрое распространение вирусов подчеркивает тот факт, что заставить пользователя сделать что-то не так уж сложно. Такие знаменитые вирусы, как I Love You и Anna Kournikova, играли как раз на природном любопытстве человека, заставлявшего его открывать почтовые сообщения с интересными темами. Существуют и другие типы вирусов, которые после заражения компьютера одного пользователя используют для своего дальнейшего распространения информацию о его личных контактах, то есть адреса электронной почты друзей, знакомых и деловых партнеров, делая ставку на доверие. Просто удивительно, сколько образованных людей, знающих о возможных рисках, становятся жертвами вирусов, распространяемых в явно сомнительных электронных посланиях, написанных на ломаном английском. Советуем вам уделить время изучению некоторых весьма эффективных приемов социотехники, применяемых для распространения вирусов; многие из них подойдут и для распространения троянских коней (краткую статью по этой теме вы можете найти по адресу [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci537875,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci537875,00.html)).

## Шпионский инструментарий: HTML-приложения

Microsoft Internet Explorer обладает поддержкой так называемых HTML-приложений (HTA). По сути, подобное приложение представляет собой HTML-файл с расширением HTA. Файл данного формата может содержать HTML-код, каскадные таблицы стилей (CSS) и программный код, написанный на различных языках сценариев. Когда операционная система обнаруживает файл с расширением HTA, она обрабатывает его, как любой другой исполняемый файл.

Среди хакеров аббревиатуру HTA иногда расшифровывают как «действия троянского коня, приводящие к тяжелым последствиям» (Heavy Trojan Actions), и тому есть веские причины. Георгий Гунинский, посвятивший себя поиску слабых мест в системе безопасности операционных систем Windows, был первым, кто обнаружил, что при помощи веб-страницы, особым способом отформатированной, можно тайно установить HTA на удаленном компьютере во время просмотра этой веб-страницы пользователем. Разработчики троянских коней оперативно отреагировали на это сообщение, начав создание утилит, использующих данную ошибку. Такие утилиты, как GodWill, GodMessage и ExeToHTML, позволяют добавлять троянского коня в HTML-код на веб-странице в виде текста, представленного в шестнадцатеричном виде. По ходу просмотра страницы этот текст преобразовывается в код HTML-приложения, помещаемого в папку Автозагрузка. Все это происходит без ведома пользователя. В результате при следующей загрузке операционной системы автоматически запускается троянский конь. (То же самое уязвимое место присутствует и в Outlook/Outlook Express при просмотре сообщений в формате HTML с внедренными HTML-приложениями).

Большинство производителей антивирусного программного обеспечения достаточно быстро среагировали на эту ошибку, выпустив обновления, позволяющие обнаруживать скрытые HTML-приложения. Компания Microsoft также достаточно оперативно выпустила «заплату», исправляющую данную ошибку. Однако, если антивирусное программное обеспечение отключено либо на целевом компьютере не установлены последние обновления системы безопасности (что случается довольно часто), пользователь подвергается опасности подобной атаки.

Подробные сведения об использовании HTML-приложений вы можете прочесть по адресу <http://msdn.microsoft.com/workshop/author/hta/overview/htaoverview.asp>, а на сайте Гунинского ([www.guninski.com](http://www.guninski.com)) описаны уязвимые места в элементе управления ActiveX ScriptLet.typeLib и другие известные бреши в системе безопасности, которые могут быть использованы в целях шпионажа.

Поскольку источник сетевой атаки сложно отследить, рассмотрите различные способы нападения. К примеру, вместо отправки вашей жертве сообщения с почтовым вложением, заставьте ее посетить некоторый веб-сайт либо загрузить троянское приложение под видом некоторой полезной утилиты. Такие типы атак называют «смешанной угрозой», и они приобретают все большее распространение. Если вашей целью является организация, постарайтесь провести против нее несколько тайных атак. По статистике, ваши шансы в этом случае возрастут, поскольку вероятность того, что кто-то из нескольких членов организации станет жертвой троянского коня и откроет вам путь для дальнейшего продвижения, намного выше.

И наконец, не атакуйте компьютер с IP-адреса, который может вывести на вас. Применяйте для доступа в Интернет общественные терминалы, «позаимствованные» беспроводные подключения к Интернету, открытые почтовые серверы-ретрансляторы или же любые другие точки доступа к сети, которые не могут быть связаны с вами.

**ЛОКАЛЬНАЯ ИНСТАЛЛЯЦИЯ.** Этот способ достаточно прост. Если вы обладаете физическим доступом к целевому компьютеру, то можете установить троянского коня на жестком диске жертвы и отправиться восвояси (однако этот способ не применим в случае с примадонной, за которой вы охотитесь, поскольку ее имение охраняется лучше, чем Белый дом). Вы даже можете выяснить IP-адрес непосредственно на компьютере жертвы. Если существующие меры безопасности не позволяют этого сделать, включите ваше воображение и действуйте творчески. В том случае, когда вы не имеете физического доступа к компьютеру, заставьте интересующий вас объект установить серверную часть за вас. Для этого нужно обладать талантом мошенника и знать, что люди менее подозрительно относятся к обычной почте, чем к источникам в сети Интернет, – особенно если письмо содержит интересную и родственную им тематику.

Предположим, что объектом вашего интереса выступает генеральный директор компании, входящей в список Fortune 500, который, как вам удалось выяснить, обожает роскошные и быстроходные автомобили. Вы нашли в Интернете несколько веб-сайтов производителей автомобилей и загрузили ряд файлов PDF с описаниями и анимационные ролики, сделанные во Flash. Затем, на скорую руку, вы состряпали интерфейс с локальными ссылками на собранные вами файлы и записали все это на компакт-диск (вместе с серверной частью троянского коня, запятанной в скрытой папке). Далее вы заказали профессиональную полиграфию

обложки с логотипом популярного журнала Luxury Car Enthusiast Driver & Track (подписчиком которого оказалась ваша потенциальная жертва). Затем вы печатаете письмо на почтовом бланке журнала вашей собственной разработки, в котором благодарите директора за то, что он является подписчиком журнала, и сообщаете, что на прилагаемом CD-ROM содержатся сравнительные данные по ряду престижных автомобилей.

В файле autorun.inf на компакт-диске задан автоматический запуск интерфейсного приложения, которое, прежде чем вывести на экран ссылки на документацию и рекламные ролики, тайно устанавливает на машине клиента троянского коня. Но даже если на компьютере директора отключена функция автозапуска компакт-дисков, рано или поздно он все равно запустит программу для просмотра картинок Our Top Picks.exe, которая и отвечает за скрытую установку троянского коня. Опустив это послание в почтовый ящик, вы выжидаете несколько дней, прежде чем пытаетесь подключиться к серверу.

## Троянские кони

К середине затянувшейся лекции (проводимой вашим младшим братом) по применению троянских коней вы не выдерживаете и в своей лучшей пародии на Джерри Мак Гвайера восклицаете: «Так покажи же мне этих троянских коней!» Брат объясняет вам, что в сети Интернет можно найти тысячу таких приложений, а какое из них выбрать – зависит от поставленной цели и от используемых целевым объектом мер безопасности. Чем серьезнее предпринятые меры безопасности, тем более незаметный сервер и способ его установки необходимо использовать. (В некоторых случаях можно прибегнуть к модифицированным версиям распространенных троянских коней, чтобы в случае их обнаружения было невозможно определить, стала ли жертва объектом целенаправленной атаки или же пострадала случайно.)

Перед началом использования троянского коня нужно убедиться в его соответствии вашим требованиям. Будьте очень осторожны, поскольку вы играете с огнем. Если вы не видели исходного кода и не являетесь его автором, вы не можете в точности знать, какие функции заложены в клиентской либо серверной части или же редакторе сервера (вы, наверно, удивитесь, однако разработчики подобных программ обычно придерживаются правил чести, поскольку для них чрезвычайно важна репутация в своих кругах.) Имея это в виду, послушайтесь следующих советов:

- Всегда проверяйте работоспособность выбранного вами троянского коня на компьютере, сконфигурированном по образу и подобию компьютера вашей жертвы.
- Если вы не знаете, какое антивирусное ПО либо специальные программы для обнаружения троянских вирусов присутствуют на компьютере вашей жертвы, установите различные популярные версии троянских коней и протестируйте каждый из них.

После успешной инсталляции и запуска серверной части троянского коня воспользуйтесь описанными в конце данной главы контрмерами, чтобы проверить, возможно ли обнаружение троянского приложения при таких условиях.

- Проводите тестирование на компьютере, изолированном от剩余ной сети, если вы не хотите случайно навредить самому себе. При этом примите должные контрмеры по защите компьютера, на котором вы собираетесь испытывать троянского коня, чтобы не допустить его распространения, которое может обернуться против вас.
- После окончания испытаний троянского коня выполните форматирование жесткого диска тестового компьютера, чтобы удалить все возможные остатки недружественного программного кода.

Теперь давайте рассмотрим примеры троянских коней, которые могут использоваться в целях шпионажа. Все троянские приложения можно разделить на три категории: классические троянские кони (впервые появившиеся всего несколько лет назад); новое поколение троянских коней, к которому принадлежат менее известные, однако наиболее смертоносные и скрытные типы; и, наконец, к третьей категории можно отнести коммерческие программы, предназначенные для системного администрирования, которые с успехом могут быть использованы в роли троянских коней.

## КЛАССИЧЕСКИЕ ТРОЯНСКИЕ КОНИ

Первый троянский конь для операционной системы Windows, предполагающий удаленную установку, появился в конце 1990-х годов, причем его распространение сопровождалось шумихой в средствах массовой информации. Некоторые из наиболее знаменитых троянских коней конца 1990-х годов описаны в следующих параграфах.

**NETBUS.** Троянский конь под названием NetBus, написанный Карлом-Фредериком Никтером в марте 1998 года, стал первым популярным троянским конем под Windows, предназначенным для удаленного использования. NetBus уже получил широкое распространение на момент появления трояна Back Orifice (описываемого в следующем абзаце), хотя и не привлек к себе столько внимания. Первые версии NetBus имели гораздо больший объем, чем Back Orifice (BO), но при этом они работали в операционных системах Windows 2000/NT. Троянский конь NetBus пережил несколько версий и, в конце концов, стал основой для нескольких коммерческих продуктов для мониторинга, таких как eBlaster и Spector от компании Spectorsoft ([www.spectorsoft.com](http://www.spectorsoft.com)). Оригинальную же версию программы NetBus вы без труда найдете при помощи любого поискового сервера.

**BACK ORIFICE.** Летом 1998 года группа хакеров, именующая себя «культом мертвый коровы» (cDc – Cult of the Dead Cow), выпустила версию программы Back Orifice, троянского коня, предоставляющего удаленный доступ к компьютерам под управлением Windows 95/98 ([www.cultdead-cow.com/tools/](http://www.cultdead-cow.com/tools/)). Своими действиями группе cDc удалось мастерски привлечь внимание к угрозе со стороны троянских коней с удаленным доступом. Год спустя cDc выпустила версию Back Orifice для работы под ОС Windows 2000 (BO2K). Со временем версия BO2K превратилась в открытый проект, скорее направленный на разработку законного средства администрирования, чем троянского коня. Работа над этим проектом продолжается и по сей день. За более подробной информацией обратитесь на веб-сайт <http://bo2k.sourceforge.net> (с него можно загрузить саму утилиту).

**SUB7.** Эта программа, написанная хакером по прозвищу МобМэн (Mob-Man), увидела свет в конце 1999 года и очень скоро превратилась в самое популярное и самое распространенное троянское приложение для Windows. В Sub7 имеется целый ряд полезных функций, включая настройку сервера на поиск других возможных жертв троянского коня. Существует множество различных версий программы, многие из которых активно используются до сегодняшнего дня. Все версии Sub7, включая релиз Дефкона, завоевавший репутацию наиболее стабильной версии, можно найти на веб-сайте [http://www.megasecurity.org/trojans/s/subseven/Subseven\\_all.html](http://www.megasecurity.org/trojans/s/subseven/Subseven_all.html).

## ТРОЯНСКИЕ КОНИ: НОВОЕ ПОКОЛЕНИЕ

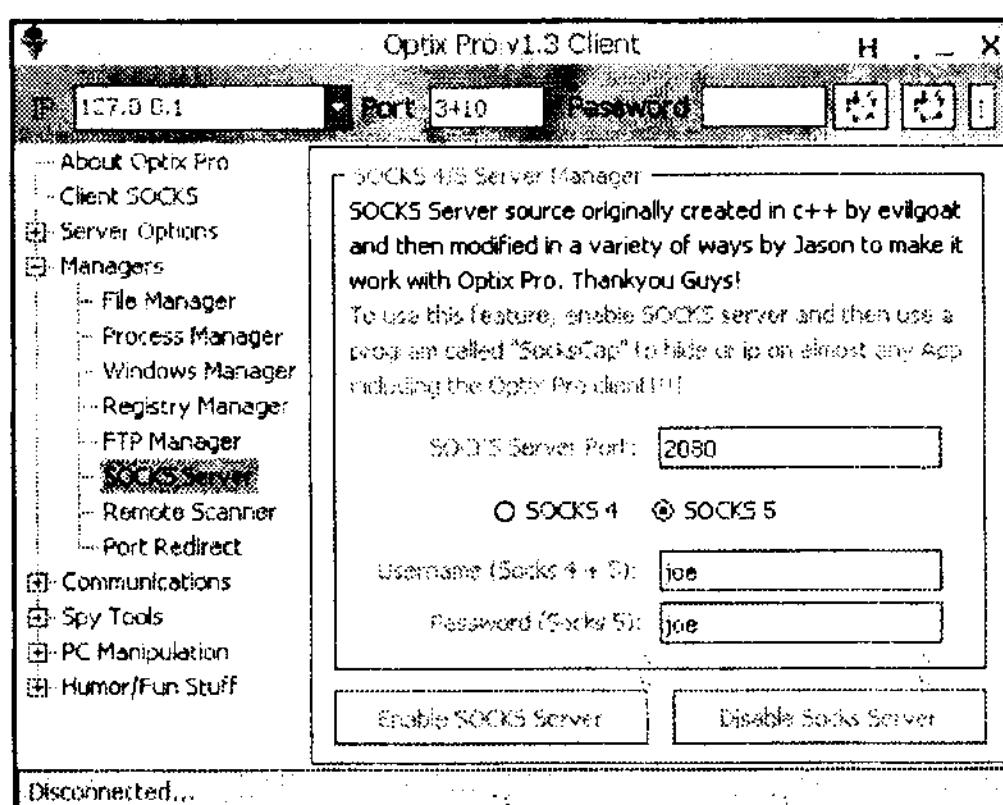
Хотя современные троянские кони имеют много общих базовых функций по сравнению со своими классическими предками, новое поколение этих программ намного сложнее и опаснее. Разработчики троянских коней активно борются с производителями программных средств защиты систем, включая в свои продукты функции отключения брандмауэров и антивирусного программного обеспечения, функции генерации фальшивых сообщений об ошибках в целях скрытия действий программы, усложняя ее обнаружение и лечение; предусматривается даже возможность отсылки уведомлений о запуске зараженного компьютера через интернет-чаты либо по электронной почте.

Некоторые представители нового поколения троянских коней, которые могут быть весьма полезны в целях шпионажа, обсуждаются в следующих параграфах:

**LANFILTRATOR.** Одна из проблем, с которой сталкиваются лица, использующие троянских коней, заключается в том, что если целевая машина подключена к сети Интернет через маршрутизатор, то используемые в этом случае внутренние IP-адреса ничем не помогут при попытке подключения к серверной части троянского коня. Программа LANFiltrator стала одним из первых троянских коней, в котором при работе использовался обратный принцип: поскольку в данном случае обращение клиентской

части к серверу было невозможным, то после своей активизации серверная часть сама выполняла обращение к клиенту. Написанная неким хакером под псевдонимом Read101, эта утилита доступна в сети по адресу [www.digitalsin/cyn/HTML\\_News.html](http://www.digitalsin/cyn/HTML_News.html).

**OPTIX.** В качестве разработчика данной утилиты выступает компания Evil Eye Software (EES), которая выпустила две разновидности программы: облегченную Optix Light и полнофункциональную Optix Pro (интерфейс клиентской части Optix Pro показан на рис. 9.2). Облегченная версия подходит для создания плацдарма на машине клиента, тогда как версия Pro реализует почти все функции, которые только могут быть у троянского коня. Популярная серия троянских коней Optix, скорее всего, в ближайшее время составит серьезную конкуренцию Sub7, как самому распространенному троянскому коню. Утилиты Optix распространяются совершенно бесплатно, но разработчики компании EES специально для вас готовы сделать не подлежащую обнаружению версию любого из своих продуктов всего за \$300. Optix и другие троянские кони производства компании EES можно найти на сайте компании по адресу [www.evileyesoftware.com](http://www.evileyesoftware.com).



**Рис. 9.2.** Клиентская часть программы Optix Pro Trojan, в которой отображаются готовые для выполнения на удаленном сервере команды, включая команду извлечения хешированных паролей

**NET-DEVIL.** Net-Devil – весьма популярная утилита, представляющая собой троянского коня с мощными возможностями, способного преодолевать защиту работающего брандмауэра и антивирусного программного обеспечения. Он зарекомендовал себя как весьма стабильный продукт, хорошо работающий под операционной системой Windows XP. После выхода ряда обновленных версий автор программы Niles прекратил разработку новых версий в начале 2003 года. Net-Devil отлично подходит на роль шпионской программы, а загрузить его вы можете с сайта [www.net-devil.com/main.html](http://www.net-devil.com/main.html).

## Тактика: поступим, как захватчики Трои

Если вы хотите научиться эффективному использованию троянских коней в качестве неотъемлемой части вашего шпионского арсенала, вам необходимо потратить некоторое время, чтобы лучше узнать о культуре разработчиков и пользователей троянских коней.

Один из наиболее популярных сайтов для получения информации о разработчиках подобных программ – сайт TrojanForge ([www.trojanforge.net](http://www.trojanforge.net)). На сайте открыт форум, зарегистрированные участники которого могут обмениваться любой информацией по программам – троянским коням и утилитам для их обнаружения. Здесь даже размещен раздел новинок, в котором авторы этих программ могут анонсировать свои последние творения и поддерживать обратную связь с другими разработчиками или пользователями.

Само собой разумеется, что множество производителей антивирусного программного обеспечения или утилит для обнаружения троянских коней регулярно посещают такие сайты, как TrojanForge, чтобы следить за своими противниками. Легко догадаться, что эта информация не ускользает и от внимания разведывательных управлений, которые заинтересованы в использовании троянских коней в целях разведки и потому не менее регулярно посещают подобные сайты. (Прежде всего, для того чтобы находиться в курсе событий и использовать все новые разработки, а также знать, против каких приемов необходимо придумывать контрмеры.) С другой стороны, рассчитывать на появление в разделе объявлений информации от ЦРУ о разработанном ими новом троянском коне, предназначенном для тайного сбора данных о давно устаревших противоракетных комплексах Северной Кореи, вам, пожалуй, не стоит.

Практически любой подпольный веб-сайт содержит информацию о троянских конях, включая интернет-ссылки, по которым их можно загрузить; мы же перечислим несколько наиболее популярных веб-узлов, которые целиком посвящены данной тематике:

- **Evil Eye Software:** На сайте имеется форум и ссылки для загрузки троянских коней, разработанных компанией Evil Eye Software ([www.evileyesoftware.com](http://www.evileyesoftware.com)).
- **Fearless:** Здесь вы также сможете найти как форум, так и ссылки от разработчиков троянского коня Fearless ([www.arestyoufearless.com](http://www.arestyoufearless.com)).
- **SinRed:** Новости и файловый архив от команды разработчиков SinRed ([www.sinred.com](http://www.sinred.com)).

- **MegaSecurity:** Сайт, посвященный теме компьютерной безопасности вообще и троянским коням в частности ([www.megasecurity.org/Main.html](http://www.megasecurity.org/Main.html)).

Если в ваши планы входит посещение одного из вышеперечисленных либо любого другого подпольного сайта, убедитесь в достаточной защищенности собственной компьютерной системы (при помощи брандмауэров, последних установленных обновлений для своего браузера, а также программного обеспечения, предназначенного для обнаружения вирусов и троянских коней). Кроме того, если вы опасаетесь, что за вами могут следить, воспользуйтесь одним из средств обеспечения собственной анонимности, о которых будет рассказано в главе 10.

## КОММЕРЧЕСКИЕ ПРОГРАММНЫЕ ПРОДУКТЫ

В предыдущих главах книги мы успели рассказать вам о многих коммерческих программных продуктах, предназначенных в первую очередь для системных администраторов, которые тем не менее часто могут быть использованы не по своему прямому назначению. Похоже обстоит ситуация и с программами, предназначенными для удаленного администрирования систем и обладающими функциональностью, характерной для обычных троянских коней (за исключением развлекательных функций, например, удаленного управления выездом каретки CD-привода). Поскольку такие коммерческие программные продукты являются абсолютно законными, антивирусные и другие программы обнаружения троянских коней не находят их, даже если они были установлены кем-то без вашего ведома.

Еще одно преимущество подобных приложений состоит в том, что они могут быть уже установлены на целевом компьютере обычным администратором, что еще больше упрощает вашу задачу (вам останется воспользоваться вашей копией программы для удаленного доступа к целевому компьютеру). Подобно троянским коням, эти коммерческие приложения используют фиксированные номера портов по умолчанию (на веб-странице [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers) вы можете найти перечень зарегистрированных портов, а также приложения и протоколы, которые их используют); к примеру, активность TCP-порта 5631 свидетельствует о том, что на компьютере запущена популярная утилита pcAnywhere. У разных коммерческих программ администрирования имеются свои уязвимые места, поэтому, если на интересующем вас компьютере установлена одна из таких программ, потратьте время на сбор информации о ней. Кроме того, легко можно найти утилиты, которые умеют выполнять подбор паролей к коммерческим приложениям, защищающим соединения с помощью паролей. Назовем две наиболее популярные утилиты, предназначенные для удаленного администрирования:

- **pcAnywhere.** Программа pcAnywhere от компании Symantec представляет собой популярное корпоративное средство для удаленного управления компьютером через сеть либо по коммутируемому

каналу. В приложение встроены функции защиты информации от перехвата, но если злоумышленник получит физический доступ к компьютеру и установит на нем это приложение, то он сможет использовать его для шпионажа. Если вы хотите подробнее узнать об этом программном продукте, посетите официальную веб-страничку программы по адресу [www.symantec.com/pcanywhere/](http://www.symantec.com/pcanywhere/).

- **VNC.** VNC (Virtual Network Computing) – свободно распространяемый по принципу открытого кода мультиплатформенный клиент-серверный программный продукт, обеспечивающий удаленный сетевой доступ к графической оболочке рабочей станции. Программа VNC позволяет работать с компьютером из любой точки земного шара, где есть подключение к Интернету. Загрузить эту программу можно с сайта компании AT&T Laboratories Cambridge [www.uk.research.att.com/vnc/](http://www.uk.research.att.com/vnc/). Расширенная версия VNC (также распространяемая вместе с исходными кодами) под названием TightVNC не менее популярна у системных администраторов за счет повышенной эффективности и защищенности. Эту версию можно найти по адресу [www.tightvnc.com/](http://www.tightvnc.com/).

Вернемся к нашей истории. После того, как ваш младший брат изложил всю известную ему информацию о троянских конях, вы решили отправить вашей певице электронное послание с вложенным троянским конем Optix Lite (разумеется, из интернет-кафе с временного почтового ящика). В ваши планы входило заражение компьютера жертвы этим небольшим троянским конем для создания плацдарма и последующей загрузки Optix Pro, чтобы иметь возможность наблюдать за всеми ее действиями. Вы воспользовались вашими талантами в эпистолярном жанре, чтобы написать вашей примадонне письмо якобы от известного ей человека, которое, вы знаете, она откроет. Вы пребываете в уверенности, что электронный шпионаж с вашей стороны позволит выяснить изобличительные факты из жизни этой певицы и написать заказанную статью, чтобы обеспечить себе путевку назад – в серьезную журналистику.

## Контрмеры

Теперь представим себя на месте «хорошего парня», нанятого по контракту этой самой поп-дивой для защиты своих интересов. Поскольку вопросами обеспечения физической безопасности резиденции занимается команда бывших работников службы контрразведки и агентов ФБР, вашей задачей является обеспечение компьютерной безопасности, в частности выслеживание фанатичных поклонников.

Для приема входящих сообщений электронной почты на адрес поп-дивы используется написанный вами фильтр, который проверяет приходя-

щие письма на предмет вирусов. Ее персональный адрес электронной почты неизвестен широкой публике, тем не менее иногда вам приходится сталкиваться с письмами от неизвестных людей, инфицированными вирусом SirCam, которые, скорее всего, были отправлены через зараженный компьютер одного из ее знакомых. Но однажды вы обнаружили в Журнале нечто более интересное – странное письмо, в котором заголовок Отправителя (From:) не соответствует его подробному обратному адресу Received: (который обычно не отображается), что очень похоже на фальсификацию сообщения, пришедшего якобы от одного из ее друзей. (Более подробно об отправлении сообщений электронной почты с фальшивых адресов и о том, как изучать заголовки электронных сообщений, вы можете прочесть по адресу [www.stopspam.org/email\\_headers/headers.html](http://www.stopspam.org/email_headers/headers.html).) Интересно, что в присланном сообщении содержался не вирус, а небольшой троянский конь.

Это фальшивое сообщение было подготовлено слишком грамотно, чтобы считать его творчеством малолетних хакеров, и у вас возникло подозрение, что вы столкнулись с опытным шпионом. Доложив об этом начальству, вы приняли решение активизировать троянского коня на тщательно контролируемом компьютере. Если кто-то попытается удаленно подключиться к нему, вы намерены выследить этого злоумышленника. Итак, несколько дней спустя некто активирует троянского коня, и вы начинаете записывать в журнал все сообщения и пытаться определить IP-адрес источника атаки.

Спустя несколько дней, в течение которых неизвестный шпион вел наблюдение за компьютером и загружал специально подготовленные вами файлы, ваш начальник решил, что этого вполне достаточно и позвонил своим друзьям из Министерства юстиции (вышеперечисленные действия уже являются нарушением целого ряда статей Закона о прослушивании и других законодательных актов по компьютерным преступлениям, а их жертва активно поддерживала нового президента на последних выборах). Вы передали все собранные материалы вашему другу из ФБР и через неделю узнали из газет об аресте в интернет-кафе некоего фаната, который занимался загрузкой электронных писем, адресованных охраняемой вами поп-диве, к компьютеру которой ему удалось подключиться. Совершенное им преступление просто не окупилось.

Хотя троянские кони могут отличаться незаметностью и коварностью, существует целый ряд мер, при помощи которых вы можете обеспечить себе относительную защищенность от шпионов. Некоторые меры обеспечения безопасности обсуждаются в следующих параграфах.

## Сетевая защита

Чтобы обнаружить и победить троянских коней, необходимо прибегнуть к следующим контрмерам:

- **Анализ сетевых подключений.** Серверная часть приложения троянского коня использует для общения с клиентом определенный

порт. Если вы просмотрите список открытых портов и обнаружите один или несколько портов, не связанных с системой или известными вам приложениями, это может служить признаком наличия в системе установленного троянского коня.

- **Использование брандмауэров.** Брандмауэры позволяют блокировать исходящие попытки установки сетевых подключений, мешая действиям троянских коней при попытках подключения к Интернету. Однако учтите, что некоторые разновидности троянских коней умеют уничтожать активный процесс брандмауэра (на что производители брандмауэров ответили внесением изменений в программный код, которые делают удаление процесса более трудным). Вам следует периодически проверять, присутствует ли значок работающего брандмауэра на Панели задач Windows, хотя особо коварные троянские кони могут после удаления процесса выводить фальшивый значок, убеждающий пользователя в том, что он находится в безопасности.
- **Мониторинг сетевого трафика.** При помощи анализатора сетевых пакетов можно отслеживать входящий и исходящий трафик вашего компьютера. Подозрительные обращения, нестандартные порты и IP-адреса неизвестного происхождения свидетельствуют о возможном наличии на вашей машине троянского коня. Некоторые троянские кони умеют шифровать передаваемые ими данные, поэтому обнаружение зашифрованной информации либо данных, не соответствующих используемому протоколу, также может являться предостерегающим знаком.

Перечисленные здесь меры, пригодные для защиты от разных видов сетевых атак, более полно обсуждаются в разделе «Контрмеры» главы 10.

## Использование мониторов реестра и программ проверки целостности файлов

Для того чтобы обеспечить свою загрузку при каждом запуске Windows, троянский конь, как правило, модифицирует соответствующие ключи реестра, добавляя ссылки в папку Автозагрузка либо внося изменения в один из стандартных загрузочных файлов, таких как AUTOEXEC.BAT или WIN.INI (для старых версий Windows).

Такие изменения можно выявить при помощи программ мониторинга реестра и проверки целостности файлов. Утилиты для мониторинга реестра позволяют собирать информацию о добавляемых либо изменяемых ключах реестра. Программы проверки целостности файлов анализируют папки на жестком диске компьютера и вычисляют хешированное значение контрольной суммы (например, по алгоритму MD5) для каждого файла и сохраняют в качестве эталона. При повторном запуске утилиты проверки целостности хешированные значения вычисляются заново, а

затем сравниваются с сохраненными эталонами. Если значения не совпадают, следовательно, данный файл был модифицирован с момента последнего запуска утилиты, и если это файл приложения либо же системный, проверьте, нет ли на вашем компьютере установленного троянского коня. При помощи подобных утилит вы сможете защититься от новейших троянских коней, которые не обнаруживаются даже специальными программами.

В качестве примера приведем две наиболее популярные утилиты для мониторинга состояния реестра и проверки целостности файлов.

- **RegistryProt:** Данная утилита производства компании CSDiamond предназначена для уведомления пользователя о любых изменениях ключей реестра. Программу можно загрузить с веб-сайта <http://www.diamondcs.com.au/index.php?page=regprot>.
- **CFI LANguard System Integrity Monitor:** Эта программа предназначена для мониторинга всех файловых операций в системе Windows 2000/XP. Вы можете загрузить LANguard с веб-страницы <http://www.gfi.com/pages/files.htm>.



Дополнительную информацию по программам проверки целостности реестра и файлов, а также другим утилитам, способным обнаруживать и останавливать работу троянских коней, вы можете найти в списке свободно распространяемых утилит, предназначенных для обеспечения компьютерной безопасности, на веб-сайте [www.wilders.org/free\\_tools.htm](http://www.wilders.org/free_tools.htm).

## Использование антивирусного программного обеспечения

Большая часть пакетов антивирусного программного обеспечения содержит в своих базах только наиболее распространенные из троянских коней. Производители антивирусного ПО акцентируют свое внимание, прежде всего, на борьбе с вирусами, ставя вопрос обнаружения троянских коней на второе место.

Из наиболее уважаемых разработчиками и пользователями средств борьбы с троянскими конями можно назвать антивирусное ПО от Касперского (KAV), отлично зарекомендовавшее себя в обнаружении как вирусов, так и троянских коней\*.

\* Более подробную информацию по Антивирусу Касперского вы можете прочесть на официальном веб-сайте [www.kaspersky.com](http://www.kaspersky.com) (причем даже на русском языке. – *Прим. перев.*

## Использование специального ПО для обнаружения троянских коней

Для полноценной защиты системы кроме антивирусного ПО вам необходимо установить специальные программы для обнаружения и удаления троянских коней. Производители подобных программ, как правило, не столь знамениты, как компании-производители антивирусного программного обеспечения, тем не менее благодаря своей узкой специализации они более тщательно подходят к решению вопроса, постоянно отслеживая происходящие события, в том числе и на подпольных сайтах. Кроме того, лица, использующие троянских коней в своих целях, меньше всего ожидают от вас применения специального программного обеспечения для защиты от троянских коней.

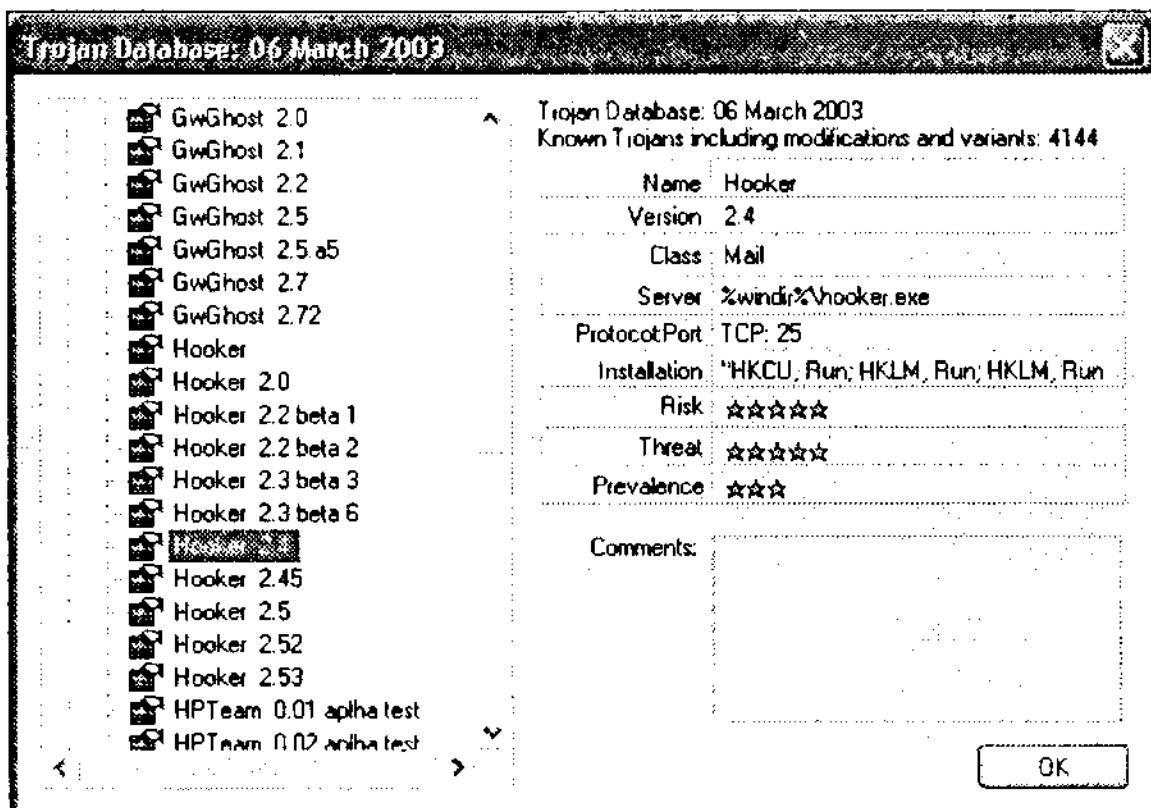
Важно понимать, что такое ПО позволяет обнаруживать только известных троянских коней, которые перечислены в базе данных этого приложения (эти базы данных следует регулярно обновлять, подобно тому, как вы это делаете для ваших антивирусных программ). Малораспространенная модификация троянского приложения может быть вообще прощена такой программой. Поэтому, если вы считаете себя объектом серьезной шпионской кампании, позаботьтесь о многоуровневой защите вашей системы.

На рынке представлено немало программных продуктов, предназначенных для защиты от троянских коней, которые, по утверждениям их разработчиков, позволяют обнаруживать и обезвреживать практически любые их разновидности. В разных обзорах встречаются разные оценки эффективности обнаружения с помощью тех или иных программ, однако наибольшее количество положительных отзывов относится к следующим утилитам:

- **Trojan Defence Suite (TDS)**, утилита стоимостью в \$49, демонстрационную версию которой можно загрузить на веб-сайте <http://tds.diamondcs.com.au/>.
- **BOClean**, программа по цене \$39,95. Ее можно заказать на сайте [www.nsclean.com/boclean.html](http://www.nsclean.com/boclean.html).
- **Tauscan**, утилита стоимостью \$29,95 плюс свободно распространяемая пробная версия (Tauscan в работе изображена на рис. 9.3), официальный сайт разработчика [www.agnitum.com/products/tauscan/](http://www.agnitum.com/products/tauscan/).
- **Trojan Hunter**, программный пакет за \$34,95, оценочную версию которого можно найти в Интернете по адресу [www.misec.net/trojanhunter/](http://www.misec.net/trojanhunter/).

Компания Mischel Internet Security, разработчик программы Trojan Hunter, предлагает вашему вниманию весьма любопытную свободно распространяемую программу-симулятор троянского коня. С ее помощью вы

можете проверить защищенность системы без риска для себя. Найти эту утилиту можно на веб-сайте [www.misec.net/trojansimulator/](http://www.misec.net/trojansimulator/).



**Рис. 9.3.** Утилита Tauscan обнаружила троянского коня, предназначенного для мониторинга клавиатуры, выведя его описание и характеристики

## Избавление от троянских коней

Хотя большинство специальных утилит позволяет автоматически удалять обнаруженных троянских коней, в подобной ситуации рекомендуется скопировать важную информацию (на CD-ROM, к примеру), а затем переформатировать жесткий диск и переустановить Windows. Пускай такие меры не покажутся вам избыточными, ведь никто не знает, что успела наделать зловредная программа с вашей системой, поэтому иногда лучше перестраховаться, чем потом все время сожалеть. (Поскольку даже файлы с данными могут оказаться заражены макровирусами, прежде чем копировать файлы на чистую систему, проверьте их антивирусным программным обеспечением с самыми последними обновлениями баз.)

Существует также несколько способов ручного удаления обнаруженных троянских приложений. Во-первых, необходимо разобраться, с чем вы имеете дело, идентифицировав, к примеру, открытый порт, связанный с установленным на вашей системе троянским конем. Задайте на поисковом сервере имя найденного вами троянского коня, чтобы найти дополнительную информацию о нем. Описания популярных троянских коней вы можете найти на многих сайтах производителей антивирусного программного обеспечения вместе с инструкциями по их удалению. Если вам удастся найти копию клиентской части троянского коня, серверная часть которого не защищена паролем, с его помощью вы сможете удалить приложение – троянского коня (в большинстве клиентов встроена функция деинсталляции и удаления серверов). Для этого скопируйте клиента на пораженный компьютер, выберите в качестве целевого IP-адреса 127.0.0.1 (localhost) и попытайтесь подключиться к серверу.

## Использование программ сторонних разработчиков

Регулярные скандалы с обнаружением ошибок системы безопасности в продуктах компании Microsoft, таких как Internet Explorer, Outlook/Outlook Express, могут послужить толчком к замене вашего браузера и почтового клиента на соответствующие программы сторонних разработчиков. Хотя корпорация Microsoft продолжает выпускать «заплаты» для своих продуктов в случае обнаружения новых уязвимых мест, огромное число известных на данный момент времени ошибок (и возможность существования многих неизвестных ошибок) увеличивает вашу незащищенность от сетевых атак.

## Заключение

Троянские кони являются весьма эффективным средством компьютерного шпионажа, в особенности против неосведомленных и неподготовленных лиц. Большинство сетевых атак с использованием троянских коней осуществляется при помощи вложений электронной почты, веб-страниц либо загружаемых пользователем модифицированных приложений, содержащих код троянского коня, обеспечивающего тайный вход для шпиона, который может прескокойно наблюдать за действиями пользователя, находясь за тысячу миль от него. Если вы обладаете физическим доступом к компьютеру, задача по установке троянского коня облегчается, поскольку вам не будут мешать сетевые средства защиты данного компьютера.

Исходя из вышеизложенного, можно прийти к выводу о том, что Святой Грааль разработчиков троянских коней (приложение, которое невозможно обнаружить или удалить) уже давно должен был быть написан. Тем не менее, воспользовавшись предлагаемыми в данной главе контрмерами, вы сможете обнаружить и обезвредить практические любое из существующих троянских приложений.

Новое поколение троянских коней развивается стремительными темпами, и сейчас разработчики троянских коней и программ для их обнаружения постоянно борются друг с другом. Официальные источники, посвященные рассмотрению вопросов безопасности, редко размещают обзоры о разработке новых троянских коней, поэтому, чтобы находиться в курсе событий, советуем вам посетить парочку подпольных сайтов.

И не забывайте с осторожностью относиться к подаркам в греческом стиле – что если в них спрятан троянский конь?

## Глава 10

# Сетевое наблюдение

«Субботним вечером я был в центре, выполняя задания для ФБР...»  
The Hollies, «Long Cool Woman», *Distant Light*

## Знакомство с сетевым шпионажем

Даже не имея физического доступа к компьютеру, вы все равно можете следить за ним, если компьютер подключен к сети. Популярность сети Интернет сделала уязвимыми для возможных сетевых атак десятки миллионов компьютеров по всему миру. Когда вы произносите фразу «сетевая атака», большинство людей представляют себе зловредных взломщиков, пытающихся проникнуть внутрь компьютерной системы. Сетевой шпионаж является близким родственником взлома, поскольку, как правило, шпионы используют те же самые приемы и технологии, что и обычные хакеры для взлома компьютерных систем. Основное различие состоит в том, что профессионально подготовленную шпионскую операцию намного труднее раскрыть, чем каждодневные случаи сетевых атак со стороны малолетних взломщиков, нередко оставляющих после себя недвусмысленные следы присутствия.

В этой главе мы поговорим о прослушивании сетей, в которых сигнал передается по кабелю (беспроводным сетевым технологиям посвящена следующая, одиннадцатая глава книги), в том числе об использовании программ перехвата сетевых пакетов, сканеров для поиска уязвимых мест и других средств, часто заимствуемых шпионами у своих, в некотором роде коллег – хакеров. Затем по традиции мы расскажем об эффективных контрахерах, позволяющих защититься от большинства видов сетевых атак.

Поскольку технологиям сетевых атак посвящено немало книг, в данном повествовании мы дадим вам лишь базовую информацию по различным нюансам техники сетевого шпионажа. Для тех из вас, кто хочет повысить свою квалификацию сетевого шпиона, мы приведем множество ссылок на интересные веб-сайты и другие источники информации, обратившись к которым вы почертнете массу дополнительной информации по теме обнаружения и использования определенных слабых мест в защите систем. Ну а перед тем как перейти к изучению тактики, применяемой шпионами для получения доступа к сетевым компьютерам, мы рассмотрим некоторые общие концепции сетевого шпионажа.

## Типы сетевых атак

Рассматривая слабые места в защите системы, которыми способен воспользоваться шпион, можно перечислить тысячу способов реализации сетевых атак. Но если говорить о методиках извлечения конфиденциальной информации, то их существует всего две:

- **Пассивная атака.** Пассивная атака подразумевает извлечение интересующей шпиона информации путем пассивного наблюдения за содержимым отправляемых по сети пакетов данных при помощи некоторой разновидности сетевого монитора. Хотя выявить подобную программу перехвата сетевых пакетов теоретически возможно, но на практике такие атаки с большим трудом поддаются обнаружению.
- **Активная атака.** В ходе активной атаки злоумышленники, используя известные уязвимые места операционной системы или приложений либо в результате несоблюдения политики безопасности, получают возможность искать интересующую их информацию непосредственно на жестком диске компьютера и других электронных носителях информации. Таким образом, можно, например, выкрасть документ, к которому был открыт общий сетевой доступ без задания пароля. Другим примером активной сетевой атаки является работа приложения – троянского коня, тайно отправляющего информацию по сети. Подобная разновидность сетевой атаки рассматривалась в главе 9.

Помимо классификации сетевых атак на пассивные и активные их также делят на целенаправленные и случайные атаки:

- **Целенаправленная атака.** Целенаправленной атака называется тогда, когда при ее реализации ставятся конкретные цели, например получение доступа к определенному компьютеру либо нескольким компьютерам. Такие атаки могут быть удаленными, направленными против компьютера с конкретным IP-адресом либо против сети в целом, если, преодолев меры обеспечения физической безопасности, злоумышленникам удалось получить физический доступ к компьютерам и установить, к примеру, сетевой монитор. Если шпионская атака была инициирована удаленно, ценная информация может быть получена при помощи инструментальных средств для работы со службой имен доменов (DNS), таких как WHOIS, DIG, tracert\*. Целенаправленная

---

\* WHOIS – сокр. от who is who (кто есть кто) – сетевая программа Internet, которая позволяет абонентам обращаться к хранимой в DNS NIC базе данных с запросами о пользователях сети, доменах, доступных сетях и прочих объектах; DIG – сокр. от domain information groper, блок сбора информации о домене; tracert – сокр. от trace route, утилита для трассировки достижимости IP-узла. – Прим. перев.

атака означает, что именно вы по какой-либо причине представляете интерес для шпионов. В этом случае простых контрмер может оказаться недостаточно, чтобы остановить злоумышленников.

- **Случайная атака.** Единственной причиной случайной атаки (а случайные атаки имеют место намного чаще, чем целенаправленные) может выступать тот факт, что некий хакер наткнулся на ваш IP-адрес в ходе сканирования систем на уязвимость. К случайнм атакам нередко прибегают хакеры в поисках плацдарма для начала целенаправленной атаки для хранения запрещенных файлов на чужих системах, для запуска распределенных атак «отказа от обслуживания» (Denial of Service – DoS), для запуска IRC-серверов (сокр. от Internet Relay Chat – форумы для общения в реальном времени) или же просто в целях вредительства. Эти бессистемные атаки, как правило, являются делом рук обычных взломщиков либо злоумышленников, воспользовавшихся благоприятным стечением обстоятельств, но никак ни профессиональных шпионов. Тем не менее, хотя в данном случае не вы являетесь конечной целью преступников, конфиденциальности вашей информации все равно может угрожать опасность, если кто-то сможет проникнуть в вашу систему.

## Отправные точки сетевой атаки

В отличие от атак, требующих физического доступа к компьютеру, сетевой шпионаж может быть инициирован из произвольной точки доступа к сети. Из-за сложности определения отправной точки сетевой атаки шпион получает ряд преимуществ, в том числе усложняется задача по его поимке. При правильном подходе проникновение в закрытую систему через сеть намного сложнее обнаружить и расследовать, чем тайное физическое проникновение, да и сами взломщики при этом намного меньше рисуют.

Итак, в качестве отправных точек для сетевой атаки могут выступать:

- **Настенная сетевая розетка либо сетевой шнур.** Очевидно, что для реализации данного вида сетевой атаки необходим физический доступ в помещение. Шпион подключается к сети через неиспользуемое соединение где-то в здании (либо через ответвление сетевого кабеля). Для этих целей идеально подходят ноутбуки либо КПК благодаря своему небольшому размеру. Технический персонал, занятый обслуживанием сети, нередко маркирует настенные сетевые розетки и сами шнуры определенными IP-адресами, которые впоследствии необходимо ввести в настройки сетевого окружения подключаемого компьютера. Если на сервере запущен протокол динамического определения настроек (DHCP), новый IP-адрес будет назначен компьютеру

шпиона автоматически, если задать в настройках поддержку динамических адресов. Это можно назвать сетевым шпионажем по принципу Plug and Play. Возможно, перед этим ему придется произвести некоторую разведку на местности, например, выяснить имена доменов и учетных записей пользователей для целенаправленной атаки.

- **Клиентский компьютер в составе сети.** В этом случае шпион полагается на компьютер, который уже подключен к сети. Хотя информация на жестком диске этого компьютера и сама по себе может представлять немалую ценность, но обычно более важной целью является получение доступа к другим компьютерам сети для работы с размещенной на них информацией. Такая атака может вызвать разрушительные последствия, поскольку большинство компаний, уделяя должное внимание защите своих сетей от вторжения извне, напрочь забывает о необходимости защиты внутри сети.
- **Сервер внутри сети.** Наличие физического доступа к серверу сети предоставляет злоумышленнику богатые возможности в плане шпионажа. Помимо использования сервера в качестве плацдарма для атаки других компьютеров, злоумышленник получает доступ ко всем журналам сервера, возможность устанавливать программы перехвата сетевых пакетов и красть хранимую на сервере информацию. Хотя, как правило, серверы защищены гораздо лучше, однако даже предпринятых мер защиты может оказаться недостаточно против серьезно настроенного шпиона.
- **Компьютер, находящийся за пределами сети.** Это классический вид сетевой атаки. В данном случае в качестве отправной точки хакер использует клиента или сервер, не принадлежащий к целевой сети. Большинство сетевых администраторов тратят львиную долю своего времени на попытки предотвращения подобных видов атак. Достаточно умный шпион использует для проведения атаки несколько промежуточных узлов, чтобы запутать свои следы. К примеру, вместо использования персональной учетной записи Интернета, злоумышленник может в интернет-кафе на другом конце города подключиться к некоторому компьютеру в Румынии. Затем подключиться с этого компьютера к другой системе в Японии, и только потом воспользоваться украденным бюджетом пользователя в сети университета в Мехико. Даже в случае если кому-то удастся проследить все международные странствования шпиона, хранители порядка смогут выяснить только местоположение интернет-кафе, с которого было инициировано вторжение.

## Кража информации в ходе сетевой атаки

Вместо того чтобы оперировать абстрактным термином «данные», давайте конкретизируем его применительно к сетевой атаке и попытаемся определить, какая именно информация может быть украдена через сеть. В главе 5 мы выяснили, какие данные или доказательства можно извлечь с жесткого диска компьютера, обладая физическим доступом к нему. Теперь пришло время поговорить о том, какие данные могут быть получены в результате сетевого шпионажа.

Если вы на стороне шпиона, то к данным, которые вы можете украсть, – или, если вы пользователь, пытающийся защитить собственную систему, то к данным, которые нуждаются в защите, – относятся:

- **Сообщения электронной почты.** Все входящие и исходящие электронные сообщения, включая сведения об их получателях и отправителях, содержимое самих сообщений (с вложениями) – все это передается по сети.
- **Пароли.** Любые имена учетных записей и пароли, пересылаемые в незашифрованной форме (в виде простого текста), включая пароли к ящикам электронной почты, FTP-серверам, пароли Telnet и пароли на подключение к веб-сайтам (если на этих веб-узлах не используется протокол SSL для шифрования информации), легко могут быть перехвачены.
- **Сеансы обмена мгновенными сообщениями.** Обе стороны, обменивающиеся мгновенными сообщениями, уязвимы для сетевого шпионажа, если при обмене не используется шифрование информации.
- **Обмен аудио- и видеоинформацией.** Незашифрованные аудиоданные (например, передаваемые по протоколу VoIP – Voice over Internet) или видеопоток могут быть перехвачены.
- **Ваша навигация по сети Интернет.** По результатам анализа выполняемых вами действий в сети Интернет (например, по сведениям о том, на какие веб-узлы вы заходили, по каким баннерам щелкали, как часто вы посещали тот или иной сайт) может быть составлено досье о ваших пристрастиях.
- **Обмен файлами.** Любые операции по отправке, загрузке и поиску определенных файлов в одноранговых сетях могут подвергаться наблюдению и перехвату.
- **Данные на жестком диске.** Шпион, прибегнувший к активной разновидности атаки, может собрать информацию о файлах и папках, к которым разрешен общий доступ. А, воспользовавшись троянским приложением, как было описано в главе 9, злоумышленник может обрести полный контроль над вашим компьютером.

## Риски, связанные с широкополосными соединениями

Распространение широкополосных подключений к сети Интернет при помощи DSL или кабельных модемов увеличило потенциальные возможности компьютерного шпионажа. Хотя государственные и корпоративные сети, как правило, хорошо защищены от сетевых атак, большинство домашних систем не обладают достаточным уровнем защищенности. Результатом являются дополнительные риски (а для шпиона – благоприятные возможности), связанные с работой на дому с конфиденциальной информацией.

### Тактика: анализ трафика

Даже если вы шифруете содержимое почтовых сообщений, злоумышленник по-прежнему может шпионить за вами, выполняя так называемый анализ трафика. Анализ трафика подразумевает запись и последующее детальное изучение сведений об отправителях и получателях электронной почты, о размерах сообщений. Эта информация сопоставляется с прошлыми или текущими событиями, на основе чего делаются выводы о содержимом сообщений. К примеру, когда правительство в очередной раз предупреждало об угрозе совершения новых террористических актов, эти выводы, как правило, делались на основе увеличения потока информации, передаваемой по каналам, уличенным в связи с террористическими организациями (имеются в виду электронная почта, телефонные линии, радио, интернет-чаты и т. д.). В этом случае возросшая активность свидетельствовала о наступлении завершающей стадии подготовки терактов либо о проводимой кампании дезинформации, поскольку возможность анализа трафика не является секретом для террористических организаций.

В реальном мире, не связанном с компьютерами, примером анализа трафика может послужить сбор статистики по количеству заказов пиццы в таких организациях, как Пентагон или Белый дом. Согласно заявлению Фрэнка Микса, владельца сети пиццерий Domino в Вашингтоне, округ Колумбия, в ходе приближения решающей стадии международного кризиса резко возросло количество вечерних заказов пиццы в офисы Пентагона и Белого дома. Микс утверждает, что во время вторжения в Панаму и Гренаду, в ходе войны в Персидском заливе и во время развития других конфликтов количество заказов на доставку пиццы возрастало в геометрической прогрессии. Таким образом, достаточно было подсчитать количество текущих заказов и, не зная, конечно, конкретных деталей, утверждать, что в правительственные кругах планируется нечто грандиозное. А если вы следите за мировыми новостями, вам не составит труда сделать соответствующие выводы.

## Разоблачения: Джон Детч и ЦРУ

Джон Детч занимал пост главы Центрального Разведывательного Управления с мая 1995-го по декабрь 1996 года. Сомнительно, чтобы должность главы ЦРУ могли предложить любому, прочитавшему статью «Шпионы против шпионов» в старом номере журнала Mad (см. ссылку Spy vs. Spy на сайте [www.1am-biek.net/prohias\\_antonio.htm](http://www.1am-biek.net/prohias_antonio.htm)), однако в политике подбора кадров бывают еще и не такие проколы.

Через несколько дней после официального назначения Детча главой ЦРУ на его компьютере, являющемся собственностью правительства США и размещенном в резиденции Детча в городе Биседа, штат Мэриленд, были обнаружены секретные документы. Официально этот компьютер предназначался для работы только с несекретными материалами. Однако все было бы не так плохо, если бы Детч не использовал тот же самый компьютер для работы в сети Интернет, а ведь помимо этого, по крайней мере, еще двое членов его семьи регулярно работали с этим компьютером. (Детч являлся поклонником Macintosh, и поэтому все пять Mac-компьютеров, находящихся в его распоряжении, имели встроенные разъемы PCMCIA для чтения 170 Мб микродисков, с помощью которых он переносил данные со своего офисного компьютера на домашний и наоборот).

Казалось бы, глава ЦРУ должен был знать о возможных рисках шпионажа, но тем не менее следователи по его делу нашли множество фактов касательно работы Детча с конфиденциальной информацией на незащищенных компьютерах. Команда судебных экспертов ЦРУ обнаружила массу секретных документов на компьютерах Детча, включая пикантные подробности о секретных операциях ЦРУ, соверенно секретные переговоры разведки и бюджет Национальной разведывательной программы. Следователи заявили, что проверить, имела ли место утечка конфиденциальной информации, трудно, однако потенциальная возможность сетевой или физической атаки компьютера существовала.

В 1999 году Детч был лишен доступа к секретной информации новым главой ЦРУ Джорджем Тенетом. Федеральные обвинители не отставали от Детча и предложили ему пойти на сделку, согласно которой он должен был признать себя виновным в хранении государственных секретов на незащищенных домашних компьютерах и, таким образом, избежать тюремного заключения.

19 января 2001 года Детч подписал признание в совершении мисдиминона\* и согласился выплатить штраф в размере 5000 долларов. Однако на следующий день, в свой последний день пребывания на должности президента Соединенных Штатов, Билл Клинтон удивил Министерство юстиции и ЦРУ, даровав Джону Детчу полную амнистию.

В настоящее время Джон Детч является факультативным сотрудником химического отделения в Массачусетском технологическом институте.

Полный несекретный отчет внутреннего расследования ЦРУ по делу Детча вы можете найти по адресу [www.fas.org/irp/cia/product/ig\\_deutch.html](http://www.fas.org/irp/cia/product/ig_deutch.html).

Если вы работаете с широкополосными подключениями к сети Интернет, вам необходимо учитывать следующие моменты, связанные с безопасностью:

- **Наличие фиксированного IP-адреса.** В отличие от коммутируемых соединений, где для каждого сеанса работы может назначаться новый IP-адрес, для широкополосных подключений характерно использование постоянного IP-адреса. Поэтому, если этот адрес становится известен, вы превращаетесь в удобную статичную цель.
- **Постоянное подключение к Сети.** В случае с широкополосным соединением вы постоянно являетесь подключенным к сети Интернет, а угроза безопасности вашей информации существует практически всегда, когда компьютер включен.
- **Доступ со стороны членов семьи.** Даже если первичный пользователь компьютера принял адекватные меры безопасности для предотвращения сетевых атак, другие члены семьи и пользователи компьютера могут не соблюсти их, увеличивая шансы злоумышленников на успех.

Тем не менее не стоит отказываться от использования широкополосных подключений и только из-за этого возвращаться к коммутируемым соединениям. Следуя советам, приведенным в разделе «Контрмеры» данной главы, вы можете свести к минимуму риск атаки на ваш компьютер.

\* Категория наименее опасных преступлений, граничащих с административными правонарушениями. – Прим. перев.

# Шпионская тактика

Рассмотрев некоторые базовые концепции применения сетевого шпиона-жа, самое время перейти к более подробному изучению уязвимых мест в защите систем и технологий их использования. В данном разделе вашей секретной миссией будет являться работа в качестве технического эксперта ФБР. Ваша текущая задача сводится к расследованию дела об иностранном террористе в одном из крупных университетских центров Соединенных Штатов. В ваших руках находится судебный ордер, предоставленный в соответствии с Законом об иностранной разведке (FISA), – если вы забыли суть закона, обратитесь к главе 2 – и одобренное судом разрешение на скрытое наблюдение за подозреваемым. Вам необходимо отслеживать все его действия за компьютером. В обычных условиях вы положились бы на систему DCS-1000 (которая ранее носила название Carnivore), однако буквально несколько недель назад исходный код системы просочился в Интернет, и программист из России обнаружил в нем скрытую ошибку переполнения буфера, приводящую к краху системы. В считанные дни в сети появились сценарии под различные платформы, предназначенные для использования этой ошибки, а ее подробное описание мог прочесть любой на сайте Slashdot ([slashdot.org](http://slashdot.org)). Создалось впечатление, что абсолютно все бросились взламывать реально существующие либо предполагаемые системы DCS-1000, в использовании которых постоянно подозревают многих провайдеров Интернета. В сложившейся ситуации ФБР временно отзвало все компоненты системы на доработку, поэтому вы вынуждены некоторое время работать по старинке. (Более подробно о принадлежащей ФБР системе DCS-1000/Carnivore читайте в главе 13; описание мнимой ошибки переполнения буфера не приводится).

## Использование уязвимых мест

Перед тем как приступить к выполнению своего патриотического долга и начать удаленный взлом компьютера нехорошего парня, вспомните, что под компьютерным шпионажем подразумевается тайный сбор информации таким образом, чтобы избежать поимки. Поэтому, перед тем как приступить к использованию инструментов, предназначенных для мониторинга сетевого трафика либо проникновения в закрытые системы, следует освежить в памяти основные правила, важные в любой ситуации:

- не выполняйте сканирование либо атаку с компьютера, IP-адрес которого может вывести непосредственно на вас;
- убедитесь, что номер телефона, с которого вы осуществляете коммутируемое подключение, нигде не записывается;
- помните о том, какие доказательства либо следы присутствия вы можете оставить в системе, в которую вам удалось проникнуть;

- вы должны полностью разобраться в принципах работы систем обнаружения сетевых вторжений (IDS);
- поступайте, исходя из предположения, что все ваши действия после проникновения в некоторую систему могут записываться;
- не тратьте слишком много времени на работу с одной взломанной системой;
- если вы находитесь на стороне правоохранительных органов и работаете в содружестве с провайдерами сети Интернет для наблюдения за подозреваемым в совершении преступления, ограничьте число сотрудников провайдера интернет-услуг, которым известно о проведении операции, и рассмотрите еще раз необходимость дополнительной секретности в ходе проведения расследования;
- для некоторых разновидностей атакуемых объектов все может быть организовано таким образом, чтобы подозрение пало на обычного взломщика, а не профессионального шпиона, тогда, даже если ваши действия окажутся раскрытыми, объект может подумать, что он оказался жертвой малолетних хакеров.

Однако поскольку вы являетесь высококвалифицированным техническим специалистом, вам прекрасно известно о необходимости соблюдения секретности операции, поэтому далее мы перейдем непосредственно к изучению методов атаки сетевых компьютеров.



За более подробной информацией об известных уязвимых местах в системах сетевой защиты, обратитесь к книге «Обнаружение хакерских атак» под авторством Джона Чирилло издательства Wiley, 2002\*. Более подробную информацию об этой книге вы можете прочесть на странице [www.wiley.com/cda/product/0,,0471232823,00.html](http://www.wiley.com/cda/product/0,,0471232823,00.html).

## ИЗУЧЕНИЕ ЦЕЛИ И ПОИСК УЯЗВИМЫХ МЕСТ

Как и в любом другом виде шпионажа, перед началом операции необходимо проанализировать ситуацию. В нашем примере целевой компьютер подключен к сети (для однозначности предположим, что речь идет о сети Интернет, однако с тем же успехом можно говорить и о подключении к корпоративной сети интранет). Обычно этап анализа состоит из трех шагов:

- Локализация цели.** Чтобы начать сетевую атаку, вам понадобится определить локализацию компьютера. Если IP-адрес целевого компьютера неизвестен, вам придется воспользоваться командой `ping` и произвести сканирование портов для идентификации потенциального объекта.

---

\* Перевод на русский язык издан в 2002 году издательством «Питер». – Прим. ред.

- **Идентификация операционной системы.** После локализации целевого объекта следующим этапом является идентификация используемого типа операционной системы и запущенных служб.
- **Поиск уязвимых мест.** После локализации и идентификации цели необходимо произвести поиск уязвимых мест.

Далее мы рассмотрим каждый шаг подробно.

**ЛОКАЛИЗАЦИЯ ЦЕЛИ.** Подобно тому, как для проведения тайного проникновения вам необходимо знать адрес дома, в котором проживает или работает ваша жертва, так и для сетевой атаки вы должны выяснить IP-адрес целевого компьютера. В данном случае вам повезло, поскольку подозреваемый в терроризме имеет DSL-подключение с фиксированным IP-адресом, который был сообщен вам провайдером интернет-услуг.

В принципе IP-адрес целевого компьютера достаточно легко вычислить при помощи утилит автоматического сканирования, предназначенных для проверки портов, и путем запуска команды ping.

- **Сканирование при помощи команды ping.** Команда ping (сокр. от Packet InterNet Grouper) осуществляет отправку интернет-пакетов, чтобы проверить доступности адресата путем передачи ему специального сигнала ICMP echo request (запроса отклика ICMP) и ожидания ответа. Если утилита получает ответ, искомый IP-адрес сохраняется. Этот метод не гарантирует стопроцентного результата, поскольку компьютер может быть настроен на отклонение запросов команды ping во избежание собственного обнаружения.
- **Сканирование портов.** Сканирование портов необходимо для выявления работающих веб-служб, запущенных на компьютере с заданным IP-адресом. Со стандартными службами связаны определенные номера портов: например, с портом 80 связан протокол HTTP и веб-серверы, тогда как с Telnet связан порт 23. Поэтому-то при обнаружении открытого порта утилита автоматического сканирования записывает IP-адрес этого компьютера, и таким образом вам становится известно о существовании работающей цели. Сканеры портов чрезвычайно удобны еще и тем, что, сообщив вам информацию о работающих службах, они могут облегчить задачу по получению доступа к интересующему вас компьютеру при помощи известных уязвимых мест этих служб.

Обычно взломщики осуществляют поиск целевого объекта, сканируя произвольные диапазоны IP-адресов и подбирая любые потенциальные жертвы. Шпионы же действуют в своей практике более избирательно: они либо используют отдельный IP-адрес, вычисленный альтернативными методами, например, с помощью приемов социотехники либо троянских приложений, либо же осуществляют поиск среди некоторого массива IP-адресов, которые принадлежат данной корпорации.

Помните о том, что брандмауэр может скрыть компьютер от обнаружения по сети (в особенности когда он подключен к сети Интернет, и при этом не запущена ни одна служба, поддерживающая внешние подключения), – в этом случае стандартная утилита сканирования может заявить, что компьютера с таким IP-адресом не существует, хотя на самом деле это не так. Кроме того, в ходе сканирования можно выявить наличие корпоративного шлюза, защищенного при помощи брандмауэра, который блокирует входящие сетевые подключения по различным портам. Тем не менее даже защиту брандмауэра можно преодолеть при определенных условиях.

Учтите также, что если вы используете сканер портов, не умеющий выполнять скрытое сканирование, ваш IP-адрес станет известен сканируемому компьютеру. Тем не менее простое сканирование вполне может пройти незамеченным на фоне того количества ежедневных обращений к вашему компьютеру со стороны взломщиков со всего мира, ищущих для себя уязвимые системы.



Полный список обычно используемых портов и связанных с ними служб можно найти на веб-сайте Internet Assigned Numbers Authority по адресу [www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers). Если вы используете сканер портов, не пытайтесь просканировать все перечисленные порты. Большинство сканеров портов позволяют проверять только чаще всего используемые порты.

**ИДЕНТИФИКАЦИЯ ОПЕРАЦИОННОЙ СИСТЕМЫ.** Выяснив IP-адрес целикового компьютера и список служб, связанных с ним, можно приступать к определению типа операционной системы. Эта стадия не менее важна, поскольку с каждым типом и версией операционной системы связаны конкретные уязвимые места. Выяснить тип и версию операционной системы удаленного компьютера можно тремя способами:

- **По уникальным номерам портов.** Наличие портов с определенными номерами может свидетельствовать о типе используемой операционной системы. К примеру, присутствие открытого порта TCP под номером 2869, связанного с функцией Universal Plug and Play, скорее всего, означает, что удаленный компьютер работает под управлением Windows XP.
- **При помощи баннеров.** Большинство служб обладают идентификационными баннерами, отображаемыми при подключении к данной службе. Например, если в результате сканирования портов вы обнаружили активный порт 25 (SMTP), попытайтесь воспользоваться службой Telnet для подключения к данному порту. Существует вероятность, что вы увидите сообщение с именем почтового сервера и его версией (хотя баннеры редко отображаются клиенту, например, почтовый клиент никогда не выводит баннер при подключении к почтовому серверу). Таким образом вы также можете определить тип операционной системы.

- **По характерным различиям в структуре пакетов TCP/IP.** В разных операционных системах реализация стека TCP/IP имеет свои характерные особенности. Поэтому определить версию удаленной операционной системы можно путем анализа возвращенных пакетов TCP. Такие утилиты, как Nmap, описываемые в разделе «Средства сбора сетевой информации и шпионажа» данной главы, позволяют достаточно легко проанализировать эту информацию.

**ПОИСК УЯЗВИМЫХ МЕСТ.** После определения активных портов, а также версии операционной системы необходимо приступить к поиску уязвимых мест, с помощью которых можно было бы получить доступ к интересующему вас компьютеру. Такой поиск может выполняться как автоматически, так и вручную. К примеру, приложение Unix Sendmail печально известно рядом ошибок в системе безопасности. Если вы обнаружили, что пользователь применяет определенную версию Sendmail (версия выводится в баннере при подключении через службу Telnet по порту 25), то, воспользовавшись известными ошибками данной версии, вы можете добиться полномочий администратора.

Разумеется, ручной поиск уязвимых мест системы – занятие весьма скучное и требующее больших затрат времени. Намного проще воспользоваться свободно распространяемыми либо коммерческими программами-сканерами, предназначенными для этой цели. Для работы программы-сканера вам придется задать IP-адрес целевого объекта, и утилита, имея в своем распоряжении базу данных известных слабых мест, проверит их наличие на целевом компьютере. Затем вам останется только найти программу, умеющую использовать данную брешь в защите системы (в виде бинарного либо исходного кода), и применить ее к целевому компьютеру.



В архивах компании Neohapsis можно найти массу полезной информации о брешах в системах защиты и средствах их использования, сведения о которых в разное время были опубликованы в бюллетенях безопасности. Доступ к архивам вы можете получить по адресу <http://archives.neohapsis.com>.

## ФАЙЛЫ WINDOWS С ОБЩИМ ДОСТУПОМ

Поскольку данная книга посвящена в первую очередь компьютерному шпионажу для операционных систем Windows, мы не можем обойти вниманием вопрос разделяемого доступа к файлам в Windows – это одно из уязвимых мест сетевой безопасности системы. (При обсуждении проблем разделяемого доступа к файлам Windows вы нередко можете услышать аббревиатуру NetBIOS. NetBIOS представляет собой интерфейс прикладного программирования, расширяющий базовый набор функций BIOS за счет поддержки сетевых возможностей. Таким образом, термины разделяемого доступа к файлам Windows и NetBIOS часто используются как синонимичные.)

Начиная с версии Windows 3.11 (Windows для рабочих групп), компания Microsoft стала включать во все свои операционные системы поддержку функций разделяемого использования файлов и папок по сети. Основой технологии разделяемого доступа к файлам в Windows является протокол CIFS (Common Internet File System – общий протокол доступа к файлам Интернета), ранее называвшийся SMB (Server Message Block – блок серверных сообщений). Протокол CIFS позволяет работать с файлами на удаленном компьютере под управлением Windows так, как если бы они находились на той машине, за которой сидит пользователь (кроме того, CIFS поддерживает связь Unix–Windows).

Прозрачный доступ к файлам – ценная возможность для работы пользователя, однако неправильная настройка этой функции может открыть доступ к важным файлам системы либо к конфиденциальной информации. Одной из причин стремительного распространения вируса Sircam и «червя» Nimda летом 2001 года явилось наличие у вируса функции обнаружения незащищенных сетевых файлов или папок с общим доступом, в которые вирус сам себя копировал. Многие компьютерные пользователи, сами того не ведая, сделали свои системы открытыми для шпионажа, разрешив свободный доступ для чтения и записи к логическим дискам компьютера коллегам либо членам семьи. Даже если доступ предоставлялся с соблюдением мер безопасности, в распоряжении шпиона всегда имеется ряд средств и технологий обхода системной защиты разделяемых файлов и папок.

Поскольку эта брешь в защите системы, связанная с разделяемыми файлами в Windows, известна не первый год, она до сих пор является любимой целью взломщиков и, конечно, шпионов. Обнаружив в системе активный порт NetBIOS, вы можете смело утверждать, что на данном компьютере работает система Windows и имеются файлы или папки с общим доступом. Впоследствии при помощи специальных сетевых утилит можно будет выяснить, какие именно файлы и папки являются разделяемыми, подключиться непосредственно к этим файлам и даже инициировать «лобовую» атаку по подбору пароля, если доступ к файлам защищен паролем. Если система не достаточно хорошо защищена, вы вполне можете преуспеть в деле кражи конфиденциальной информации.

Однако вернемся к ситуации с нашим злоумышленником, подозреваемым в терроризме: вы сообщили вашему боссу о том, что необходимость в атаке разделемых файлов через NetBIOS отсутствует. Группа тайного проникновения уже завершила к этому моменту создание образа с оригинального жесткого диска. Кроме того, поскольку уязвимые места NetBIOS слишком хорошо известны, многие провайдеры услуг Интернета, особенно в случае с широкополосными подключениями, блокируют попытки сканирования и доступа к портам 137, 138 и 139 из сети Интернет. Тогда можно воспользоваться и другими, более эффективными в данных условиях технологиями.



Чтобы узнать подробности об атаках через NetBIOS, просмотрите путеводитель хакера. Его собрал «этичный хакер» Гаав Кумар на сайте [www.myugiserver.com/~ethicalhackers/netbios.html](http://www.myugiserver.com/~ethicalhackers/netbios.html).

## СЕТЕВОЙ МОНИТОРИНГ

Перехваченные по сети данные могут служить источником всех видов интересующей шпиона информации. В принципе вы легко можете просматривать любые незашифрованные данные так, что ваша жертва даже не будет подозревать об этом.

В ходе проводимого вами расследования по делу о терроризме перед вами встают две задачи: собрать возможные доказательства противоправной деятельности злоумышленников и выведать информацию о готовящихся террористических актах. Исходя из этого, вы решили сконцентрировать свои усилия на сетевом мониторинге.

**ПРОГРАММЫ ПЕРЕХВАТА СЕТЕВЫХ ПАКЕТОВ.** Программа перехвата сетевых пакетов (sniffer, также называемая анализатором трафика либо сетевым монитором) позволяет вести наблюдение за сетевым трафиком. Сетевой трафик в необработанном виде – это загадочный набор символов в духе Матрицы. А поскольку мало кто из нас умеет читать информацию по набору шестнадцатеричных кодов, то помимо перехвата потока байтов сетевой монитор должен уметь декодировать бинарные данные и преобразовывать их в удобочитаемый вид, основываясь на типе протокола, используемого для передачи этих данных. К примеру, если запрос, пришедший на веб-сервер со стороны браузера, будет корректно декодирован, то вы легко сможете прочесть информацию, которой обмениваются два компьютера по протоколу HTTP.

В сети Ethernet пакеты отправляются всем компьютерам сети, при этом каждая сетевая карта принимает только те пакеты, которые адресованы ей. (Если заголовок пакета содержит MAC-адрес, отличный от MAC-адреса сетевой карты, пакет игнорируется.) Однако можно настроить сетевую карту для работы в смешанном режиме, чтобы она принимала все отсылаемые по сети пакеты. Это может быть сделано при помощи самой программы перехвата сетевых пакетов, которая будет собирать все отсылаемые по сети данные.

Программы перехвата сетевых пакетов отлично приспособлены для работы в традиционных сетях Ethernet, содержащих хабы и маршрутизаторы. Но если в состав сети входит коммутатор, тогда сетевой монитор сможет получать только те пакеты, которые были адресованы именно ему. Изначально коммутаторы предназначались для передачи сетевого трафика непосредственно с одного физического порта на другой. Обычно они не отправляют широковещательный сигнал всем компьютерам в сети. Для перехвата сетевых пакетов в сети, имеющей в своем составе коммутаторы, вам необходимо установить сетевой разветвитель между компьютером и портом коммутатора. Разветвитель позволит перехватывать

продублированный сигнал между компьютером и оставшейся частью сети. Сетевой монитор в этом случае должен быть подключен непосредственно к разветвителю. Для тех же целей может быть использована технология ARP\*. Отличную статью на эту тему, подготовленную Томом Кингом, вы можете найти по адресу [www.sans.org/rr/netdevices/packet.php](http://www.sans.org/rr/netdevices/packet.php).

Большинство программ перехвата сетевых пакетов позволяют отображать перехватываемую информацию в режиме реального времени либо сохранять ее для дальнейшего просмотра. Кроме того, вы можете использовать фильтры для хранения только определенного типа трафика (к примеру, данных, поступающих с конкретного IP-адреса). В ходе расследования деятельности подозреваемых в терроризме лиц, вы можете установить программу на сервере провайдера интернет-услуг и отслеживать сетевой трафик для определенного пользователя, не нарушая прав на неприкасновенность частной жизни других пользователей данного провайдера. Кроме того, по сети обычно передается огромное количество управляющих пакетов, связанных с запросами DNS и другой абсолютно не нужной вам информацией. Фильтры могут применяться и для сохранения определенных протоколов, например SMTP или POP при работе с почтовым клиентом либо HTTP при навигации по сети Интернет.

## Шпионский инструментарий: коммерческие аналоги пакета Carnivore

Используемая ФБР программа DCS-1000/Carnivore будет детально рассматриваться в главе 13, но поскольку сейчас мы обсуждаем программы перехвата сетевых пакетов, в этом контексте не лишним будет упомянуть ряд других коммерческих продуктов, выполняющих некоторые функции сетевого мониторинга, доступные в программе DCS-1000. Вам не нужен значок полицейского для их приобретения – достаточно иметь в кошельке круглую сумму. Итак, к наиболее популярным программам можно отнести:

- **SilentRunner.** Программа SilentRunner, выпущенная компанией Raytheon (которая уже довольно давно сотрудничает с правительством), представляет собой высококлассный программный продукт, предназначенный для сетевого наблюдения и анализа. Детальную информацию по этой утилите вы можете найти на официальном веб-сайте [www.silentranner.com](http://www.silentranner.com)\*\*.

\* Address Resolution Protocol – протокол разрешения адресов, позволяющий преобразовывать IP-адреса в MAC-адреса. – *Прим. перев.*

\*\* В настоящее время эта программа под названием eTrust Network Forensics распространяется фирмой Computer Associates <http://ca.com>. – *Прим. ред.*

- **NetIntercept.** Еще одной утилитой для сбора сетевых данных и их последующего анализа является программа NetIntercept, разработанная компанией Sandstorm Enterprises. Более подробно о программе вы сможете узнать по адресу [www.sandstorm.net/products/netintercept/](http://www.sandstorm.net/products/netintercept/).
- **DragNet.** Программа DragNet, первоначально разработанная компанией Traxess Incorporated (которая была приобретена Network Associates в августе 2002 года), сочетает в себе функции мониторинга клавиатуры и сети. Выход этого продукта ожидался в 2003 году, а информацию по нему можно попробовать найти на сайте [www.nai.com](http://www.nai.com).
- **RetrievalWare.** Одно дело собрать несколько гигабайт информации, а совсем другое – проанализировать всю эту массу данных и найти в них что-либо полезное. Не предназначенные изначально для целей мониторинга приложения для добычи данных, такие как RetrievalWare от компании Convera, активно используются в ФБР и других государственных разведслужбах. Официальный сайт компании-производителя: [www.convera.com](http://www.convera.com).

Если вы ограничены фиксированным бюджетом, но при этом обладаете навыками программирования, в том числе сетевого, на С, вы можете разобрать копию программы Altivore (свободно распространяемой по принципу открытого кода версии программы Carnivore, но без стартовых блоков). Исходные коды и более подробную информацию вы можете найти по адресу [www.robertgraham.com/altivore/](http://www.robertgraham.com/altivore/).



На собственном сайте Роберта Грэхема, ветерана компьютерной индустрии и разработчика брандмауэра BlackICE, вы можете найти ответы на часто задаваемые вопросы по программам сетевого мониторинга. Адрес сайта: [www.robertgraham.com/pubs/sniffing-faq.html](http://www.robertgraham.com/pubs/sniffing-faq.html).

**СЕРВЕРНЫЕ ЖУРНАЛЫ.** Помимо перехвата сетевых пакетов вы можете заняться сбором информации по сетевому трафику путем изучения серверных журналов. В подобных журналах обычно сохраняются заголовки пакетов, например входящие и исходящие IP-адреса, дата и время транзакции, информация, связанная с определенным типом сервера (к примеру, почтовые серверы хранят информацию о получателях и отправителях сообщений, времени отправки или получения, размере сообщения и т. д.). Любое лицо, обладающее физическим либо удаленным доступом к серверу, включая полноправных системных администраторов, офицеров полиции с судебным ордером либо шпионов, которым удалось найти брешь в защите системы, могут получить доступ к этим данным. (Кроме того, не забывайте о журналах, создаваемых брандмауэрами на домашних либо небольших офисных компьютерах.)

В нашем гипотетическом расследовании террористической угрозы провайдер интернет-услуг подозреваемого пошел нам навстречу, предоставив возможность просмотра записей, касающихся нашего злоумышленника, в журнале сервера. Чтобы не нарушать права на невмешательство в частную жизнь других пользователей, вы запросили только те записи в журнале, в которых фигурировал IP-адрес подозреваемого. В этом вам помог системный администратор, написавший на Perl небольшой сценарий, выполняющий грамматический разбор записей и извлекающий только те строки, которые имеют отношение к нашему террористу. Просмотрев сценарий, вы попросили включить в программный код хеширование извлеченных данных по алгоритму MD5, чтобы гарантировать аутентичность полученной информации. Администратор задал автоматическое выполнение данного сценария каждый день в 7:30. Причем выходные данные, как вы и просили, должны автоматически шифроваться и отсыпаться на подставной адрес электронной почты где-то на Hotmail. (Заказать отправку информации на ваш личный почтовый ящик в домене fbi.gov, пожалуй, будет не слишком разумно.)

Поскольку серверные приложения могут генерировать достаточно большие объемы информации, файлы журнала регулярно удаляются для сохранения дискового пространства. В деле Закариса Мусауи, 20-го угонщика самолета во время террористической атаки 11 сентября, из-за автоматического удаления файлов журнала на серверах Kinko и Hotmail Microsoft следователи не смогли собрать возможные доказательства. Поэтому в целях расследования вы попросили, чтобы журналы на сервере регулярно архивировались. В случае предъявления обвинений вашему подозреваемому эти журналы смогут сыграть немаловажную роль в ходе следствия, например, в качестве подтверждения источника хешированных записей в файле журнала.

Вы поблагодарили всех сотрудников провайдера услуг Интернета за оказанное содействие в проведении следствия, подчеркнув, что дело касается национальной безопасности, и поэтому в данном случае особенно важно соблюдение тайны следствия. Пошутив в духе «Секретных материалов», вы попросили менеджера организации поддерживать связь с вами и сообщить в случае появления какой-либо новой интересной информации.

## ИНСПЕКТИРОВАНИЕ СЕТЕВОГО ОБОРУДОВАНИЯ

Сетевое оборудование, такое как маршрутизаторы, коммутаторы и брандмауэры (как аппаратные, так и программные), также может дать немало ценной информации о деятельности целевого объекта. В особенности это справедливо для домашних либо небольших офисных сетей, пользователи которых не обладают достаточным опытом и техническими познаниями, необходимыми для понимания возможных рисков.

**ИЗУЧЕНИЕ ФАЙЛОВ ЖУРНАЛА.** Обычно протокол работы сетевого оборудования и приложений сохраняется в файлах журнала. Эти журналы

могут являться ценным источником информации, изучив который можно выяснить, для каких целей использовалась сеть тем или иным пользователем. Файлы журнала обычно содержат дату и время поступления пакета, исходящие и входящие IP-адреса и номера портов (с помощью которых вы сможете представить себе общую картину происходящего; например, активность порта 23, как правило, говорит об использовании зашифрованного SSH-соединения).

## Разоблачения: грязные уловки политиков

В ходе предвыборной гонки в Сенат в штате Миннесота, проходившей в 2000 году, делегатам от Демократической партии аграрного труда были отосланы сообщения электронной почты, убеждающие их не поддерживать кандидата Майка Цирези на собрании по выдвижению кандидатур на выборные должности. В этих сообщениях содержались обвинения в антипартийных амбициях Цирези. Все сообщения, подписанные «прогрессивным членом партии» по имени Кати Стивенс, были отправлены с одного бесплатного почтового ящика службы Hotmail ([kylomb@hotmail.com](mailto:kylomb@hotmail.com)).

Когда помощники Цирези начали расследование по данному факту, они не смогли найти никакой Кати Стивенс. Следы привели их к оппоненту Цирези, республиканцу Робу Грэмсу, занимающему должность сенатора. Эта кампания Грэма, направленная против Цирези, была инициирована его невестой Кристиной Ганхас. Проанализировав электронные послания, следователи нашли нити, приведшие их к мисс Ганхас и ее политической кампании.

Некоторые вложения электронной почты содержали документы в формате Microsoft Word, автором которых значилась та самая Кристина Ганхас. (Word автоматически добавляет в документ эту информацию, основываясь на регистрационных сведениях пользователя программного продукта.) Это раз.

Заголовки всех писем, отправляемых через службу Hotmail, содержат заголовок X-originating-IP (в нем хранится оригинальный IP-адрес, с которого пришло сообщение). Анализ показал, что первые сообщения были отправлены с рабочей станции с поминутной оплатой в копицентре Kinko. Последующие сообщения отправлялись через бюджет AT&T WorldNet. К несчастью для злоумышленников, компания AT&T вела учет всех входящих звонков, поступивших на их модемные пулы. Когда власти запросили информацию по звонкам, связанным с данным IP-адресом в период отправки этих сообщений, они обнаружили, что один из телефонных номеров, использовавшийся для подключения к службе коммутируемого доступа, принадлежал Кристине Ганхас. Это два.

Ганхас использовала старую версию Word, в которой в документ включался GUID-идентификатор. Как известно, при вычислении GUID используется MAC-адрес сетевой карты, если таковая установлена в системе. Поскольку подразумевается уникальность MAC-адресов, то знание GUID может опять-таки привести к пользователю, создавшему этот документ, либо, по крайней мере, к компьютеру с данной сетевой картой. Когда полицейские получили на руки ордер для обыска в доме Кристины Ганхас, они выяснили, что MAC-адрес сетевой карты действительно соответствует GUID документа, отправленного по электронной почте. Это три, и вы вне игры!

Действия Кристины Ганхас были квалифицированы как уголовно наказуемые в соответствии с действующим в Миннесоте Законом о честной предвыборной кампании, который запрещает распространение анонимной информации. В июне 2001 года Ганхас признала себя виновной и была оштрафована; обвинители решили не настаивать на более суровых мерах пресечения, как тюремное заключение. Цирези со своей партией утратил лидирующие позиции (отнюдь не из-за электронных писем своей невесты, а в результате жесткой рекламной кампании своего оппонента Майка Дэйтона), а Грэмс безоговорочно проиграл следующие выборы, не удержавшись в кресле сенатора.

Данные журнала хранятся в памяти устройства, и получить к ним доступ можно при помощи программного обеспечения, представляющего собой интерфейс для аппаратного устройства. Затем данные из памяти записываются в файл журнала на жестком диске пользователя. По умолчанию большинство программных брандмауэров сохраняют текстовые файлы журнала со статистикой сетевых подключений. Многие пользователи вообще не имеют об этом представления и, удаляя все следы своей деятельности в Интернете на уровне браузера, игнорируют при этом файлы журналов маршрутизаторов и брандмауэров, которые содержат списки посещенных пользователями сайтов с указанием даты и времени обращения.

**ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ ПО УМОЛЧАНИЮ.** Большая часть сетевых устройств имеет пароли для ограничения доступа к функциям управления устройством, и во многих случаях пользователи или системные администраторы забывают изменить пароль по умолчанию. На самом деле такие незадачливые пользователи весьма рисуют, поскольку списки паролей по умолчанию легко можно найти на многих Интернет-сайтах. Если вам удастся определить тип используемого сетевого устройства, а затем локально либо же удаленно подключиться к нему при помощи известного пароля по умолчанию, вы сможете поменять настройки безопасности устройства и таким образом получить доступ к хранимой на нем информации.



Постоянно обновляемый и расширяемый список используемых по умолчанию паролей для различного сетевого оборудования можно найти на веб-сайте [www.phenoelit.de/dpl/index.html](http://www.phenoelit.de/dpl/index.html).

## ДРУГИЕ ВИДЫ СЕТЕВЫХ АТАК

Помимо удаленного проникновения в систему, использования программ перехвата сетевых пакетов либо изучения серверных журналов, для кражи конфиденциальной информации могут применяться и другие виды сетевых атак.

**АТАКА ПРИ ПОМОЩИ ПРИЛОЖЕНИЙ, НАПИСАННЫХ ЗЛОУМЫШЛЕННИКАМИ.** Еще один способ сетевого мониторинга заключается в установке на целевом компьютере некоторого приложения, созданного злоумышленником для сбора информации (сетевой и не только) и ее отправки шпиону. В главе 8 обсуждалась тема коммерческих программ мониторинга клавиатуры, обладающих подобными функциями, а в главе 9 рассматривались приложения, относящиеся к разновидности «троянских коней».

Недружественные приложения могут быть установлены в ходе тайного физического проникновения либо удаленно тем же методом, что используется для распространения вирусов и «червей», например, через вложения электронной почты. В нашем деле подозреваемого в терроризме наиболее подходящим вариантом кажется проведение тайного проникновения, подобного тому, которое было организовано в деле Никодермо Скарфо. (Неизвестно, выполнял ли используемый ФБР в этом деле клавиатурный регистратор удаленную отправку информации. Мы вряд ли когда-нибудь узнаем это достоверно, поскольку детали дела так и не были обнародованы, и нам остается только надеяться на новую редакцию Закона о свободе информации, которая бы включала в себя дополнительные пункты, касающиеся разглашения сведений по уже рассмотренным в суде делам.)



Классическим примером недружественного приложения, использующего сетевые подключения, является Stealth Email Redirector (SER). После установки эта программа перенаправления почтовой корреспонденции автоматически начинает отсылать копии всех исходящих сообщений, передаваемых через порт 25 (SMTP) на заданный адрес электронной почты (постарайтесь использовать учетную запись, которую будет трудно связать с вами). Информацию по программе SER можно найти на сайте <http://www.soft-security.com/bigbrother.html>.

Недружественные приложения особенно удобны, если целевые объекты имеют широкополосное подключение к Интернету, поскольку такие компьютеры постоянно подключены к сети и, как следствие, могут отправлять и принимать данные в любое время, например, когда жертва

спит и даже не ведает о сетевой активности. Основным недостатком подобного вида атак является тот факт, что пользователь, сведущий в вопросах компьютерной безопасности, почти наверняка прибегнет к помощи брандмауэра и другим контрмерам, позволяющим легко вычислить и уничтожить недружественное приложение после его установки.

**АТАКА ПРИ ПОМОЩИ ВЕБ-САЙТОВ, СОЗДАННЫХ ЗЛОУМЫШЛЕННИКАМИ.** Рядом с недружественным программным кодом, устанавливаемым непосредственно на целевую систему, стоит программный код, запускаемый при посещении определенных веб-страниц. На сегодняшний день самым распространенным веб-браузером был и остается Internet Explorer, репутация которого в плане безопасности сильно подмочена из-за множества существующих ошибок. Написанные злоумышленниками элементы управления ActiveX, уязвимые места активных серверных сценариев, бреши в защите виртуальной машины Java, ошибки переполнения стека – все это может быть использовано шпионами на фиктивных веб-сайтах, специально предназначенных для кражи информации с жестких дисков пользователей, подключившихся к этому сайту. Вопрос состоит только в том, как заставить целевой объект посетить этот сайт – с помощью приемов социотехники через электронную почту либо по телефону.

Эти виды атак показывают свою высокую эффективность по следующим причинам:

- большинство пользователей угрозу со стороны созданных злоумышленниками веб-сайтов не принимает всерьез, в отличие от вирусной угрозы;
- при правильной постановке дела обнаружить такую атаку довольно сложно;
- большинство пользователей не спешат устанавливать программные «заплаты» для защиты уязвимых мест системы.



Полный список недавно обнаруженных ошибок безопасности Internet Explorer (и тех, для которых уже были выпущены «заплаты», и тех, что только ожидают своей очереди) вы можете найти на сайте [rivx.com/larholm/unpatched/](http://rivx.com/larholm/unpatched/).

**АТАКА С ИСПОЛЬЗОВАНИЕМ ПУБЛИЧНЫХ МЕСТ ДЛЯ ДОСТУПА В ИНТЕРНЕТ.** Еще один способ шпионажа связан с растущей популярностью различного рода интернет-кафе, библиотек, отелей, интернет-киосков и т. д., предлагающих дешевый и удобный способ подключения к Интернету. При помощи общественных мест доступа к Интернету весьма занятые люди получают возможность посетить интересующие их сайты либо проверить электронную почту где-нибудь в дороге. Вот некоторые способы кражи конфиденциальной информации:

- **Подглядывание.** Обычно подглядывание из-за плеча используется для выяснения имени учетной записи и пароля, вводимых с клавиатуры. Любой публичный терминал для выхода в Интернет предоставляет вам подобную возможность (главное, чтобы это не бросалось в глаза). Даже если из-за плеча клавиатура не видна полностью, хороший специалист в области подглядывания может вычислить пароль, исходя из позиции пальцев на клавиатуре и количества нажатий клавиш. Эти навыки пригодятся всегда, когда кто-либо подключается к компьютеру.
- **Keylogger.** Программные либо аппаратные средства мониторинга клавиатуры легко могут быть установлены на общественных компьютерах для записи данных, вводимых пользователем. Напоминаем вам, что подробное описание keylogger-средств приводилось в главе 8.
- **Доступ к серверу либо сети.** С помощью судебного ордера, дачи взяток, использования приемов социотехники, взлома либо просто в результате недосмотра обслуживающего персонала шпион может получить доступ к сети. Имеется информация о том, что в некоторых европейских гостиницах на общественных компьютерах, предназначенных для предоставления услуг связи, в целях экономического шпионажа, по указанию местных правительств отслеживаются действия приезжих туристов. В Соединенных Штатах ФБР не менее активно использует в своих расследованиях информацию, поступившую от провайдеров услуг Интернета, обслуживающих места доступа к Интернету общественного пользования.

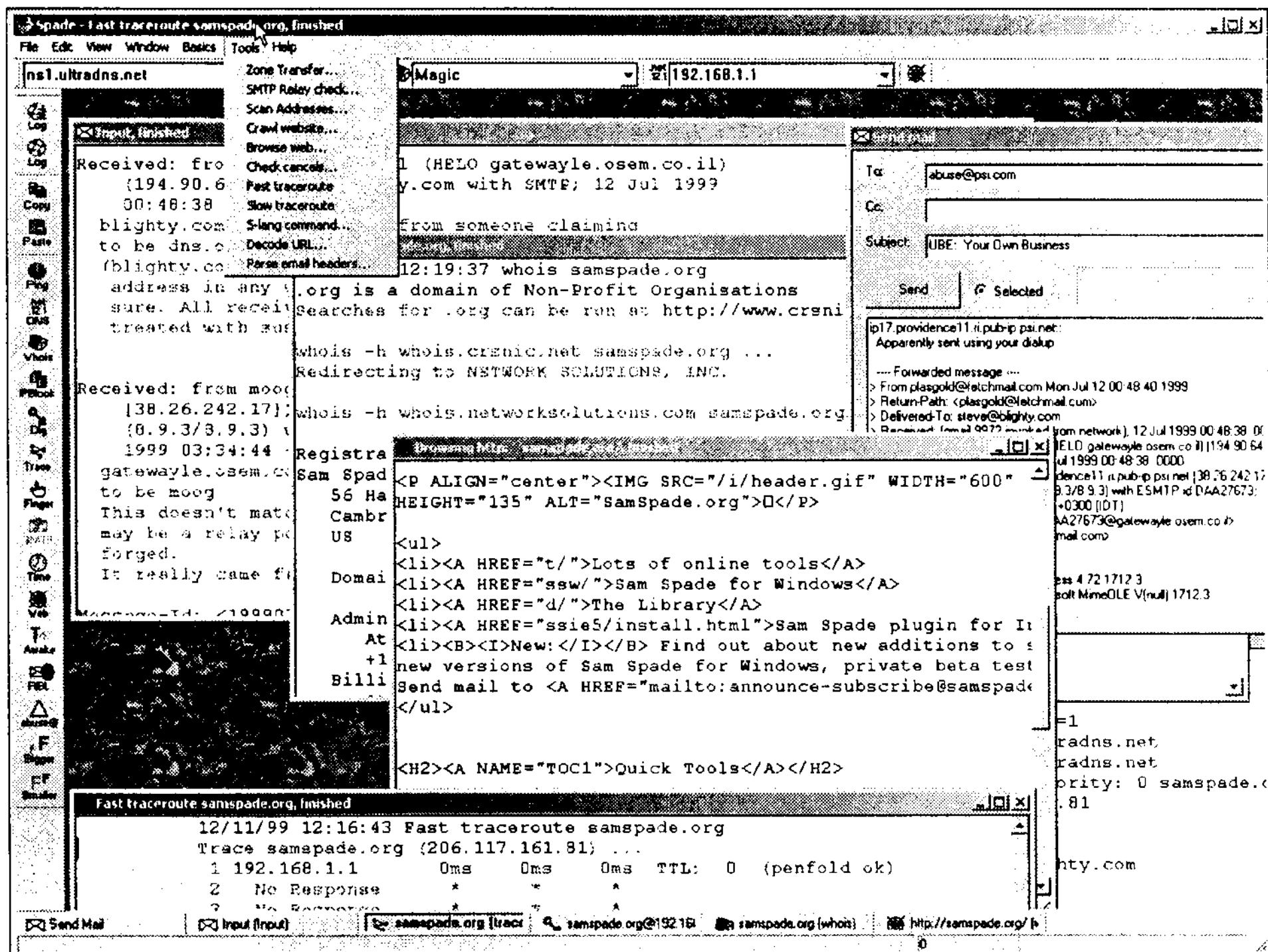
## Средства сбора сетевой информации и шпионажа

Теперь, когда вы познакомились с главными уязвимыми местами защиты сетей, узнали, какие виды атак могут быть применены в том или ином случае, пришло время рассмотреть некоторые полезные утилиты, которые помогут вам облегчить решение задач наблюдения. Большинство утилит распространяются свободно, и вам не понадобится доставать значок полицейского, чтобы заполучить их.

### SAMSPADE

SamSpade представляет собой свободно распространяемую утилиту, предназначенную для сбора сетевой информации и поиска доказательств (внешний вид главного окна утилиты показан на рис. 10.1 на след. странице). Она включает в себя функции таких утилит, как whois, tracert, ping и dig, предназначенных для сбора информации о сетевых компьютерах. Эта утилита окажет вам неоценимую помощь при наблюдении за специфическими целями. Загрузить программу можно с официального веб-сайта [www.samspade.org](http://www.samspade.org). На этом же сайте вы также найдете онлайновые

версии программ на случай, когда вы забыли взять свой набор шпионских утилит, но в вашем распоряжении имеется доступ к сети Интернет.



**Рис. 10.1.** Внешний вид окна программы SamSpade, в котором отображается различная информация о сети компании, являющейся объектом вашего интереса. Подобная информация может оказаться чрезвычайно полезной при планировании сетевой атаки

## NMAP

В Интернете можно найти массу разнообразнейших программ для сканирования портов, но профессионалы в сфере безопасности и шпионы на первое место по праву ставят утилиту Nmap. Nmap (расшифровывается как Network Mapper) распространяется свободно по принципу открытого кода. Автором утилиты является некий Феодор (Fyodor). Среди возможностей программы – локализация целевых компьютеров, проверка активных служб и идентификация типа/версии ОС на интересующем нас компьютере.

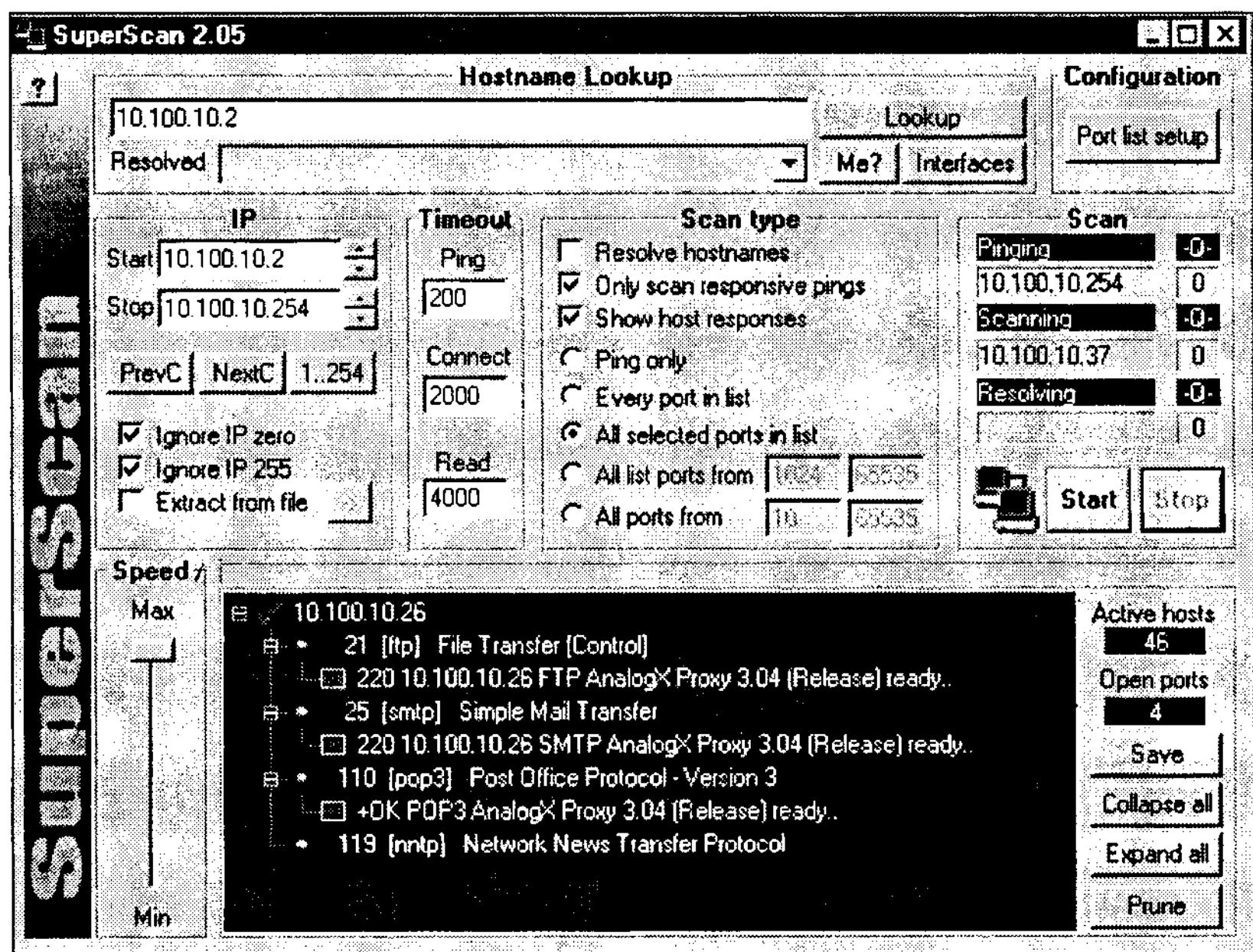
Программу Nmap на фоне других подобных сканеров портов выделяет использование различных методов получения информации о целевом компьютере. Некоторые технологии сканирования настолько незаметны и трудны для обнаружения, что успешно работают даже против

компьютеров, оснащенных системами обнаружения вторжений (IDS – intrusion detection systems). Одна из технологий, называемая IdleScan, позволяет шпиону обращаться к компьютеру без разглашения собственного IP-адреса, путем отправления пакетов от имени ничего не подозревающего хоста.

Изначально Nmap представляла собой утилиту командной строки, предназначенную для запуска из-под Unix, хотя со временем появилась версия и под Windows. Оригинальную Unix-версию можно найти по адресу [www.insecure.org/nmap/](http://www.insecure.org/nmap/), а Windows-версию – на сайте [www.nmap-win.org](http://www.nmap-win.org).

## SUPERSCAN

Если вас не беспокоит возможность обнаружения ваших действий (что, однако, вас, как шпиона должно волновать), но вы ищете легкий в использовании, быстродействующий сканер TCP-портов, попробуйте такую программу, как SuperScan от компании Foundstone (см. рис. 10.2). Эта утилита также распространяется абсолютно бесплатно, а загрузить ее можно с сайта [www.foundstone.com/knowledge/proddesc/superscan.html](http://www.foundstone.com/knowledge/proddesc/superscan.html).



**Рис. 10.2.** Сканер портов SuperScan в действии. В окне программы отображаются компьютеры локальной сети в пределах маршрутизатора и соответствующие им открытые порты

## NESSUS

Свободно распространяемая по принципу открытого кода утилита Nessus, написанная Ренодом Дирэйсоном, предназначена для проверки безопасности систем. Она существует на рынке еще с 1998 года. Программа Nessus состоит из двух частей: серверного компонента, берущего на себя задачи по проверке безопасности, и клиентской части, обеспечивающей интерфейс пользователя. В состав утилиты входит расширяемая библиотека известных уязвимых мест, которая может пополняться. По состоянию на январь 2003 года существовало около 1100 дополнительных подключаемых модулей, с помощью которых можно было осуществлять поиск уязвимых мест в защите различных устройств и операционных систем. Список сценариев проверки постоянно пополняется с обнаружением новых брешей систем безопасности.

Настроив серверную и клиентскую часть программы, введите интересующий вас IP-адрес (программа Nessus может работать в содружестве с Nmap для выполнения скрытого сканирования портов), выберите, какие виды проверок безопасности вы желаете провести, и т. д. По окончании сканирования утилита генерирует детальный отчет, содержащий список обнаруженных брешей в защите системы, внешние ссылки и возможные варианты решения проблемы.

Недостатком данной программы для пользователей Windows является тот факт, что серверные компоненты доступны только для Unix-совместимых систем. Тем не менее эта утилита стоит того, чтобы установить операционную систему Linux и научиться в ней работать. Более подробную информацию об этой программе вы можете найти на ее официальном сайте [www.nessus.org](http://www.nessus.org) – там же ее можно и загрузить. (Если вам позарез нужна программа проверки безопасности системы под Windows, то придется обратиться к относительно дорогим коммерческим утилитам, таким как Internet Scanner от компании Internet Security Systems, информация о которой размещена на сайте [www.iss.net](http://www.iss.net).)

## СРЕДСТВА NETBIOS

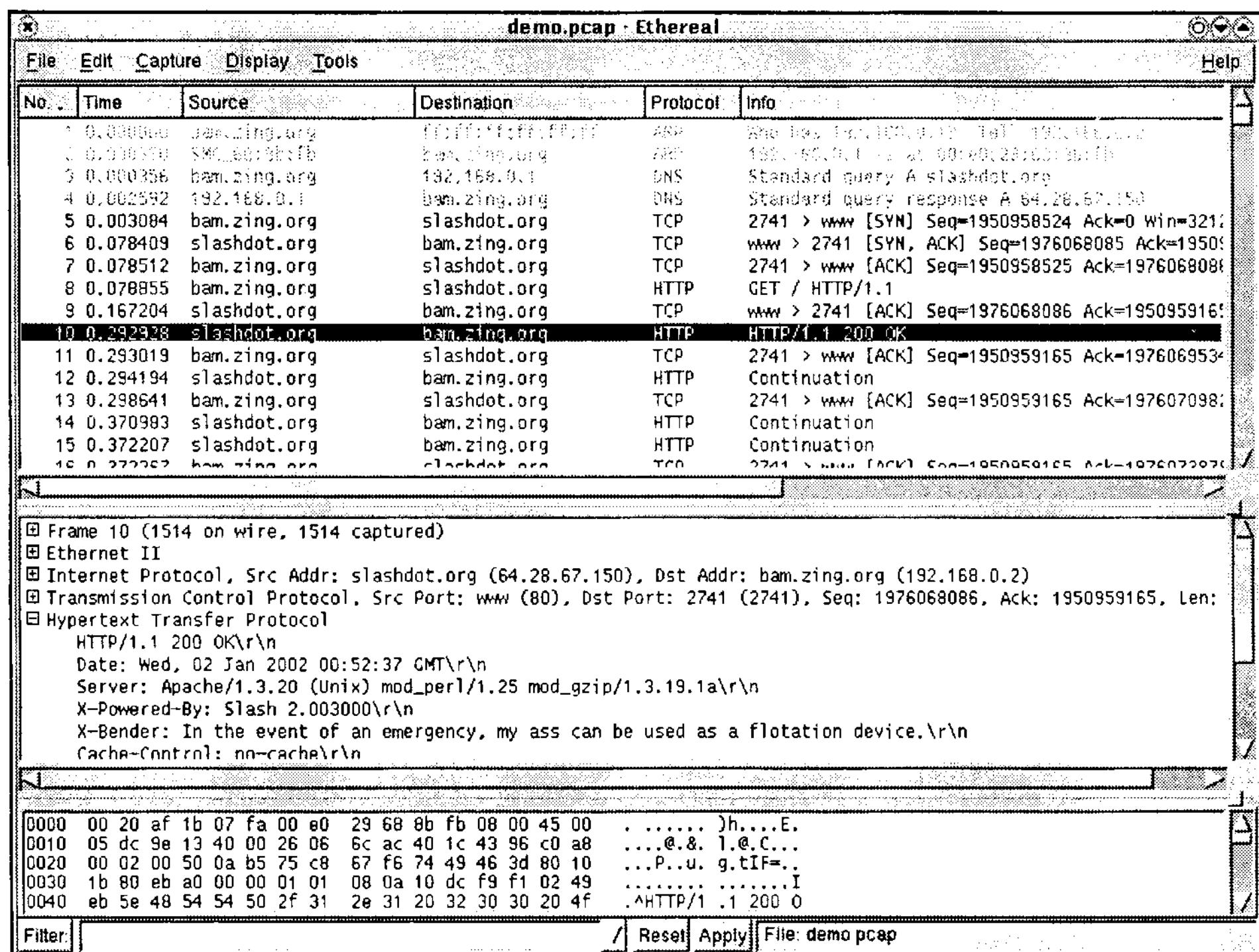
Существует ряд программ, позволяющих проникать в системы, в которых используются файлы и папки с общим доступом. Расскажем вкратце о двух наиболее популярных утилитах для сетевых атак через NetBIOS:

- **NAT (NetBIOS Auditing Tool)** – утилита командной строки, предназначенная для поиска файлов и папок с общим доступом. Для обнаруженных файлов и папок при необходимости начинается подбор паролей по методу «любовой атаки». Программа распространяется бесплатно. Загрузить ее можно с сайта <http://online.securityfocus.com/tools/543>.
- **Legion** – программа, имеющая схожую с NAT функциональность, но при этом написанная на Visual Basic и обладающая пользовательским интерфейсом Windows. Авторство утилиты принадлежит уже несуществующей группе экспертов по безопасности

Rhino9, причем программа остается свободно распространяемой со дня своего появления в 1997 году. Несмотря на свой солидный возраст, эта утилита отлично уживается с самыми последними версиями Windows. Загрузить программу можно с веб-узла [packetstormsecurity.org/groups/rhino9/legionv21.zip](http://packetstormsecurity.org/groups/rhino9/legionv21.zip).

## ETHEREAL

Одной из наиболее популярных программ перехвата сетевых пакетов для систем под управлением как Windows, так и Linux, является свободно распространяемая утилита под названием Ethereal (см. рис. 10.3). Программа Ethereal, автором первой версии которой был Жеральд Комб, со временем превратилась в проект, распространяемый по принципу открытого кода, свой вклад в развитие которого внесли многие люди, и теперь эта утилита пользуется огромной популярностью среди сетевых администраторов, шпионов и хакеров по всему миру.



**Рис. 10.3.** Программа Ethereal, осуществляющая перехват сетевого трафика HTTP-сессии

Программа Ethereal позволяет перехватывать трафик в сетях Ethernet, Token-Ring и т. д., а также считывать данные, перехваченные другими программами (ее службы позволяют восстанавливать данные из более чем 340 различных протоколов). Это чрезвычайно удобно, если вы хотите установить небольшую программу сетевого мониторинга, такую как WinDump (см. веб-сайт [windump.polito.it](http://windump.polito.it)) для автоматического мониторинга сетевой активности с последующим анализом полученной информации. Ethereal обладает обширными возможностями в плане настройки различных фильтров, а имеющаяся опция «Follow TCP stream» позволяет целиком просматривать поток данных сессии.

Ethereal – это программа, которую просто обязан иметь шпион, занимающийся сетевым наблюдением. Изучить инструкцию по использованию этой утилиты и загрузить установочный модуль можно с веб-узла [www.ethereal.com](http://www.ethereal.com).



Многие сетевые мониторы под Windows, такие как Ethereal, требуют наличия в системе WinPCap – Unix-порта libpcap для Win32 (широко распространенный API для сетевого программирования, предназначенный для захвата и отправки пакетов по сети). Исследователи из Итальянского политехнического института в Торино (Politecnico di Torino) разработали свободно распространяемую версию WinPCap и сопутствующие приложения. Если вы используете операционную систему Windows XP, вам необходимо иметь WinPCap версии 2.3 или более поздней. За более подробной информацией по программе WinPCap и инсталляционным файлом обращайтесь на веб-сайт <http://winpcap.polito.it>.

## ДРУГИЕ СЕТЕВЫЕ МОНИТОРЫ

Хотя программы, подобные Ethereal, отлично подходят как для шпионских целей, так и для применения системными администраторами для повседневных нужд, советуем вам также обратить внимание на возможности альтернативных программ, созданных специально для выполнения шпионажа:

- **Dsniff.** Dsniff – это программа, предназначенная для подслушивания паролей. Ее написал Даг Сонг, причем изначально она работала только под Unix. Вместо перехвата и сохранения всего сетевого трафика, Dsniff действует более избирательно, сохраняя имена учетных записей и пароли, передаваемые через FTP, Telnet, HTTP, POP, NNTP, IMAP, IRC, AIM, Microsoft SMB и аутентификационные последовательности многих других протоколов. Перенос программы в среду Windows выполнил Майк Дэвис – теперь Windows-версию можно найти на сайте [www.datanerds.net/~mike/dsniff.html](http://www.datanerds.net/~mike/dsniff.html).
- **Ettercap.** Еще одним многоплатформенным сетевым монитором является разработанная Альберто Орнаги и Марко Валери программа Ettercap, позволяющая работать в сетях с коммутаторами путем использования ARP-спуфинга. При помощи данной

программы вы можете осуществлять в сети поиск специфической информации и собирать пароли, используемые во многих протоколах. Ettercap можно загрузить с веб-узла <http://ettercap.sourceforge.net>.

- **Cain & Abel.** Программа Cain & Abel (Каин и Авель) представляет собой еще одну разновидность швейцарского складного ножа. Она способна перехватывать данные в сетях, имеющих в своем составе коммутаторы, и расшифровывать пароли, с которыми ей приходится сталкиваться по ходу дела. Эта утилита, автором которой является Массимилиано Монторо, размещена на веб-сайте [www.oxid.it](http://www.oxid.it).

## Контрмеры

Существует множество способов укрепления защиты системы от сетевых шпионов. Эти же контрмеры помогут вам защититься и от обычных взломщиков, которые были и остаются главной угрозой простого пользователя из-за своего огромного числа и наличия большого количества вспомогательных хакерских утилит в сети Интернет.



Более подробные сведения по различным контрмерам вы можете найти в книге «Защита от хакеров» Джона Чирилло, выпущенной издательством Wiley в 2002 году. Информацию о книге можно прочесть на сайте издательства по адресу [www.wiley.com/cda/product/0,,0471232831,00.html](http://www.wiley.com/cda/product/0,,0471232831,00.html)<sup>\*</sup>.

Некоторые контрмеры подразумевают применение тех же самых утилит, которые хакеры могут использовать против вас (по принципу «клип клином вышибают»), – научившись пользоваться ими, вы лучше поймете уязвимые места вашей собственной системы. Наш следующий раздел мы посвятим рассмотрению ключевых контрмер по борьбе с сетевыми шпионами.

## Установка пакетов обновлений для операционной системы и отдельных приложений

Прежде всего, убедитесь в том, что для самой операционной системы Windows, Internet Explorer, Outlook, Microsoft Office и любых других программных продуктов, связанных с работой в Интернете, вами установлены все имеющиеся на данный момент времени пакеты исправлений системы безопасности. (В главе 4 мы рассказывали вам, как нужно оста-

<sup>\*</sup> Перевод книги на русский язык выпущен в 2002 году издательством «Питер». – Прим. ред.

ваться в курсе событий о выходе последних обновлений и «заплат» для продуктов компании Microsoft.)

Огромное количество ошибок, обнаруженных в программах производства Microsoft, таких как Outlook, Outlook Express и Internet Explorer, может служить аргументом в пользу замены вашего почтового клиента и веб-браузера на аналогичные программы сторонних производителей, если вы всерьез обеспокоены безопасностью системы. На рынке представлено множество бесплатных или недорогих аналогов известных продуктов от Microsoft. (Возьмите на заметку, что в некоторых программах сторонних производителей может осуществляться вызов программного кода Outlook или Explorer, соответственно, приводя к угрозе использования тех же уязвимых мест. Поэтому, прежде чем использовать то или иное приложение от стороннего разработчика, убедитесь, что в нем не используются функции стандартных программ Microsoft, в противном случае обязательно установите все выпущенные на данный момент пакеты обновлений для Outlook и Internet Explorer, даже если вы не используете сами программы.) Кроме того, подумайте над идеей установки настольной версии Linux, поскольку процесс инсталляции этой операционной системы можно даже назвать дружественным пользователю. Помните, что такие программные продукты, как Open Office (версии которых доступны как для Windows, так и для Linux), представляют собой бесплатную альтернативу оболочке Microsoft Office. (Сей факт, однако, не означает, что ОС Linux либо приложения для нее неуязвимы для сетевых атак. Скорее всего, с ростом популярности Linux в этой системе, как и в приложениях для нее, будут обнаруживаться все новые слабые места системы защиты. Как показывает практика, между популярностью программного продукта и количеством найденных в нем ошибок существует прямая зависимость.)

## Использование систем обнаружения вторжений

Системы обнаружения вторжений (IDS – intrusion detection system) представляют собой программные утилиты для выявления попыток сетевого нападения. Сетевые IDS осуществляют наблюдение и анализ сетевого трафика, ища признаки проведения атаки. Централизованная система обнаружения вторжений изучает серверные журналы, пытаясь найти следы сетевых атак, и может также включать в себя опцию проверки целостности файлов (чтобы выявлять случаи скрытого внесения изменений в системные файлы). Если по ряду признаков можно судить о проведении сетевой атаки, IDS немедленно уведомляет об этом сетевого администратора.

Приведем примеры коммерческих и свободно распространяемых систем обнаружения вторжения для Windows:

- **Snort.** Эта программа является одной из наиболее популярных, свободно распространяемых по принципу открытого кода систем обнаружения вторжений. Первые ее версии были разработаны для ОС Unix и только затем перенесены в Windows. Программа Snort умеет анализировать сетевой трафик в режиме реального времени, сохранять в журнал содержимое сетевых пакетов и обнаруживать огромное количество разновидностей сетевых атак и тестовых проникновений, таких как вызов ошибки переполнения буфера, скрытое сканирование портов, CGI-атаки, попытки доступа к блоку серверных сообщений (SMB), а также операции определения версии операционной системы. Для неспециалиста утилиты Snort может показаться немного сложной в установке и настройке, однако в комплекте с ней идет небольшое руководство по установке под Windows. Загрузить программу вы можете с веб-узла [www.snort.org](http://www.snort.org).
- **BlackIce PC Protection.** Некоторые специалисты в области безопасности до сих продолжают спор, к какой категории программ в первую очередь следует отнести BlackIce (ранее известную как BlackIce Defender) – брандмауэрам или системам обнаружения вторжений. Эта пионерская разработка в сфере безопасности реализует ряд мощных возможностей для средних и опытных пользователей. Стоимость однопользовательской лицензии на программу составляет \$39,95, тогда как серверная версия продается по цене \$299,95. Подробная информация по данному продукту, включая доступную для загрузки пробную версию, размещена на сайте [www.iss.net](http://www.iss.net).
- **Securepoint Intrusion Detection.** Securepoint Intrusion Detection является относительно новой, подающей надежды бесплатной программной утилитой для Windows. Эта программа была разработана немецкой компанией Securepoint, и ее можно найти на официальном сайте компании [www.securepoint.cc/en/products-sids.html](http://www.securepoint.cc/en/products-sids.html).



На личном сайте Роберта Грэхема опубликованы ответы на наиболее часто задаваемые вопросы (FAQ) о системах обнаружения вторжений. Адрес сайта в сети Интернет: [www.robertgraham.com/pubs/network-intrusion-detection.html](http://www.robertgraham.com/pubs/network-intrusion-detection.html).

## Использование брандмауэров

Брандмауэры предназначены для защиты системы от вторжения извне за счет создания некоего барьера между вашей компьютерной системой и внешним миром (обычно сетью Интернет). Принцип работы брандмауэров основан на избирательном пропуске одних сетевых пакетов и задержке других. Представьте себе брандмауэр в виде охранника трафика по протоколу TCP/IP, который постоянно проверяет все поступающие и отправляемые пакеты на дружественность на основе заданного набора признаков.

Существуют как программные, так и аппаратные брандмауэры, а в некоторых случаях оба типа брандмауэров могут работать совместно. Обычно в брандмауэрах используется три различных механизма фильтрации сетевого трафика:

- **Фильтрация на уровне приложений.** Такой тип фильтрации характерен для персональных программных брандмауэров, когда работа в сети разрешена для заслуживающих доверия приложений, а при попытке установки внешнего подключения со стороны непроверенного приложения происходит его блокировка либо выводится предупреждение для пользователя. Данный тип фильтрации позволяет выявлять троянских коней и другое шпионское программное обеспечение (spyware), пытающееся тайно отправлять данные через Интернет.
- **Фильтрация на уровне пакетов.** Пакетная фильтрация сводится к пропуску или блокированию пакетов на основе содержащегося в них заголовка. Вам требуется настроить набор правил избирательной обработки пакетов на основе определенных критериев, таких как IP-адреса отправителя или получателя, номера портов либо типы сетевого протокола.
- **Анализ статуса пакета.** Брандмауэр проверяет IP-адрес отправителя и получателя, номера портов отправителя и получателя, а также последовательность нумерации, чтобы определить, принадлежит ли данный пакет текущему активному подключению. Таким образом гарантируется, что весь сетевой обмен инициирован данным компьютером, находящимся под защитой брандмауэра, и общение происходит только с теми удаленными компьютерами, которые заслужили доверие, исходя из предыдущих сеансов работы. Брандмауэры, анализирующие статус пакетов, обычно держат другие порты закрытыми до тех пор, пока к ним не поступит запрос из текущего подключения, – это помогает решить проблему сканирования портов извне.

Тем не менее вы должны понимать, что даже брандмауэры не всесильны, и потому их нельзя считать несокрушимым уровнем защиты системы. Существует масса способов обхода защиты брандмауэров, с учетом их архитектуры и обнаруженных брешей, для которых не были установлены «заплаты». (Если вы посетите веб-сайт [www.paoloiorio.it/fw.htm](http://www.paoloiorio.it/fw.htm), то

попробуйте воспользоваться размещенной здесь программой FIREWAR, написанной автором сайта Паоло Иорио, – она позволяет удаленно отключать многие популярные персональные брандмауэры.) Поэтому перед тем как доверить безопасность системы определенному брандмауэру, изучите его возможности и ограничения.



Вы можете найти в сети Интернет множество веб-служб, позволяющих выполнять тестовые проникновения и сканирование портов компьютера с заданным IP-адресом, проверяющих тип установленного брандмауэра (либо его отсутствие). Веб-страница Стива Гибсона *Shield is Up* (по адресу [www.grc.com/x/ne.dll?bh0bkyd2](http://www.grc.com/x/ne.dll?bh0bkyd2)) пользуется немалой популярностью, кроме того, на ней приведены ссылки на дружественные сайты. Возможность более тщательного сканирования портов предоставляет вам компания Sygate на сайте <http://scan.sygatetech.com>.

## АППАРАТНЫЕ БРАНДМАУЭРЫ

Функции аппаратного брандмауэра обычно встроены в сетевые маршрутизаторы или коммутаторы, выступающие в роли шлюза между локальной сетью и Всемирной паутиной. Входящий и исходящий трафик контролируется на основе определенного пользователем набора правил. Вы задаете правила и настраиваете брандмауэр при помощи Telnet либо специального браузера, предназначенного для подключения к устройству и его конфигурирования.

Многие маршрутизаторы поддерживают протокол DHCP (динамического конфигурирования) и NAT (трансляции сетевых адресов). Протокол DHCP позволяет автоматически назначать IP-адрес подключенными к маршрутизатору компьютерам. Эта утилита популярна среди пользователей домашних компьютеров и представителей малого бизнеса, использующих сетевые решения для разделяемого широкополосного подключения. NAT делает IP-адрес конкретного компьютера невидимым за пределами маршрутизатора, в результате чего весь исходящий трафик как бы отправляется с одного и того же адреса. Некоторые производители называют устройства с поддержкой NAT брандмауэрами, что в принципе не совсем правильно.

Важно понимать, что не все аппаратные брандмауэры обладают одинаковыми возможностями. К примеру, маршрутизатор от компании Linksys, входящий в ценовой диапазон до \$100, который предназначен для домашнего применения либо использования в сетях небольших компаний, не обладает функциями, присущими маршрутизатору Cisco, ориентированному на корпоративное применение. Корпоративные брандмауэры обладают более сложными функциями фильтрации пакетов и возможностями их сохранения, а также лучше приспособлены для управления большими объемами передаваемых данных.

## ПРОГРАММНЫЕ БРАНДМАУЭРЫ

### Контрмеры: наблюдение за брандмауэром

Если вы всерьез обеспокоены собственной безопасностью, вам следует регулярно проверять журналы брандмауэра. Записанная в них информация может вывести вас на злоумышленников, заинтересованных во взломе вашей системы безопасности.

Многие популярные аппаратные брандмауэры нижнего уровня обладают весьма ограниченными функциями в плане сохранения в журналах информации о попытках сетевых атак и т. п. Для этой цели предназначены специальные программы, взаимодействующие с аппаратным обеспечением и предлагающие более широкие возможности анализа сетевой активности, включая данные о пробных проникновениях и широкомасштабных сетевых атаках. Двумя наиболее популярными утилитами считаются:

- **WallWatcher**, свободно распространяемая утилита от компании Linksys, которую можно загрузить по адресу [www.wallwatcher.com](http://www.wallwatcher.com).
- **Kiwi Syslog Daemon**, средство для работы с брандмауэрами, позволяющее генерировать стандартные системные журналы. Свободно распространяемую и коммерческую версию утилиты можно найти по адресу [www.kiwisyslog.com](http://www.kiwisyslog.com).

Эти утилиты позволяют собирать детальную статистику сетевого трафика, включая сведения о недружественных соединениях.

С распространением широкополосных подключений на дому и на малых предприятиях за последние несколько лет резко возросла популярность программных брандмауэров. Существует две разновидности программных брандмауэров:

- **Шлюз.** Шлюзом называют компьютер, расположенный между сетью Интернет и локальной сетью, который отвечает исключительно за работу брандмауэра либо программного обеспечения, играющего роль маршрутизатора. Старые компьютеры (486-й или Pentium I) под управлением Linux и с установленным бесплатным ПО для обеспечения безопасности – отличные кандидаты на эту роль. (Если вас заинтересовала данная тема, посетите веб-сайт [www.linux-firewall-tools.com/linux/](http://www.linux-firewall-tools.com/linux/).)
- **Персональный брандмауэр.** Персональный брандмауэр устанавливается на отдельном компьютере и выполняет сторожевые

функции для входящего и исходящего трафика. Среди популярных персональных брандмауэров под Windows можно назвать Kerio, Norton, Sygate и ZoneAlarm.

Персональные брандмауэры просты в установке и использовании. Они могут применяться автономно либо в содружестве с аппаратными брандмауэрами, обеспечивая двойную защиту.

Дополнительная причина использования персональных программных брандмауэров заключается в том, что они поддерживают функциональность, которая отсутствует у аппаратных брандмауэров, – фильтрацию исходящих соединений. Такие брандмауэры защищают вас от троянских коней, выдавая предупреждение, в случае если некоторое приложение попытается подключиться к Интернету для отправки данных. Вам нужно будет только указать заслуживающие полного доверия программы, такие как, например, веб-браузер, чтобы предупреждение не выводилось каждый раз, когда дружественное приложение пытается подключиться к сети Интернет. (Входящий в состав операционной системы Windows XP брандмауэр подключения к Интернету (ICF – Internet Connection Firewall) не поддерживает функцию фильтрации исходящих подключений. Из-за этого существенного недостатка советуем вам поискать свободно распространяемые или коммерческие брандмауэры сторонних производителей для укрепления защиты вашей системы.)

Для опытного шпиона не составит труда организовать тайную передачу данных через тот же Internet Explorer, минуя защиту брандмауэра, поэтому, если вас по-настоящему волнует вопрос безопасности, подумайте о переходе на другие браузеры, такие как Mozilla, Phoenix или Opera.

Большинство производителей коммерческих персональных брандмауэров выпускают бесплатно распространяемые версии своих программных продуктов с ограниченными возможностями (которых вполне достаточно среднестатистическому пользователю для защиты своего домашнего компьютера от сетевой атаки).



Список производителей брандмауэров, в большинстве своем корпоративной направленности, вы можете найти в руководстве для покупателя Computerworld на сайте [www.computerworld.com/services/buyersguide/subcat/0,4846,KEY73\\_SUB16,00.html](http://www.computerworld.com/services/buyersguide/subcat/0,4846,KEY73_SUB16,00.html). Более подробную информацию по брандмауэрам SOHO (Small Office Home Office), включая спецификации и обзоры, вы можете найти на сайте [www.firewallguide.com](http://www.firewallguide.com).

## Виртуальные частные сети

Виртуальные частные сети (VPN – virtual private network) – это сети, в которых для связи между компьютерами используется подключение к Интернету, а не непосредственное соединение при помощи сетевого шнура. При помощи VPN вы можете легко подключиться к своему домашнему или офисному компьютеру отовсюду, где имеется подключение к сети Интернет.

Для работы виртуальных частных сетей используются специальные протоколы, такие как IPSec, L2TP или PPTP, для передачи данных между двумя компьютерами либо сетями, подключенными к Интернету. Этот процесс называют *туннелированием*. Каждый IP-пакет шифруется, а затем помещается внутрь другого пакета с заголовком, позволяющим передавать его из одного пункта в другой. Когда пакет достигает пункта назначения, программное обеспечение для VPN удаляет заголовок, дешифрует содержимое пакета и перенаправляет его адресату. Виртуальные частные сети представляют безопасный способ сетевого общения через Интернет, с помощью которого ваши данные оказываются защищены от армии шпионов, вооруженных программами перехвата сетевых пакетов.

## Контрмеры: узнаем, кто наш враг

Определить, являетесь ли вы жертвой целенаправленной сетевой атаки или просто случайным объектом серии пробных нападений со стороны хакеров, можно при помощи специальной программы анализа журнала вашего брандмауэра, отправляющей содержимое журнала на центральный сервер для более тщательного изучения.

Существует несколько бесплатных служб, обрабатывающих файлы журнала брандмауэра и сообщающих об атаках хакеров провайдеру услуг Интернета, с которого были инициированы эти действия. Если провайдер услуг Интернета представит вам отчет, вы сможете выяснить, были ли предприняты какие-либо действия в отношении лиц, подозреваемых в причастности к сетевой атаке. Вы также можете просмотреть информацию об IP-адресе отправителя запроса и выяснить, использовался ли этот адрес для сканирования либо незаконного получения доступа к другим компьютерам (или же вы являетесь его единственной целью).

К двум наиболее популярным клиентам, распространяемым к тому же совершенно бесплатно, относятся MyNetWatchman и Dshield. Чтобы узнать о них подробнее и загрузить сами утилиты, посетите веб-сайты:

- ❑ [www.mynewwatchman.com](http://www.mynewwatchman.com),
- ❑ [www.dshield.org](http://www.dshield.org).

Провайдеры услуг, разработавшие эти программы и занимающиеся поддержкой вышеперечисленных сайтов, полагают, что чем больше людей начнет использовать подобные утилиты, тем сложнее будет отдельным хакерам инициировать свои атаки, поскольку их действия будут на корню пресекаться провайдерами интернет-услуг.

В Windows 2000 и XP имеется встроенная поддержка VPN-соединений и возможность использования данного компьютера в качестве клиента. На рынке представлено огромное количество свободно распространяемых и коммерческих программных продуктов и оборудования, предназначенных для создания виртуальных частных сетей. (Одной из таких свободно распространяемых утилит является программа Stunnel, использующая SSL для безопасного общения между сервером и клиентом. За более подробной информацией обращайтесь на сайт [www.stunnel.org](http://www.stunnel.org).)



В качестве хорошего информационного ресурса для изучения вопросов, связанных с использованием виртуальных частных сетей, можем порекомендовать веб-сайт компании VPN Labs, размещенный по адресу [www.vpnlabs.com](http://www.vpnlabs.com).

## Мониторинг сетевых подключений

Иногда вам нужна не вся информация, которая может быть собрана при помощи программы перехвата сетевых пакетов. Возможно, вас интересует только присутствие некоторого тайно установленного шпионского ПО, передающего информацию с вашего компьютера на другой. Для того чтобы отслеживать, какие порты вашего компьютера активны и заняты приемом данных, можно воспользоваться целым рядом утилит.

Простейший способ получить информацию об открытых в данный момент времени портах – набрать в командной строке `netstat -a`.

Единственная проблема заключается в том, что с помощью этой команды нельзя определить, какая программа какой порт использует. К счастью, существуют и другие, более дружественные к пользователю утилиты под Windows, позволяющие получать подробную информацию:

- **Inzider.** Эта утилита выводит список процессов и используемых ими портов. Она распространяется бесплатно, а найти ее можно на сайте [www.ntsecurity.nu/toolbox/inzider/](http://www.ntsecurity.nu/toolbox/inzider/).
- **TCPView.** Отображает список процессов, занятых прослушиванием определенных портов либо уже установивших соединение через некоторый порт. Утилиту можно загрузить с сайта [www.sysinternals.com](http://www.sysinternals.com).
- **TDIMon.** Еще одна программа от сайта [www.sysinternals.com](http://www.sysinternals.com), которая может отображать в режиме реального времени информацию, отправляемую по протоколам TCP и UDP, включая имя процесса, подключенного к Интернету, порты и IP-адреса источника и получателя и другую сетевую информацию.

## Применение программ перехвата сетевых пакетов

### Разоблачения: Рассел Филлер и НАСА

В ноябре 2002 года 47-летний пилот НАСА Рассел Филлер отправился в полет на одномоторном самолете Cessna вместе со своим летным инструктором, для того чтобы возобновить летную лицензию. После того как самолет поднялся на высоту трех тысяч метров, в момент, когда его летный инструктор отвлекся, Филлер отстегнул ремни безопасности, открыл дверь кабины и выпрыгнул из самолета. Его тело нашли через два дня.

Постепенно начали всплывать некоторые подробности дела. Оказалось, что Филлера собирались обвинить в краже принадлежащего НАСА ноутбука, который был похищен из космического центра Джонсона в конце октября. Средства массовой информации постоянно муссировали эту историю, сообщая о том, что на резиденцию Филлера полицейских вывел «жучок», встроенный в украденный ноутбук.

До своего самоубийства Филлер заявлял следователям, что он увидел в супермаркете объявление о продаже ноутбука за 500 долларов. Он сказал, что догадывался, что ноутбук, скорее всего, краденный, однако отказаться от такого выгодного предложения не смог. Следователи не поверили версии Филлера, и обвинения оставались в силе до самой его смерти.

Власти сообщили, что на похищенном компьютере не содержалось никакой конфиденциальной информации, однако так и не рассказали, как же они вычислили Филлера. Имел ли компьютер встроенный GPS, специальную сетевую карту, умеющую «звонить домой» через Интернет, или же спрятанный внутри миниатюрный радиопередатчик? Все это, конечно, возможно, однако маловероятно.

Некоторые косвенные доказательства позволяют предположить, что бывший владелец ноутбука НАСА просто сохранил в настройках коммутируемого соединения имя своей учетной записи и пароль для подключения к серверу НАСА. Скорее всего, Филлер обнаружил эти настройки и, подключив компьютер к телефонной линии, попытался установить соединение. Соединение с сервером было установлено, после чего, вероятно, сервер записал телефонный номер, с которого поступил звонок, благодаря чему правоохранительные органы и вышли на Филлера. Поэтому, хотя версию с наличием в ноутбуке встроенного следящего устройства нельзя полностью отбрасывать, наиболее вероятной причиной всей цепочки произошедших событий с трагической развязкой послужила одна совершенная владельцем ошибка.

Вновь наденьте свой черный плащ и сыграйте роль шпиона, запустившего программу Ethereal или Ettercap в своей сети, чтобы определить, какие данные могут быть украдены потенциальным злоумышленником. Результаты могут оказаться для вас сюрпризом. Чем больше вы знаете о сетевых протоколах, тем лучше сможете разобраться в увиденном, хотя не нужно быть компьютерным гуру, чтобы вычислить пароли, передаваемые в виде простого текста, и найти фрагменты другой конфиденциальной информации.

## Применение сканеров портов и уязвимых мест

Наряду с использованием в вашей сети программ перехвата сетевых пакетов, следует произвести сканирование портов компьютеров и выполнить поиск уязвимых мест. (Пожалуйста, не забудьте вначале получить согласие руководства на проведение подобных мероприятий, дабы не оказаться пойманными в роли шпиона и не провести свои лучшие годы в тюрьме.) Так вы сможете на один шаг опередить настоящего шпиона, залатав все обнаруженные бреши, прежде чем ими успеет воспользоваться злоумышленник. Это также поможет вам научиться идентифицировать признаки проводимых пробных проникновений и сетевых атак, поскольку вам потребуется изучить журналы ОС и системы обнаружения вторжений после проведения тестового сканирования. Проверка безопасности системы должна проводиться как изнутри, так и вне пределов защитного брандмауэра, поскольку сетевая атака может быть организована с любой стороны. Подобное сканирование должно проводиться регулярно для обнаружения новых компьютеров в сети, выявления случаев модификации программного обеспечения на существующих компьютерах и поиска новых уязвимых мест в защите систем (не забывайте своевременно обновлять ваше программное обеспечение для сканирования портов и обнаружения уязвимых мест – не реже, чем вы это делаете для антивирусного ПО).

## Шифрование сообщений электронной почты

Чтобы защитить свою личную и деловую корреспонденцию от шпионов, необходимо воспользоваться шифрованием сообщений электронной почты перед отправкой и заставить людей, с которыми вы переписываетесь, сделать то же самое. Напомним вам, что стандартом шифрования переписки де-факто является утилита PGP, благодаря своей популярности и устойчивому алгоритму шифрования.



Более подробную информацию о программе PGP вы найдете в главе 5.

С шифрованием данных связана одна проблема – если за вами кто-то следит, то передача зашифрованной информации может привлечь внимание к вашим действиям. Даже если шифрование используется на законных основаниях (как на данный момент в Соединенных Штатах), в некоторых ситуациях бывает нежелательно, чтобы люди подозрительно относились к вашей корреспонденции. (Ведь если вы прибегли к шифрованию, очевидно, вам есть что скрывать?) Один из способов избавиться от излишне пристального внимания – воспользоваться технологией стеганографии, то есть передачей сообщений внутри файлов другого типа – например, в картинках либо файлах mp3. В разделе «Контрмеры» главы 4 мы подробно рассказывали об этой технологии и даже перечислили некоторые утилиты, реализующие ее. (В связи с повсеместным распространением компьютерного «спама», одним из эффективных приемов стеганографии является использование предварительно оговоренных кодовых слов внутри электронных сообщений рекламного характера, обещающих сделать вас богатыми, улучшить вашу личную жизнь либо предлагающих вам свободно купить онлайн лекарства, отпускаемые только по рецепту врача. Получатель определяет, что данное электронное письмо не является «спамом», а содержит зашифрованное послание, которое декодируется с помощью предварительно определенных кодовых слов. Если все сделать правильно, то вероятность того, что наблюдающий за вами шпион что-то заподозрит, чрезвычайно мала.)

## Шифрование мгновенных сообщений

В последнее время необычайную популярность в личном и деловом общении приобрели службы обмена мгновенными сообщениями. Однако до недавних пор переговоры с помощью мгновенных сообщений легко можно было подслушать при помощи программ перехвата сетевых пакетов, поскольку используемые при этом протоколы подразумевают передачу этих сообщений в виде простого текста. Тем не менее в последнее время появилось множество дополнительных подключаемых модулей для служб обмена мгновенными сообщениями, позволяющих выполнять шифрование при помощи стойких алгоритмов для защиты содержимого посланий от чужих глаз. Если вы пользуетесь службами обмена мгновенными сообщениями для делового общения, вам стоит всерьез задуматься о шифровании данных ради обеспечения конфиденциальности.

В качестве примера недорогих или бесплатно распространяемых утилит шифрования для служб обмена мгновенными сообщениями можно привести:

- **Trillian.** Универсальная программа шифрования, поддерживающая большинство протоколов обмена мгновенными сообщениями, реализованных в одном пользовательском интерфейсе. И коммерческая (по цене в \$25), и свободно распространяемая версии программ поддерживают стойкие алгоритмы шифрования мгновенных сообщений AIM и ICQ. Более подробно об этой программе вы можете узнать на сайте [www.trillian.cc](http://www.trillian.cc).

- **SpyShield.** Этот свободно распространяемый дополнительный подключаемый модуль шифрования PGP, предназначенный для использования в программах MSN Messenger и Windows Messenger, можно загрузить с сайта [www.commandcode.com](http://www.commandcode.com).
- **IIP (Invisible IRC Project).** IIP представляет собой приложение прокси, предоставляющее анонимный защищенный доступ к Internet Relay Chat (IRC). Это прокси-приложение работает со стандартными клиентами IRC (такими, как mIRC или X-Chat), а для обеспечения секретности переговоров подключается к специальным серверам IIP IRC. Более подробную информацию о IIP можно получить на веб-странице [www.invisiblenet.net/iip/index.php](http://www.invisiblenet.net/iip/index.php).

## Использование безопасных протоколов

Каждый раз, когда у вас появляется возможность использования безопасного протокола, не упускайте ее. К примеру, вместо Telnet применяйте SSH (Secure Shell). Вместо FTP – SSH или SCP (Secure Copy). Если сервер на другом конце соединения поддерживает вышеперечисленные протоколы, а многие серверы это уже умеют, ваша транзакция будет зашифрована целиком (включая имя учетной записи и пароль) и ее нельзя будет подслушать. Вы можете найти как коммерческие, так и бесплатные версии серверов и клиентов SSH. При использовании SSH убедитесь в том, что у вас установлена его самая последняя версия, в особенности это касается сервера, поскольку в предыдущих версиях были обнаружены критичные ошибки в системе защиты.



Джон Фитцгибон поддерживает веб-страницу, посвященную использованию бесплатных утилит SSH и SCP под Windows для обеспечения безопасности сетевого трафика. Найти этот сайт можно по адресу [www.jfitz.com/tips/ssh\\_for\\_windows.html](http://www.jfitz.com/tips/ssh_for_windows.html).

## Не доверяйте неизвестным вам компьютерам и сетям

Это не означает, что вам не следует использовать компьютеры Macintosh или AppleTalk. Мы хотим сказать вам другое: вы должны с осторожностью относиться к тем компьютерам в вашей сети, о которых вы не знаете, можно ли им доверять и какая система безопасности на них используется. К примеру, на компьютерах с общим доступом могут быть установлены keylogger-модули либо сетевые мониторы. Если вы вынуждены были прибегнуть к помощи компьютера, предназначенного для общественного использования, советуем вам сменить все пароли, которыми вы пользовались при работе с этим компьютером, как только вы доберетесь до заслуживающей доверия системы.

Предназначенные для общественного использования сети в этом случае намного безопаснее, если вы подключаетесь к ним с помощью собственного защищенного ноутбука и применяете для сетевого общения безопасные протоколы.

## Повышение безопасности системы при разделяемом доступе к файлам

Когда речь заходит о предоставлении общего доступа к файлам и папкам компьютера, вы можете предпринять несколько простых шагов, позволяющих защитить компьютер от атак NetBIOS. Практические меры сводятся к следующему:

- Если вам не нужен общий доступ к файлам и принтерам, не забудьте отключить его.
- Отключите использование протокола TCP/IP для общего доступа к файлам и принтерам, назначив для этой цели протокол IPX/SPX. Таким образом вы значительно осложните злоумышленникам задачу доступа к разделяемым ресурсам из сети Интернет.
- Всегда используйте надежные пароли для доступа к разделяемым данным.
- Ограничьте доступ к компьютеру только теми папками, которые содержат файлы, необходимые для совместной работы. Никогда не разрешайте совместный доступ к корневой папке диска.
- Задавайте только необходимый уровень доступа к совместно используемым папкам и файлам (например, доступ только для чтения). Никогда не предоставляйте разрешение на запись, если в этом нет крайней необходимости.
- Подумайте над настройкой доступа к разделяемым ресурсам с конкретных IP-адресов, поскольку DNS-имена легко можно сфальсифицировать.
- Заблокируйте порты NetBIOS, используемые по умолчанию для доступа к разделяемым ресурсам в Windows, по всему периметру сети при помощи внешнего маршрутизатора либо брандмауэра. Должны быть заблокированы порты TCP и UDP с номерами 137-139 и 445.

## Использование безопасных веб-служб электронной почты

Популярные почтовые системы, такие как Microsoft Hotmail или Yahoo-Mail, не имеют надежной защиты от просмотра. Сообщения могут быть перехвачены при помощи сетевого монитора или просмотрены на сервере системным администратором. Кроме того, многие подразделения правоохранительных органов имеют соглашения с основными провайдерами услуг Интернета и электронной почты для доступа к электронной почте пользователей. До 11 сентября правила выдачи ордеров на просмотр электронной почты соблюдались более строго, но с тех пор многие провайдеры стали чаще сотрудничать с полицией даже без ордеров, стремясь продемонстрировать свою лояльность.

Еще один вопрос, связанный с использованием общественных служб доступа к электронной почте, касается надежности систем. К примеру, в августе 1999 года в работе почтового сервиса Hotmail была обнаружена следующая ошибка: при вводе известного имени пользователя в сценарии HTML можно было получить полный доступ к почтовому ящику этого пользователя, включая возможность просмотра, отправки и удаления сообщений. Информация об этой ошибке успела приобрести широкую огласку, прежде чем она была исправлена, поэтому остается только догадываться, сколько почтовых ящиков могли быть взломаны таким образом.

Если вы вынуждены использовать общедоступные службы электронной почты, подумайте об альтернативных службах, таких как Hushmail. Hushmail предлагает целый ряд различных технологий шифрования, способных защитить ваши сообщения от внимания со стороны шпионов. Прежде всего, для работы с сервером почтовой службы используется соединение SSL, защищающее пересылаемые между компьютером и веб-сервером данные от чужих глаз. Затем для доступа к вашему почтовому ящику вам потребуется ввести пароль. Hushmail использует стандарт шифрования OpenPGP с 2048-битным ключом для отправки и получения зашифрованной почты. (Только пользователи Hushmail могут безопасно общаться друг с другом.)

Система Hushmail организована таким образом, что открытый и секретный ключи пользователя хранятся на сервере и зашифровываются при помощи заданной пользователем фразы-пароля. Если даже судебные органы предъявят ордер на предоставлении копии ключей либо отправленных пользователем сообщений, компания Hushmail сможет в лучшем случае предоставить им зашифрованные версии, поскольку расшифровать их без помощи пользовательского пароля невозможно.

Вы можете абсолютно бесплатно завести себе почтовый ящик, обладающий всеми базовыми возможностями шифрования, либо заказать ящик с расширенными возможностями на сайте [www.hushmail.com](http://www.hushmail.com).

## Использование программ анонимной пересылки корреспонденции

Программы анонимной пересылки сообщений позволяют перенаправлять электронные сообщения на определенный адрес. В отличие от генераторов фальшивых электронных писем, оставляющих в заголовке письма информацию об IP-адресе отправителя, дате и времени отправления и т. п. информации, программы анонимной пересылки сообщений отсекают всю заголовочную информацию, которая могла бы идентифицировать отправителя.

Для того чтобы воспользоваться утилитой анонимной пересылки информации, вам необходимо отправить специальным образом отформатированное сообщение электронной почты на сервер с текстом, зашифрованным при помощи PGP-ключа программы пересылки. Когда программа пересылки корреспонденции получит это сообщение, она автоматически расшифрует его; затем, основываясь на заданном формате сообщения, перешлет письмо нужному адресату. В результате в конечном сообщении будет присутствовать только заголовок программы пересылки почты, без каких бы то ни было указаний на то, кто в действительности является отправителем послания. Если шпион следит за вашей почтой, все, что он сможет узнать, так это то, что вы послали кому-то письмо при помощи программы анонимной пересылки почты (не зная, кому именно). Если же кто-то наблюдает за почтовым трафиком получателя, он увидит только письмо, присланное программой анонимной рассылки почты, не имея представления о том, кто является первичным отправителем.

Программы анонимной пересылки почты обладают различными функциями безопасности, которые вы можете применять или не применять в зависимости от вашего уровня паранойи. Например, если вы хотите обеспечить себе безопасное общение с некой Наташей, вам необходимо зашифровать сообщение с помощью ее открытого ключа PGP, прежде чем отправить его с помощью программы анонимной пересылки почты. Кроме того, в формировании сообщения можно задать временную задержку, чтобы отправленное вами сообщение было переслано адресату не сразу, а, например, через несколько минут. (Если кто-либо ведет наблюдение за сервером, предоставляющим услуги по анонимной пересылке почты, он может связать между собой некоторые входящие и исходящие сообщения, наличие же временной задержки не позволит отследить связь сообщений.) И наконец, можно осуществить пересылку сообщений через целую цепочку серверов для анонимной пересылки информации. При этом для каждого следующего сервера сообщение должно быть закодировано с соответствующим ключом PGP. После того как вы корректно отформатируете и зашифруете ваше послание, вы можете отправить его на первый сервер, где оно будет расшифровано и передано на второй сервер, и т. д. по цепочке, пока оно не достигнет адресата.

Этот алгоритм нельзя назвать тривиальным для рядового пользователя, поэтому, когда серверы для анонимной пересылки корреспонденции

только начинали появляться, правильно зашифровать и отформатировать сообщение считалось далеко не простой задачей. К счастью, сейчас появились утилиты, позволяющие значительно облегчить этот процесс.

Программы анонимной пересылки почты, как правило, распространяются свободно по принципу открытого кода, поддерживаемого группами защитников прав на неприкосновенность частной жизни, использующими эти программы на своих почтовых серверах. Распространение получили два типа программ анонимной пересылки почты: Cypherpunk Type I и более безопасный Mixmaster Type II, в котором используется усовершенствованная технология защиты от анализа трафика. В начале 2003 года по всему миру насчитывалось более 50 активных серверов для анонимной пересылки корреспонденции.

За более подробной информацией по программам анонимной пересылки сообщений обращайтесь к следующим веб-ресурсам:

- [www.sendfakemail.com/~raph/remailer-list.html](http://www.sendfakemail.com/~raph/remailer-list.html). Содержит немало информации о различных программах анонимной пересылки корреспонденции. Хотя некоторые ресурсы и ссылки устарели, однако в целом этот сайт можно назвать неплохим источником информации общего плана.
- [www.chez.com/frogadmin/](http://www.chez.com/frogadmin/). Французский веб-сайт, содержащий современную статистику по программам анонимной пересылки корреспонденции и доступный для загрузки в файловый архив клиентских программ.



Автор написал одну из первых удобных в использовании утилит под Windows для анонимной пересылки почты, использующую шифрование PGP. Она увидела свет в 1995 году под названием Private Idaho (PI). Конечно, на сегодняшний день она несколько устарела, тем не менее кое-кто пользуется ею до сих пор. Эта программа, в конце концов, была выложена в Интернете вместе с кодами, поэтому сейчас вы можете найти ее новые версии, сделанные другими разработчиками. Подробная информация по программе Private Idaho и некоторым другим утилитам анонимной пересылки почты размещена по адресу [www.eskimo.com/~joelm/pi.html](http://www.eskimo.com/~joelm/pi.html).

## Использование прокси-серверов

Прокси-сервер – это компьютер, находящийся между клиентским компьютером и другим сервером. Прокси-сервер обрабатывает все запросы, отправляемые от клиентского компьютера к серверу и обратно. Прокси-серверы в среде веб часто используются для повышения производительности сети за счет кэширования часто посещаемых страниц, что экономит время и пропускную способность сети, поскольку информация передается по локальной сети, а не загружается заново из сети Интернет. Прокси-серверы могут быть также настроены на фильтрацию запросов. К примеру, в

корпоративной ЛВС при попытке обращения сотрудника к некоторому веб-сайту в сети Интернет запрос вначале обрабатывается прокси-сервером, который решает, предоставлять ли доступ к тому или иному сайту.

Помимо прокси-серверов, ориентированных на традиционную сферу применения, существуют специальные прокси-серверы, разработанные для обеспечения конфиденциальности. Обычно, когда браузер обращается к некоторому веб-сайту в сети Интернет, веб-сервер записывает IP-адрес клиента и другую доступную информацию о нем. Если же вы подключаетесь через прокси-сервер, искомый веб-сайт сможет записать в журнал только сведения о прокси-сервере, но не о вас.

Содержимое веб-страниц отправляется браузеру в незашифрованном виде, поэтому любое лицо, наблюдающее за вашим сетевым трафиком, сможет перехватить эту информацию. Это невозможно сделать при использовании вами протокола уровня безопасных сокетов (SSL – Secure Socket Layer), поскольку в этом случае данные перед отправкой шифруются. Некоторые прокси, предназначенные для обеспечения конфиденциальности, поддерживают передачу данных по протоколу SSL, однако будет ли ваше соединение являться полностью безопасным, зависит от того, поддерживается ли протокол SSL-сервером. Например, если вы захотите посетить веб-сайт cia.gov, прокси-сервер зашифрует запрошенные страницы при помощи SSL и отправит их вашему браузеру для дальнейшей расшифровки. Кто бы ни осуществлял мониторинг подключения, ему будет известно только то, что вы подключались к прокси-серверу, а затем получали от него зашифрованные данные. Никто не узнает, что вы подключались к веб-сайту ЦРУ, и, кроме того, сервер ЦРУ не запишет ваш IP-адрес посетителя.

Задайте в настройках браузера опцию использования прокси-сервера, затем укажите его IP-адрес и номер порта. При следующем посещении веб-страницы ваш браузер вначале перенаправит запрос на прокси-сервер. Существуют еще более простые в использовании прокси-серверы, реализованные непосредственно на веб-страницах в сети Интернет. Посетив такую страницу, вы можете задать на ней ссылку URL, к которой вы будете совершенно анонимно подключены.

Если вы намерены прибегнуть к помощи прокси-сервера для обеспечения секретности ваших действий в сети Интернет, учтите следующие моменты:

- Так или иначе, вам придется довериться некой компании, являющейся владельцем прокси-сервера, поскольку она может отслеживать и записывать в журнал все ваши действия.
- Предпочтительнее использовать прокси-серверы, поддерживающие протокол HTTPS (Hypertext Transfer Protocol Secure). Этот протокол фактически представляет собой реализацию того же HTTP, но с поддержкой SSL, позволяющего шифровать передаваемые данные.

- Хотя содержимое может передаваться в зашифрованном виде, адресная строка (URL), отображаемая в истории браузера, не подлежит шифрованию. В то же время некоторые прокси позволяют зашифровывать и адресную строку, так что ваш потенциальный шпион не сможет узнать, какие сайты вы посещали за последнее время.
- Навигация может осуществляться намного медленнее, в зависимости от загруженности сервера.
- По-прежнему может выполняться анализ трафика на основе сведений об объемах передаваемой информации; к примеру, повышенная сетевая активность может говорить о загрузке больших файлов, таких как музыка в формате mp3 или пиратское программное обеспечение, что, как правило, происходит без соблюдения авторских прав.

Существует целый ряд бесплатных и коммерческих прокси-серверов в сети веб, которые помогут обезопасить ваши действия в Интернете от потенциальных шпионов. Зайдите на поисковый сервер Google, чтобы просмотреть список бесплатных прокси-серверов с указанием предоставляемых услуг. Найти его можно по адресу <http://directory.google.com/Top/Computers/Internet/Proxies/Free/>.

## Заключение

Сети предоставляют в распоряжение шпиона различные способы похищения конфиденциальной информации. Шпионские технологии, описанные в этой главе, – это только верхушка айсберга. Опытный и решительный шпион воспользуется всеми доступными ему методами и средствами сетевого шпионажа для достижения своих целей.

Если вы работаете с конфиденциальной информацией, отнеситесь к вопросу сетевой безопасности серьезно. Важно, чтобы вы или кто-то другой в вашей организации посвятил время подробному изучению всех существующих уязвимых мест в сетевой защите систем, и впоследствии постоянно следил за сообщениями об обнаружении уязвимых мест и выпусксе соответствующих «заплат» к ним – такие сведения появляются в Интернете чуть ли не каждый день.

## Глава 11

# Беспроводные сети 802.11b

«Мы следим за компьютерами, мы прослушиваем телефонные линии. Я знаю, что это не разрешено».

Talking Heads, “Life During Wartime”, *Fear of Music*

## Знакомство с беспроводными технологиями

Популярность беспроводных локальных сетей (WLAN – wireless local area network) стандарта 802.11b растет огромными темпами. Беспроводные ЛВС можно встретить в больших корпорациях, жилых домах, аэропортах, ресторанах и кафе. В соответствии с расчетами компании Gartner Dataquest, объемы продаж оборудования для беспроводных сетей в 2003 году должны были превысить 26 000 000 единиц, по сравнению с 15 000 000 единиц оборудования, проданных в 2002 году. Причем развитие этого рынка ожидается вплоть до 2007 года. По расчетам Gartner, к концу 2003 года почти 50% используемых в деловой сфере ноутбуков должны были поддерживать беспроводные технологии связи.

Беспроводные ЛВС просты в установке и настройке (в этой главе термин «беспроводные ЛВС» будет применяться для беспроводных сетей стандарта 802.11b). В то же время беспроводные решения упрощают жизнь потенциального шпиона. Если вы будете использовать ненадежные протоколы, небезопасные настройки аппаратного обеспечения и при всем этом иметь дело с неграмотными пользователями, работающими с дешевым беспроводным оборудованием и программным обеспечением, не обеспечивающим должного уровня безопасности, – вы превратитесь в идеальную цель для любого шпиона.

Но перед тем как начать разговор о том, каким образом шпионы могут перехватывать информацию, передаваемую по беспроводной ЛВС, рассмотрим основы данной технологии. Если вы и так уже хорошо знакомы с ней, можете пропустить следующий раздел и переходить непосредственно к «шпионской тактике».

## История беспроводных технологий

В 1997 году американский Институт инженеров по электротехнике и электронике (IEEE) принял стандарт 802.11, создав основу для развития современных беспроводных технологий передачи данных. Одной из разновидностей стандарта стал стандарт 802.11b, называемый также Wi-Fi или Wireless Ethernet. После выпуска в 1999 году первых устройств с поддержкой 802.11b этот стандарт приобрел наибольшую популярность и востребованность при разработке беспроводных локальных сетей.

В соответствии со спецификацией стандарта 802.11b данные передаются в радиодиапазоне на скорости 11 Мб/с. Используемая ширина полосы частот составляет 2,4 ГГц с 15 каналами (в США, согласно требованиям Федеральной комиссии по средствам связи, используются 11 каналов). Для работы в беспроводной сети компьютер должен быть оборудован специальной сетевой интерфейсной картой (NIC – Network Interface Card) с приемопередатчиком. В качестве этой карты может выступать карта PC Card для ноутбука, карта расширения для настольного ПК либо устройство, подключенное к порту USB.

Помимо отдельных сетевых карт в состав большинства беспроводных ЛВС должно входить устройство, называемое точкой доступа (AP – Access Point) или базовой станцией, с приемопередатчиком, подключенным непосредственно к сети Интернет либо сетевому хабу или маршрутизатору. Базовая станция в этом случае служит как бы связующим звеном между проводной сетью и компьютерами, подключенными к внутренней беспроводной сети. А поскольку популярность беспроводных сетей непрерывно растет, многие производители начали предлагать беспроводные маршрутизаторы.

И сетевые интерфейсные карты, и базовые станции должны иметь встроенные антенны для приема и передачи радиоволн. Радиус действия беспроводной связи может составлять от 15 до 50 метров внутри помещения, причем в некоторых случаях возможна установка дополнительных внешних антенн для увеличения площади покрытия.

Главное преимущество беспроводных ЛВС заключается в быстроте и легкости настройки без необходимости прокладки кабелей и наличия глубоких знаний по сетям. Организация небольшой сети обойдется вам буквально в несколько сотен долларов – вам понадобится закупить необходимое оборудование и подключить его к компьютерной технике.

В то же время при отсутствии должного внимания к вопросам безопасности беспроводная сеть может стать для шпиона легкой добычей. Злоумышленник, сидя в машине, припаркованной на другой стороне улицы, может преспокойно жевать бургер и картофель «фри», одновременно подключившись к беспроводной сети и записывая информацию конфиденциального содержания.

## Шпионская тактика

Снова пришло время начать думать как шпион. На этот раз вам предстоит сыграть роль технического специалиста по обнаружению устройств наблюдения (его иногда называют «чистильщиком»). В ваши обязанности входит поиск аудио- и видеожучков, установленных «некорошими дядями» для слежки за вашими клиентами, среди которых встречаются известные политики, бизнесмены и другие люди, полагающие, что их частная жизнь может представлять интерес для шпионов. Вы зарабатываете неплохие деньги, однако, чтобы оставаться конкурентоспособным, вам необходимо заняться расширением сферы услуг. Вы решили, что лучше всего развиваться в плане компьютерной безопасности, а поскольку вы имели дело с беспроводными «жучками» уже довольно долгое время, первой из ваших новых услуг стало обеспечение безопасности беспроводных сетей. Хороший способ изучения беспроводных сетей – взглянуть на них с точки зрения шпиона.

Первый вопрос, который вы обязаны себе задать, звучит так: «Зачем шпиону проникать в беспроводную сеть?» Подумайте над ним пару минут, а когда закончите, сравните ваши ответы с приведенными ниже вариантами:

- для получения доступа к файлам и информации, размещенной на некотором компьютере в сети;
- чтобы узнать имена учетных записей и пароли пользователей;
- для тайной установки троянского коня или другого программного обеспечения на некотором компьютере в сети;
- для использования беспроводной сети в качестве плацдарма другой целенаправленной атаки.

Несмотря на всю сложность технической реализации беспроводных ЛВС, методы получения несанкционированного доступа к ним достаточно просты. В подавляющем большинстве случаев вам даже не понадобится опыт работы с сетью, подтвержденный несколькими сертификатами. Представьте себе, что какой-то подросток, сидящий в своем обшарпанном автомобиле марки Toyota на противоположной стороне улицы, может заниматься этим делом прямо сейчас.

Честно говоря, технологии беспроводной передачи данных еще нельзя назвать устоявшимися, и многие пользователи даже не подозревают о том, какие опасности может таить их применение. Поэтому сейчас мы изучим некоторые уязвимые места (посчитав, что в роли шпиона сейчас выступаете вы), которыми вы могли бы воспользоваться в своих целях.

## Использование уязвимых мест

Прежде всего, обратим ваше внимание на тот факт, что при разработке стандарта беспроводной связи 802.11b не ставилось целью обеспечение промышленной безопасности. Поэтому данному стандарту присущ ряд слабых мест, которыми вы можете воспользоваться.

### SSID

В протоколе 802.11b для обеспечения безопасности используются идентификаторы набора служб SSID (service set identifiers), содержащие идентификатор конкретной сети. Вероятно, что в качестве названия рабочей группы будет выступать Microsoft Network. Чтобы подключить к беспроводной ЛВС новый компьютер, необходимо задать в нем в качестве SSID то же имя, что заложено в базовой станции (точке доступа). Эта схема сама по себе не лишена целого ряда дизайнерских огехов и ошибок реализации, которыми могут воспользоваться шпионы.

Первое слабое место состоит в том, что производители обычно задают имена по умолчанию для SSID базовой станции. Если, например, вы работаете с базовой станцией Cisco, ее SSID по умолчанию будет *tsunami*. Список применяемых по умолчанию SSID базовых станций различных производителей приведен в таблице 11.1.

**Таблица 11.1. SSID по умолчанию для наиболее распространенных базовых станций**

Производитель	SSID
Cisco	Tsunami, WaveLan Network
3Com	101, comcomcom
Dlink	WLAN
Bay	Default SSID
Addtron	WLAN
Intel	101, 195, intel, xlan
Linksys	Linksys, Wireless
Netgear	Wireless
SMC	WLAN, BRIDGE
Lucent/Cabletron	RoamAbout Default Network Name
Compaq	Compaq

Если SSID вашей сетевой интерфейской карты соответствует SSID базовой станции и никакие другие меры безопасности не используются, ваш компьютер автоматически подключается к данной сети. Став абонентом сети, вы можете воспользоваться любыми утилитами из вашего набора взломщика для дальнейшего проникновения в систему безопасности.

Задавать SSID по умолчанию методом проб и ошибок – процесс довольно нудный, к тому же как быть, если администратор решил сменить имя, используемое по умолчанию?

Дело в том, что базовая станция передает SSID несколько раз в минуту в так называемом «кадре неисправности». Поэтому вам нужна только сетевая интерфейсная карта с приемопередатчиком и соответствующее ПО для перехвата SSID, чтобы далее вы могли задать его в настройках карты и таким образом подключиться к сети.

## WEP

В роли «чистильщика» вам удалось обнаружить несколько профессиональных «жучков», скорее всего установленных представителями правительственные служб. Вместо передачи обычного аналогового сигнала, они передавали цифровой сигнал в зашифрованном виде. Вы слышали, что беспроводные сети поддерживают возможность шифрования, но насколько будут защищены ваши данные при включении этой опции?

Достаточно серьезную защиту стандарта 802.11b обеспечивает шифрование Wired Equivalent Privacy (WEP). Разработчики стандарта 802.11b прекрасно понимали, что перехватить радиосигнал очень легко, поэтому целью разработки WEP являлось приближение безопасности беспроводных коммуникаций к уровню традиционных проводных технологий путем шифрования информации.

В технологии WEP используется 64-битовое шифрование потока по алгоритму RC4. Ключ шифра генерируется на основе 40-битового ключа WEP и 24-битового вектора инициализации (IV). Причина такой малой длины ключа WEP заключается в том, что на момент разработки стандарта это была максимальная длина ключа, разрешенная для экспорта. Таким образом, длина ключа составляла всего 5 символов в кодировке ASCII либо 10 символов в шестнадцатеричной системе счисления.

Из-за малой длины ключа шифр RC4 можно было достаточно легко взломать методом перебора в течение нескольких дней, и поэтому многие разработчики оборудования для 802.11b начали включать в свои продукты поддержку 128-битового шифрования RC4. Так и не став частью официального стандарта, тем не менее такой более строгий уровень шифрования приобрел всеобщее распространение, и теперь тот же 24-битовый вектор инициализации используется вместе с 104-битовым WEP-ключом. В этом случае ключ состоит из 26 символов шестнадцатеричной системы счисления либо 13 символов ASCII.

В протоколе также предусмотрена дополнительная схема аутентификации, предназначенная для использования в механизме шифрования WEP. Автоматизированная аутентификация при помощи разделяемых ключей реализована довольно примитивно – она включает систему шифрования запроса/ответа, в которой осуществляется генерирование информации и ее отправка клиенту; клиент в свою очередь шифрует данные и отсылает их назад; затем ответ дешифрируется и проверяется на аутентичность.

При использовании WEP в беспроводных сетях базовая станция и отдельные сетевые интерфейсные карты должны применять одни и те же WEP-ключи. Это необходимо для корректного шифрования и дешифрования информации, а также идентификации подключенных к сети клиентов. Одновременно могут применяться до четырех 40-битовых либо один 104-битовый ключ.

В WEP-шифровании имеется целый ряд уязвимых мест. Первое слабое место существует не по вине протокола, и оно связано с тем, что многие производители по умолчанию не включают WEP-шифрование в своих продуктах. А без шифрования любая передаваемая по сети информация легко может быть прочитана при помощи программы перехвата сетевых пакетов (о чем мы поговорим в разделе «Средства шпионажа для беспроводных сетей» данной главы).

Второе уязвимое место связано с тем, что даже при включении шифрования WEP-кодированию подвергаются только пакеты с данными. Отдельные пакеты с управляющей информацией, например с адресами отправителя и получателя, SSID- и MAC-адресами, передаются в виде простого текста. Поэтому даже если вы не сможете прочитать зашифрованные пакеты данных при помощи сетевого монитора, тем не менее вы можете восстановить общую картину происходящего по содержимому управляющих пакетов.

Последняя и наиболее вопиющая ошибка связана с реализацией алгоритма шифрования. С приходом популярности к той или иной компьютерной технологии ее безопасность подвергается более тщательному анализу, и в этом отношении технология WEP не стала исключением. В течение первой половины 2001 года проводилась целая серия исследований по сетевой безопасности стандарта 802.11b. Теоретические исследования устойчивости протокола дали толчок появлению целого ряда программных утилит, предназначенных для проникновения в защищенные с помощью WEP сети.

Таким образом, практически за один вечер пользователь, не обладающий глубокими техническими познаниями, может взломать WEP-ключ при помощи доступного недорогого оборудования и бесплатно распространяемого ПО.

## КОНТРОЛЬ СПИСКА МАС-АДРЕСОВ

Все беспроводные сетевые интерфейсные карты и базовые станции имеют свой уникальный MAC-адрес. Его значение жестко прошито в каждом сетевом устройстве. Численное значение MAC-адреса наносится где-то на самом устройстве. Первые шесть цифр MAC-адреса идентифицируют производителя, а оставшиеся представляют собой уникальный идентификатор данного экземпляра устройства.

Подобно IP-адресам, MAC-адреса также передаются от одного устройства к другому при их взаимодействии друг с другом.

## Тактика: атаки сетей, защищенных WEP

Шпионы обожают теоретиков компьютерных наук: блестяще образованные, любознательные люди настойчиво пытаются найти лазейку в предположительно хорошо спроектированной системе безопасности. Многочисленным тестам на выживаемость подвергался в 2001 году и стандарт 802.11b, который, к сожалению, показал себя не с лучшей стороны.

**Январь 2001-го** – группа ISAAK (The Internet Security, Application, Authentication and Cryptography) калифорнийского университета выпустила статью с описанием ошибок при подсчете контрольной суммы в векторе инициализации и самом алгоритме RC4. Комитет по разработке протокола 802.11 заявил, что ему и так известно об этих недостатках, и необходимые доработки будут реализованы в последующих версиях. Потенциальная угроза атак была признана несущественной, поскольку для ее реализации потребовались бы слишком большие вычислительные мощности.

**Март 2001-го** – исследователи из университета в Мэриленде опубликовали статью, посвященную раскрытию уязвимых мест, связанных с отправкой незашифрованных управляющих данных и ошибками в процессе аутентификации с использованием разделяемых ключей (о чем мы поговорим чуточку позже).

**Июль 2001-го** – исследователи Флурер, Мантин и Шамир обнаружили, что, зная незашифрованное значение вектора инициализации (IV) и первые байты пакетов, можно определить значение WEP-ключа. Месяц спустя, команда из университета Rice и корпорации AT&T успешно продемонстрировала на практике вычисление WEP-ключей, взломав их при помощи подручных средств в течение нескольких часов.

Хотя исследователи из университета Rice и AT&T никогда не публиковали разработанный ими программный код, удержать джина в бутылке им не удалось. В течение последующих нескольких месяцев в Интернете появился ряд утилит, позволяющих получать несанкционированный доступ к беспроводным сетям. Взломав WEP-ключ и воспользовавшись им для вашей сетевой интерфейской карты, вы получаете возможность перехватывать и расшифровывать любые передаваемые по сети пакеты данных (при отсутствии других мер безопасности).

Поэтому не забывайте следить за текущими научными исследованиями. Чем больше уязвимых мест вы будете знать и чем больше шпионских штучек будет в вашем арсенале, тем лучше.

Еще одной мерой предосторожности, предназначенней для защиты беспроводных сетей, является задание списка МАС-адресов, с которых разрешен доступ к данной сети. Если к беспроводной сети попытается подключиться ноутбук, сетевая интерфейсная карточка которого имеет адрес, отсутствующий в списке авторизованных МАС-адресов базовой станции, этому ноутбуку будет отказано в доступе.

## Тактика: фальсификация МАС-адресов в Windows

Компьютеры под управлением Windows 2000 и XP хранят МАС-адреса в реестре. Для того чтобы фальсифицировать МАС-адрес сетевой карты, необходимо сделать следующее:

- 1.** Создайте резервную копию существующего реестра.
- 2.** Найдите «NIC driver» в разделе реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}.
- 3.** Найдите ключи для вашей беспроводной сетевой интерфейсной карты.
- 4.** Укажите в ключе реестра NetworkAddress нужный МАС-адрес. Как правило, префикс должен соответствовать производителю вашей сетевой карты для корректной привязки (установки канала связи между драйвером протокола, например TCP/IP, и NIC) к IP-адресу. К примеру, если у вас в системе установлена сетевая карта Lucent, а вы хотите назначить ей новый МАС-адрес с префиксом Linksys, привязка, скорее всего, не сработает. Полный список префиксов МАС-адресов различных производителей приведен на странице <http://standards.ieee.org/regauth/oui/index.shtml>.
- 5.** Запустите команду IPCONFIG /ALL, чтобы проверить, была ли произведена привязка нового адреса.

Для некоторых сетевых интерфейсных карт, например ORiNO-CO Gold и ORiNOCO Silver, процедура изменения МАС-адресов еще проще. При помощи специального управляющего ПО можно заменить оригинальный МАС-адрес, зашитый в самой карте. Данная функция нужна не только шпионам, поскольку в некоторых сетевых операционных системах возникает необходимость локального переопределения МАС-адресов. Если же для вас это чересчур сложно, воспользуйтесь утилитой командной строки под названием BMACHAK (под авторством некоего хакера в области беспроводных технологий, называющего себя BlackWave), которая позволяет быстро менять МАС-адреса.

Хотя такой механизм фильтрации MAC-адресов может показаться не-плохой мерой безопасности, однако и он имеет несколько уязвимых мест:

- Во-первых, если у вас есть физический доступ к авторизованному компьютеру либо даже только к его сетевой интерфейсной карте, базовая станция автоматически разрешит вам подключиться к сети.
- Во-вторых, даже если вы не обладаете физическим доступом, вы можете выдать себя за авторизованного клиента, фальсифицировав MAC-адрес карты. Хотя сам MAC-адрес и считывается аппаратно, однако в дальнейшем это значение можно подменить с помощью функций операционной системы либо специальных утилит.

Взглянув на ситуацию с точки зрения шпиона, предположим, что вы хотите подключиться к беспроводной сети, в которой не включена функция шифрования, зная, какие MAC-адреса и SSID в ней используются. Вы задаете известный SSID в настройках вашей сетевой интерфейсной карты, однако подключиться к сети вам по-прежнему не удается. Вашим следующим шагом в этом случае будет фальсификация вашего собственного MAC-адреса путем его подмены одним из MAC-адресов, перечисленных в списке контроля доступа.

## РАДИОВОЛНЫ

За свою карьеру вы обнаруживали множество «жучков», работающих в диапазоне частот 398...399,5 МГц. Подобные устройства нижней ценовой категории продаются во многих «шпионских магазинах». Переходя к радиодиапазону в 2,4 ГГц, мы попадаем в область, занятую беспроводными сетями 802.11b. Этот частотный диапазон является достаточно перегруженным: в нем работают микроволновые печи, медицинские устройства, люминесцентные лампы и даже некоторые типы беспроводных телефонов, чьи паразитные сигналы отрицательно сказываются на функционировании беспроводных сетей.

Поскольку принцип работы беспроводных сетей основан на передаче радиосигналов, они уязвимы к так называемым атакам отказа в обслуживании за счет глушения оригинального сигнала. Глушение осуществляется путем передачи сигнала, мощность которого выше, чем у стандартных сетевых интерфейсных карт или базовых станций. Хотя для беспроводных сетей могут применяться те же технологии создания избирательных помех, что и в традиционных проводных технологиях передачи данных, в случае с беспроводными ЛВС шпиону легче воспользоваться высокомощным передатчиком, работающим в диапазоне 2,4 ГГц, чтобы нарушить работу всей сети. Поскольку максимальная мощность передатчиков беспроводного сетевого оборудования не превышает 4 Вт, даже простой радиолюбитель может переделать базовую станцию таким образом, чтобы

разрушить работу сети. Нельзя сказать, что применение постановщика помех такая уж красивая идея, однако поскольку его использование наверняка нарушает ряд законов, то почему бы вам не добавить его в свой шпионский арсенал.

Каким же образом атака типа «отказа в обслуживании» может помочь вам в ведении шпионажа? Дело в том, что она может создать вам предлог для посещения данного учреждения. Посудите сами.

Работая в офисе, вы уже устали от ежедневных проблем с сетью, когда никто не имеет ни малейшего понятия, что происходит. И вдруг на пороге офиса появляется улыбающийся мужчина в голубой форме с прикрепленным к рубашке удостоверением. «Здравствуйте, меня зовут Джон Смит. Я из телефонной компании. Мы получили сообщение о том, что у вас постоянные проблемы с сетью. Это может быть связано с помехами, излучаемыми проходящей рядом с вами телефонной магистралью. Я полагаю, что смогу это исправить. Вы можете показать мне, где находятся ваши маршрутизаторы?» Таким образом, этот «ремонтный рабочий», якобы из телефонной компании, который сам занимался постановкой помех в работе сети, проникает прямиком в офис компании, чтобы выкрасть интересующую его информацию.

## ПРОБЛЕМЫ С НАСТРОЙКАМИ ПО УМОЛЧАНИЮ

Изучив уязвимые места стандарта 802.11b, вы, должно быть, подумали, что дела законного пользователя в плане безопасности «хуже некуда» или «куда уж лучше» для шпиона. Всякий, кто когда-либо сталкивался с вопросами безопасности, знает о постоянной необходимости поиска компромисса между безопасностью системы и удобством ее использования. Такая необходимость выбора справедлива и для беспроводных технологий. Производители настраивают сетевые интерфейсные карты и базовые станции таким образом, чтобы обеспечить максимальную скорость и простоту установки. К сожалению, эта простота идет вразрез с требованиями безопасности.

«Искатели сетей» (о которых мы поговорим в следующем разделе) сообщают, что от 50 до 80% базовых станций содержат настройки SSID по умолчанию, и возможность шифрования с помощью WEP-ключей в них отключена. Пользователи и администраторы любят простоту – включил устройство и работай, и производители, идя навстречу пожеланиям трудящихся, стараются продавать как можно более простое в использовании оборудование. Итак, в целях шпионажа вы можете использовать следующие уязвимые места подобного оборудования:

- **WEP-ключи по умолчанию отключены.** Последствия очевидны. Шпион при помощи программы перехвата сетевых пакетов сможет просматривать всю передаваемую по сети информацию.
- **Применение WEP-ключей, задаваемых по умолчанию.** Даже если служба шифрования при помощи WEP-ключей включена, некоторые поставщики оборудования задают значения ключей

по умолчанию, которые могут быть оставлены без изменений неграмотными либо просто ленивыми пользователями. Эти ключи известны, поэтому, если шпиону удастся подключиться к сети, в которой базовая станция и сетевые интерфейсные карты идентифицируются по своему MAC-адресу, и в сети используется SSID по умолчанию, он может попробовать расшифровать передаваемые данные с помощью одного из известных WEP-ключей.

- **Слабые места в защите удаленного администрирования.** Как правило, базовые станции поддерживают функцию удаленного администрирования, позволяющую сетевому администратору изменять соответствующие настройки. При этом для работы используются протоколы SNMP (Simple Network Management Protocol), Telnet и HTTP. Общая проблема этих протоколов состоит в том, что по сети отправляется незашифрованная информация. Любое лицо, занимающееся в этот момент времени мониторингом сети, может без проблем перехватить, к примеру, пароль, вводимый администратором для доступа к управляющему ПО. Но это еще не самое худшее, ведь в некоторых случаях подключиться к базовой станции для изменения настроек вообще бывает смехотворно легко. Подключившись к беспроводной сети и зная IP-адрес базовой станции (его достаточно просто выяснить при мониторинге сетевого трафика), вы можете задать в браузере этот IP-адрес и запустить менеджер настроек. Пароли менеджера по умолчанию хорошо известны, поэтому, если их никто не догадался сменить, вы сможете получить доступ к любым настройкам базовой станции.



Более подробно о программах перехвата сетевых пакетов (сетевых мониторах) речь шла в главе 9.

Несмотря на то что вопрос безопасности беспроводных технологий активно муссируется в популярной и специализированной прессе в течение последних нескольких лет, пользователи и администраторы продолжают использовать настройки по умолчанию. Такое всеобщее невежество и игнорирование опасности быть подслушанным только облегчает задачи сегодняшних шпионов.

## Средства шпионажа для беспроводных сетей

Определив главные уязвимые места в системе защиты беспроводных сетей стандарта 802.11b, далее мы займемся изучением инструментальных средств, пригодных для использования этих уязвимых мест. Для получения доступа к беспроводным сетям можно использовать множество разнообразных программных средств в сочетании с недорогим аппаратным обеспечением. Многие средства и методики беспроводного шпионажа выросли на

основе целой субкультуры Интернета, называемой *war driving* (воинственная езда). Для того чтобы полностью представить себе всю картину, необходимо поговорить о том, как происходила разработка этих инструментальных средств, и немного изучить людей, которые занимались их разработкой.

## WAR DRIVING

В терминах компьютерной безопасности выражение «*war driving*» означает мобильный мониторинг беспроводных сетей\*. Проще говоря, это подразумевает езду в машине (с чем в первую очередь и связан термин «*driving*» – вождение автомобиля) со своим мобильным компьютером, имеющим встроенную сетевую интерфейсную карту, в поисках беспроводных сетей, к которым можно было бы подключиться. (Ваш фургон идеально подходит для ведения шпионской деятельности, когда вы не заняты вашей основной работой по очистке помещений от «жучков». Ирония состоит в том, что для тестирования безопасности беспроводных сетей вы используете те же самые методы, что и шпионы для проникновения в защищенные сети.)

### Тактика: а я тебя вижу

Стандарт 802.11b применяется не только для подключения к сети Интернет и беспроводного доступа в локальных сетях. Он приобретает популярность в беспроводных видеокамерах наблюдения, в результате чего шпионы получают возможность использовать старые уязвимые места по-новому.

В августе 2002 года увидел свет отчет Агентства по оборонным информационным системам (DISA). Агентство, базирующееся в Арлингтоне, штат Виргиния, отвечает за безопасность сетей Министерства обороны, а также их командных и управляющих систем. Консультант агентства, воспользовавшись NetStumbler, выяснил, что охранные камеры в штаб-квартире агентства являлись частью сети 802.11b. NetStumbler показал, что шифрование при помощи ключей WEP в данной сети не было включено, а SSID базовой станции имел вид «AP-BLDG 12», что в точности соответствовало ее физическому местоположению, поскольку снаружи на здании имелась бирка BLDG 12. Таким образом, при желании шпион мог легко осуществить перехват видеосигнала (зная источник передачи благодаря идентификатору SSID), а приложив некоторые усилия, даже фальсифицировать видеосигнал, передаваемый на экраны мониторов в охранный офис. А это довольно шокирующая ситуация, учитывая то, о каком министерстве идет речь, и тот факт, что это происходило уже после событий 11 сентября.

\* Мы же будем называть специалистов в этой области «искателями сетей», по аналогии с «искателями приключений». – *Прим. перев.*

Даже детские игрушки могут послужить целям шпионажа. Высокоинтеллектуальная собачка-робот AIBO, выпущенная компанией Sony, имеет встроенный приемопередатчик стандарта 802.11b, позволяющий управлять собачкой с ноутбука или настольного ПК. При помощи программного обеспечения AIBO Navigator робот может передавать изображение и звук обратно на управляющий ПК. Возможности наблюдения, предоставляемые этой игрушкой, практически неограничены. Вы можете дать ее похитить, чтобы, попав в другое помещение, собачка-робот могла перемещаться по комнатам и собирать любопытную информацию. Если, воспользовавшись программой NetStumbler, вы обнаружите рядом сеть 802.11b с SSID «AIBO-NET», значит, где-то рядом находится беспроводная собачка. Используемый для нее по умолчанию WEP-ключ имеет вид AIBO2.

Еще одним весьма популярным продуктом является отлично подходящая для выполнения шпионских задач беспроводная видеокамера X-10. С некоторых пор всплывающие банеры с рекламой миниатюрной, размером с мячик для гольфа, камеры X-10 можно встретить практически на каждом сайте. Камера использует диапазон 2,4 ГГц, передавая информацию на удаленный приемник, картинка с которого может поступать на экран телевизора, видеомагнитофон или компьютер. Радиус действия передатчика составляет 30 метров. Одна маленькая деталь, о которой не упоминается в рекламе, связана с тем, что в этой камере не предусмотрена защита от перехвата информации. Поэтому любители совать свой нос в чужие дела могут разъезжать по городу, подключаясь к подобным камерам и просматривая видео из душевых, с детских площадок либо из охранных систем. Сигнал от большинства других беспроводных камер, работающих на частоте около 900 МГц, также может быть перехвачен при помощи специальных радиосканеров. Сканер R-3 производства компании Icom может перехватывать не только аудио-, но и видеосигнал. И хотя у него ограничены время автономной работы и радиус действия, его вполне можно рассматривать в качестве претендента на роль наблюдательного устройства в беспроводных системах наблюдения.

Американский термин *war driving* является адаптацией обозначения популярной среди хакеров в 80-х годах прошлого века практики *war dialing*. До того, как появилась возможность идентифицировать потенциальные целевые компьютеры при помощи сканирования портов Интернета, взломщики использовали модемы и специальные программы, такие как TCH-Scan или ToneLoc, для подключения к компьютерам по ту сторону телефонного провода. При помощи этих программ они называли по разным телефонным номерам, дожидаясь ответа от модема. Добившись ответа, означающего, что к данной телефонной линии подключен компь-

ютер, программа записывала номер телефона, который в дальнейшем использовался взломщиками для подключения к этой системе.

Осенью 2000 года консультант по компьютерной безопасности в Калифорнии Пит Шипли, взяв с собой ноутбук, оборудованный беспроводной сетевой картой, базовое программное обеспечение для обнаружения беспроводных сетей и устройство GPS, начал колесить по улицам в районе Залива. За 18 месяцев Шипли обнаружил более 9 тысяч базовых станций. 85% сетей оказались уязвимы к атакам взломщиков, поскольку в них даже не было включено WEP-шифрование. Шипли опубликовал результаты своего исследования, впервые употребив термин *war driving* при описании своих занятий поиском беспроводных сетей. Этот термин был подхвачен средствами массовой информации и рядом компьютерных сообществ.

К 2001 году популярность подобного рода занятий возросла не в последнюю очередь благодаря появлению утилиты для обнаружения беспроводных сетей под Windows – NetStumbler. Воспользовавшись данной утилитой и подключив сетевую интерфейсную карту к ноутбуку, вам останется только запустить программу и начать колесить по улицам города. Если еще и подключить к вашему ноутбуку устройство GPS, NetStumbler сможет даже записывать точное местоположение каждой обнаруженной сети.

Благодаря необычайной простоте использования программы NetStumbler, «поиск сетей» приобрел огромную популярность во всем мире. Существуют базы данных, в которых собрана информация об обнаруженных сетях, опубликованы карты с нанесенными на них точками нахождения базовых станций беспроводных сетей, проводятся активные общественные дебаты по поводу того, какое программное и аппаратное обеспечение лучше всего использовать для их обнаружения.

Характеризовать подобную деятельность можно с двух сторон. С одной стороны, многие люди рассматривают поиск беспроводных сетей как абсолютно безобидную деятельность. «Искатели сетей» не пытаются взломать их – поиск сетей представляет для них спортивный интерес. Большинство людей воспринимает это занятие как увлекательное хобби, охоту за электронными сокровищами, похваляясь количеством обнаруженных сетей. Тем не менее у каждой медали есть оборотная сторона. Обнаружив беспроводную сеть, к тому же не защищенную при помощи WEP-ключей, трудно устоять, чтобы не сорвать этот легкодоступный запретный плод. Как будто какой-то тихий голосок внутри вас говорит: «Только одним глазком взгляну, что это за сеть, и, может быть, ненадолго воспользуюсь бесплатным подключением к Интернету. Никто ведь не узнает». Но с этого момента вы преступаете границу Закона и превращаетесь в компьютерного преступника.

## Разоблачения: империя наносит ответный удар

До июля 2002 года, когда некий Стефан Пуффер был обвинен федеральным жюри присяжных по двум статьям Закона о мошенничестве, к действиям «искателей сетей» практически не применялись какие-либо законные меры пресечения. Именно Пуффер, 33-летний консультант по безопасности из Хьюстона, штат Техас, стал первой показательной жертвой. 18 марта 2002 года он продемонстрировал главе IT-отдела компании Harris County и репортеру газеты *Houston Chronicle* незащищенность беспроводной сети в офисе окружных секретарей компании County. Ранее он уже занимался поиском беспроводных сетей и, обнаружив сеть компании County, решил действовать как порядочный гражданин (когда-то Пуффер работал в этой компании).

Компания заявила, что действия Пуффера вынудили ее остановить работу беспроводной сети, что привело к ущербу в размере минимум 5000 долларов (обычная сумма для федерального обвинения) и вызвало необходимость расследования со стороны ФБР. Любопытно, что компания заявила о том, что никакой информации украдено не было, и поэтому не понятно, почему, вместо принятия должных мер безопасности, сеть была отключена. В сентябре 2002 года компания County пристановила проведение собственного расследования, отказавшись представить прессе окончательный отчет и обвинения.

В феврале 2003 года после 15-минутного совещания жюри присяжных пришло к выводу, что Пуффер не собирался нанести ущерб компании, и оправдало его. В случае признания его виновным Пуфферу грозило до пяти лет тюремного заключения и штраф в размере 250 000 долларов по каждому из пунктов обвинения.

Скорее всего, данное слушание должно было явиться предупреждением со стороны Министерства юстиции о начале решительных действий против «искателей сетей». Так что, шпионы и взломщики беспроводных сетей, вы должны об этом задуматься.

«Как же все эти события связаны со шпионажем?» – спросите вы. Непосредственно. «Искатели сетей» заложили фундамент для работы шпионов в беспроводных сетях. И теперь в распоряжении злоумышленника есть инструменты, технологии и даже группы неформальной поддержки, заинтересованные в наблюдении за беспроводными сетями.

## АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

В отличие от других форм высокотехнологичного шпионажа, обнаружение и подключение к беспроводным сетям не требует наличия сложного и дорогостоящего оборудования. Скорее всего, вы уже располагаете базовым набором аппаратных компонентов и легко можете приобрести оставшееся оборудование всего за пару сотен долларов.

**НОУТБУКИ.** Хотя подключиться к беспроводной сети можно и при помощи настольного ПК, ноутбуки в этом плане несколько удобнее. Для поисков сети вам нужно только положить соответствующим образом оснащенный ноутбук на пассажирское сиденье, пол машины или спрятать его в рюкзак – и вы можете отправляться в путь.

К тому же необязательно иметь навороченную суперсовременную систему. Даже видающий виды ноутбук, при условии достаточного количества оперативной памяти и процессорной мощности для работы Windows 98 или Linux, ничем не хуже в этом плане, чем новейший Pentium IV. Единственное требование к такому ноутбуку – наличие свободного слота PC Card и параллельного порта, если вы хотите использовать GPS для записи местоположения сети.

Еще одним важным требованием к ноутбуку является читабельность экрана. При ярком солнечном свете разобрать, что написано на экране ноутбука, бывает довольно затруднительно, поэтому вам необходим дисплей с такими характеристиками, которые бы подошли для работы вне помещения. Кроме того, можно повысить читабельность экрана за счет изменения цветовой гаммы в операционной системе, выбрав, к примеру, легкую для восприятия монохромную цветовую схему.

Разумеется, предпочтительнее использовать ноутбуки малых размеров (субноутбуки, занимающие промежуточное положение между ноутбуками и КПК). Они более универсальны: их можно использовать в машине, положить, к примеру, в рюкзак либо сумку для более близкого мониторинга – для этого достаточно включить такой ноутбук и запустить ПО для сканирования, пока вы прогуливаетесь.

Поскольку время автономной работы ноутбуков ограничено емкостью батарей\*, то при планировании достаточно длительного рейда вам следует позаботиться о дополнительных батареях либо внешних источниках питания, которые можно подключить к гнезду зажигалки в вашем авто.

**КПК.** В плане незаметности беспроводного шпионажа карманные ПК дадут фору любым другим мобильным компьютерам. Идеальным решением можно считать КПК iPAQ производства компании Compaq, благодаря их малому размеру, совместимости с беспроводными разновидностями сетевых карт и наличию встроенного GPS, а также возможности запуска популярных утилит поиска беспроводных сетей под Linux и Windows.

---

\* Правда, если раньше они могли работать 2...4 часа, то сейчас некоторые модели позволяют работать без подзарядки до 10 часов. – Прим. перев.

КПК iPAQ отлично подходят для скрытого обнаружения беспроводных сетей изнутри и снаружи зданий. Такой пеший поиск сетей называется *war chalking*, в отличие от разведки на автомобиле, именуемой *war driving*. Существуют даже программы перехвата сетевых пакетов, специально предназначенные для КПК, с помощью которых вы можете осуществлять мониторинг найденных сетей.



Более подробно о термине «*war chalking*» и других названиях вы можете прочесть на сайте [www.warchalking.org](http://www.warchalking.org).

**СЕТЕВЫЕ КАРТЫ.** Чтобы подключиться к беспроводной сети, вам необходимо экипировать ваш ноутбук беспроводной сетевой интерфейсной картой. Такая сетевая карта вставляется в свободный разъем PC Card и оснащена антенной, торчащей примерно на дюйм наружу (некоторые модели, например OfficeConnect от компании 3Com, комплектуются выдвижной антенной). С ростом популярности 802.11b сетевые интерфейсные карты для беспроводной связи резко упали в цене, и сейчас даже для карт верхнего уровня розничная цена составляет менее \$100.

Новые модели ноутбуков начинают комплектоваться встроенными сетевыми картами для беспроводной связи. И теперь, вместо того чтобы торчать из разъема PC Card, антенна встраивается в корпус самого ноутбука. Таким образом, вас, сидящего на скамейке в парке напротив интересующего вас офиса с ноутбуком на коленях, никто не заподозрит в шпионской деятельности.

Наибольшее распространение получили микросхемы для устройств беспроводной связи стандарта 802.11b трех основных производителей: Hermes, Prism-2 и Aironet.

- Карты на микросхемах Hermes выпускаются под торговыми марками Lucent, WaveLAN, ORiNOCO (см. следующую врезку), Avaya, RoamAbout BuffaloTechnology. У них лучше характеристики приема, чем у карт на микросхемах Prism, и имеется возможность подключения внешней антенны.
- Сетевые карты Prism выпускаются компаниями SMC, D-Link, Linksys, Microsoft и некоторыми другими производителями. Эти карты занимают наибольшую долю рынка благодаря своей дешевизне, хотя и обладают меньшим радиусом действия, чем карты Hermes. Их основное преимущество – возможность работы в смешанном режиме для перехвата необработанных пакетов 802.11b, а также наличие большого количества специально написанного программного обеспечения для их поддержки.
- Карты Aironet отличает современность и высокая производительность. Сетевые интерфейсные карты на микросхемах Aironet выпускаются компанией Cisco. Они менее распространены, чем, например, карты на микросхемах Hermes или Prism-2, и для них написано меньше утилит.

## Тактика: War Chalking

Использование КПК или небольших ноутбуков для ведения пешей разведки сетей дало толчок развитию нового вида развлекательной деятельности под названием *war chalking*. Во времена Великой депрессии бродяги применяли свою систему символов, чтобы охарактеризовать местные условия. Определенный символ, начертанный на заборе, означал, что в этом доме живут добрые люди, готовые поделиться пищей, или, наоборот, здесь следует осторегаться злой собаки. Летом 2002 года веб-дизайнер Мэт Джонс привнес новую жизнь в идею бродяжьей символики, назвав ее «*war chalking*». Джон опубликовал серию стандартизованных символов, связанных с беспроводными сетями, которые могли бы наноситься на стены зданий либо тротуары в местах, где были обнаружены беспроводные сети (рис. 11.1). Таким образом, увидев определенный знак возле офисного здания, «искатель сети», несущий ноутбук с картой беспроводной связи, знал бы, к примеру, о наличии рядом бесплатного подключения к Интернету. Некоторые консультанты по безопасности отнеслись к этим символам скорее как к юмористической пародии. Тем не менее ФБР восприняло это достаточно серьезно и посоветовало деловым людям обращать внимание на странные знаки, начертанные поблизости от их офиса.

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth

blackbeltjones.com/warchalking

**Рис. 11.1.** Шпионская символика для обозначения состояния беспроводной сети. Идентификатор SSID и значение полосы пропускания bandwidth обычно наносятся рядом с символом. В области контактов access contact указывается такая информация, как адрес электронной почты или номер телефона для получения доступа к беспроводным сетям, защищенным при помощи WEP-ключей.

Поскольку вы сообразительный малый, вы не станете делиться информацией о вашей жертве с другими конкурентами, но, зная смысл тех или иных символов, вы облегчите себе работу, если столкнетесь с ними.

Для каждого типа сетевой карты характерны свои приемы программирования, поэтому программные утилиты, написанные под одну карту, не будут работать для другой. В качестве классического примера можно привести утилиту NetStumbler, разработанную для работы с сетевыми картами Hermes, хотя ее последние версии умеют работать и с некоторыми картами Prism под Windows XP.

Беспроводные сетевые интерфейсные карты достаточно дешевы, поэтому вы вполне можете приобрести две карты (Hermes и Prism), чтобы использовать преимущества различных программных утилит. В настоящее время не существует программ для беспроводного наблюдения, предназначенных для карт на определенной микросхеме, поэтому вы можете выбирать из широкого диапазона универсальных утилит ту, которая наиболее точно соответствует вашим нуждам. Рекомендуем вам приобрести две карты: ORiNOCO Gold (Hermes) и Proxim RangeLAN-DS (Prism-2).

**АНТЕННЫ.** Все беспроводные сетевые интерфейсные карты имеют небольшие встроенные антенны, радиус действия которых достаточен для работы в условиях небольшого офиса или дома. Именно радиус действия стандартных антенн ограничивает возможности обнаружения и подключения к беспроводным сетям снаружи зданий. При использовании внешней антенны вы сможете найти большее количество сетей, находясь при этом достаточно далеко для того, чтобы остаться незамеченным.

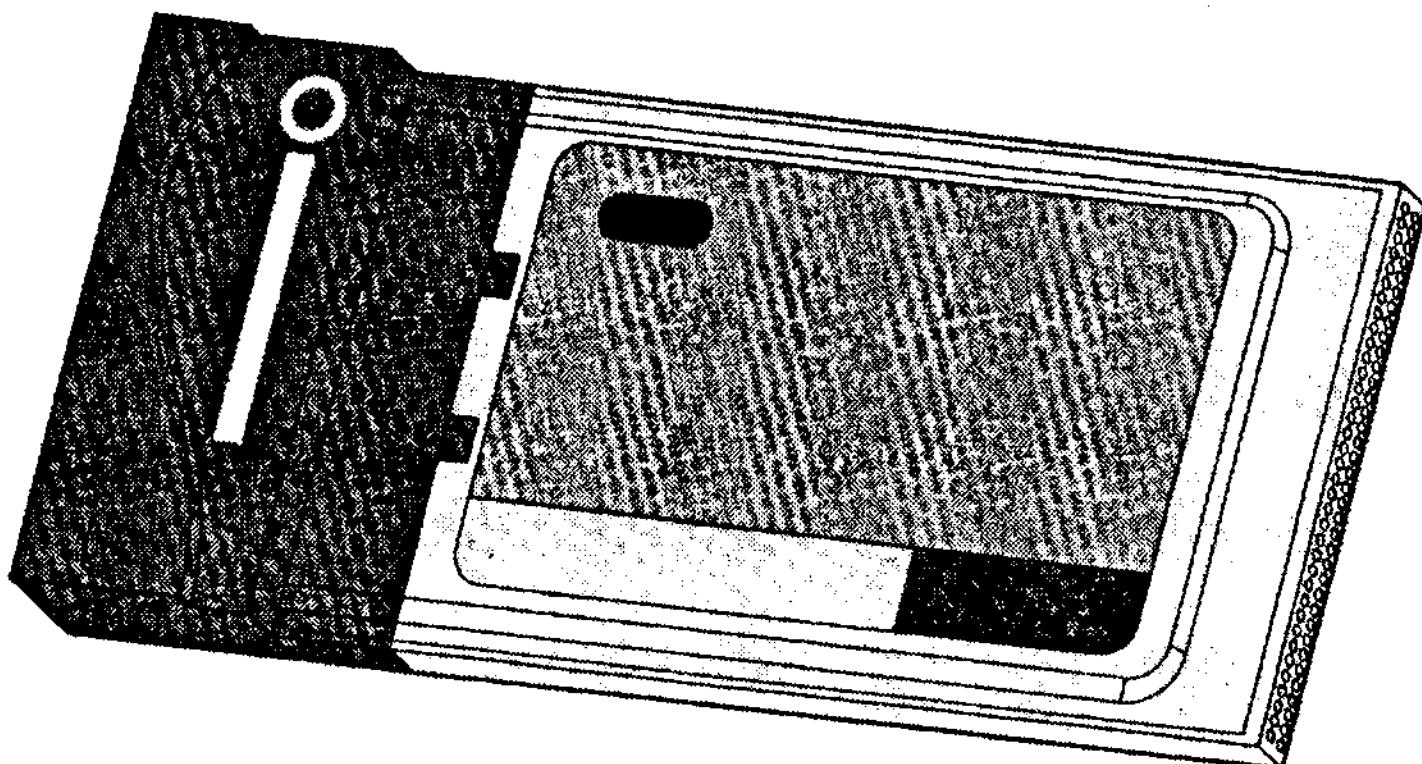
Для мобильного мониторинга обязательно необходимо выбирать сетевые карты, поддерживающие работу с внешней антенной. Такие карты не всегда легко найти, и, хотя существуют схемы переделки карт для подключения внешней антенны, гораздо проще и надежнее приобрести уже готовое оборудование. Обе рекомендуемых нами карты – ORiNOCO Gold и Proxim RangeLAN-DS имеют разъемы для подключения внешней антенны. Многие антенны промышленного изготовления имеют штепсельный разъем N-типа (большой металлический разъем с резьбовым фиксатором и накидной гайкой, используемый в любительской и промышленной радиоаппаратуре). Поэтому для подключения антенного кабеля к сетевой карте вам понадобится переходник, только постарайтесь осторожно обращаться с такими переходниками (не скручивайте и не перегибайте их).

«Искатели сетей» изначально применяли небольшие антенны, специально предназначенные для увеличения радиуса действия беспроводных сетей. С ростом популярности этого вида деятельности появилась возможность выбора из еще более незаметных устройств.

Внешняя антенна должна быть предназначена для работы с частотами 2,4 ГГц. Не всякая (особенно старая) антенна способна работать в этом диапазоне. К примеру, для этих целей не подойдет обычная телевизионная антенна, поскольку она оптимизирована для приема сигнала в диапазоне от 50 до 220 МГц.

## Шпионский инструментарий: сканер для сетей

Посетив ряд сайтов, посвященных вопросу «поиска сетей», и почитав тематические форумы, вы обязательно услышите о такой сетевой карте, как ORiNOCO Gold (рис. 11.2). Выпущенная компанией ORiNOCO Wireless, которая была приобретена корпорацией Proxim в августе 2002 года, эта беспроводная сетевая карта, спроектированная компанией Lucent, постоянно получает наивысшие оценки за производительность. В ней даже предусмотрен разъем для подключения внешней антенны, позволяющей значительно расширить радиус действия карты.



**Рис. 11.2.** Беспроводная сетевая карта ORiNOCO Gold.  
Антенна размещена слева

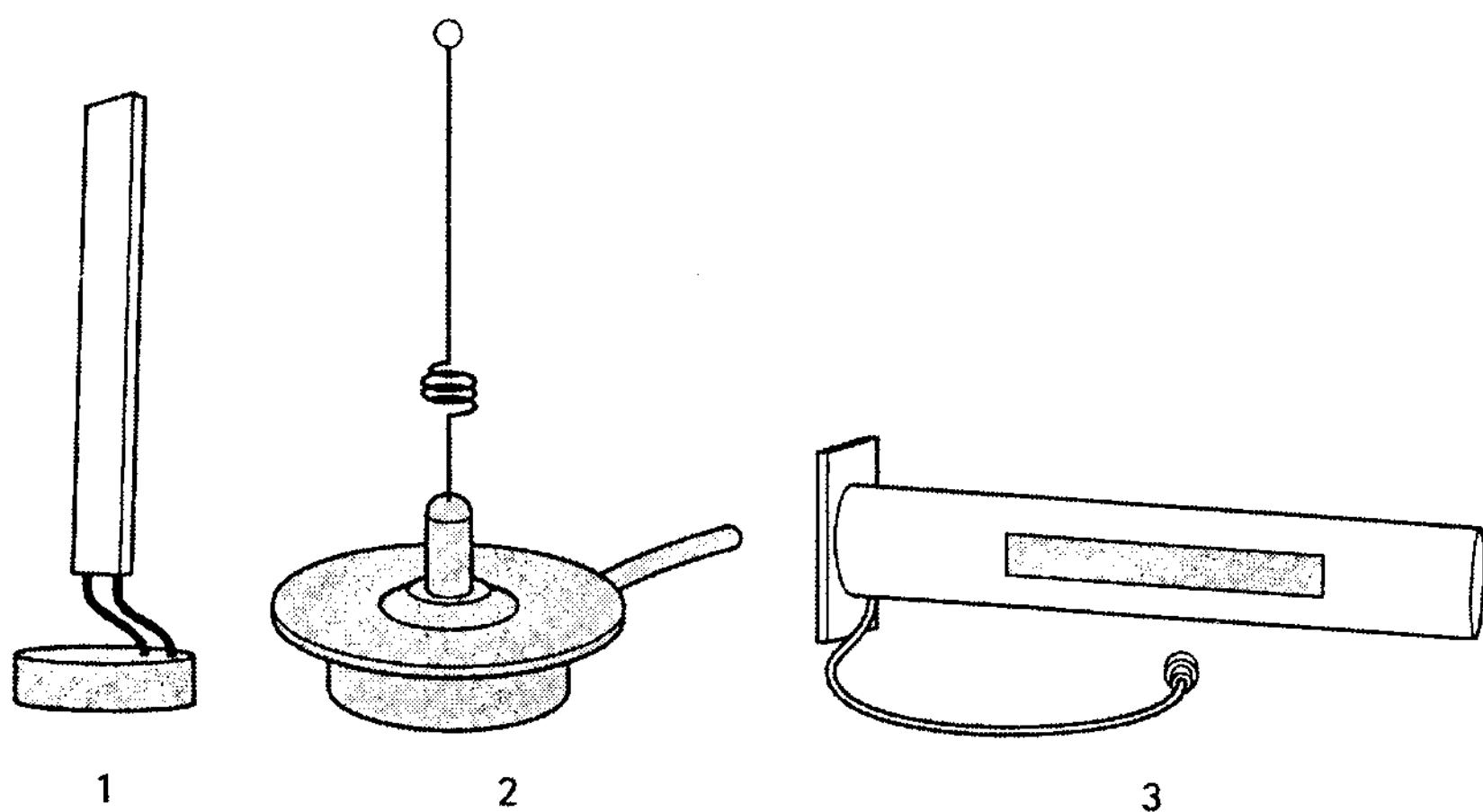
Приложение Client Manager, поставляемое в комплекте с сетевой интерфейсной картой, позволяет выполнять сканирование беспроводных сетей. Чтобы начать поиск, необходимо:

- 1.** Запустить приложение Client Manager.
- 2.** Выбрать в меню Actions пункт Add/Edit Configuration Profile.
- 3.** Создать профиль со значением SSID «ANY» или пустым. В этом случае будет осуществляться сканирование всех близлежащих беспроводных сетей.
- 4.** Указать использование созданного профиля настроек в качестве текущего.
- 5.** Из меню Advanced выбрать пункт Site Monitor.

Хотя программа Client Manager и не предоставляет таких подробных сведений как, например, NetStumbler, она может послужить целям общей разведки.

Изучая спецификацию антенны, обратите внимание на параметр в единицах dB<sub>i</sub>, связанный с коэффициентом усиления антенны и характеризующий ее чувствительность. Чем выше коэффициент усиления, тем более слабый сигнал сможет принять антenna. Небольшие антенны обычно имеют значение этого параметра около 5 dB<sub>i</sub>, тогда как антенны большего размера могут иметь значение более 10 dB<sub>i</sub>.

Не все антенны, предназначенные для приема (и передачи) сигнала в диапазоне 2,4 ГГц, работают одинаково. Существует две разновидности антенн: всенаправленные и узконаправленные, у каждой из которых своя область применения (см. рис. 11.3).



**Рис. 11.3.** Три антенны, работающие в диапазоне 2,4 ГГц, слева направо (масштаб не соблюден): (1) расширитель радиуса действия антенны, популярный на заре «war driving»; (2) всенаправленная антenna с магнитной подставкой, часто используемая для поиска сетей; (3) закрытая узконаправленная антenna Yagi, пригодная для поиска беспроводных сетей на достаточном расстоянии

- **Всенаправленные антенны.** Всенаправленные антенны, как следует из названия, могут принимать и передавать сигнал во всех направлениях. Такие антенны идеально подходят для поиска беспроводных сетей. Некоторые модели комплектуются магнитной подставкой для упрощения монтажа на крыше автомобиля, например. Стоимость всенаправленных антенн для беспроводного шпионажа варьируется в пределах от 50 до 150 долларов.
- **Узконаправленные антенны.** Узконаправленные антенны проектируются таким образом, чтобы передавать или принимать усиленный сигнал в одном направлении, ослабляя сигнал, пришедший из других мест. Такие антенны лучше всего подходят

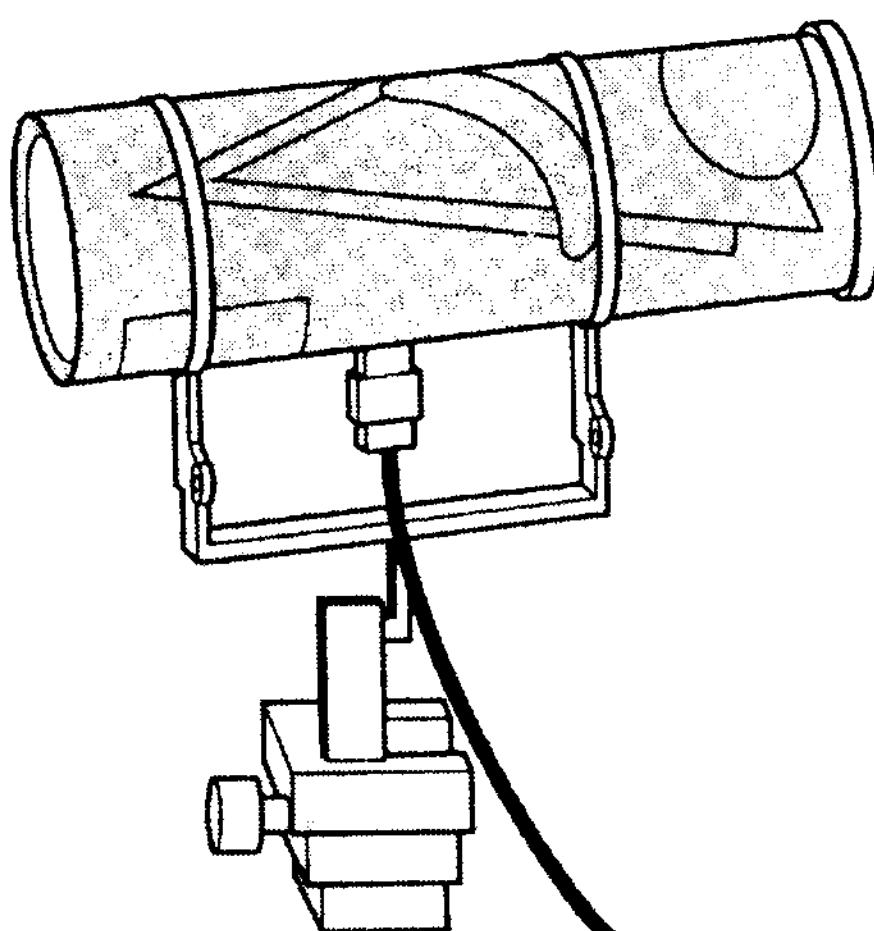
для целенаправленной работы с найденной беспроводной сетью. Находясь вдалеке, вы можете направить антенну на здание для удаленного наблюдения за сетью либо, находясь ближе, принимать из глубины здания слабый сигнал, который не смогла бы воспринять всенаправленная антенна. Можно позиционировать антенну вручную, сидя в машине, но желательно для этих целей использовать треножник (например, применяемый при видеосъемке), чтобы зафиксировать положение антенны. Направленную антенну можно приобрести по цене всего \$200.

Вам наверняка приходилось видеть телевизионные новости, в которых «искатели сетей» с ноутбуками весьма интересным образом использовали картонные упаковки, например из-под чипсов Pringles. «Упаковки от чипсов Pringles?» – спросите вы.

Если вы ограничены скромным бюджетом, можете попробовать заняться поиском в сети Интернет инструкций по созданию узконаправленных 2,4-ГГц антенн из самых обычных материалов, которые можно найти на кухне любой домохозяйки, таких как упаковки или банки из-под кофе, соусов, чипсов Pringles и т. д. (рис. 11.4). Всего за \$5 (не считая стоимости содержимого упаковки) из подручных материалов можно создать антенну, превосходящую по своим показателям промышленные аналоги. Подобные антенны идеально подходят для социально-грамотных шпионов, верящих в утилизацию отходов.



Описание антенн, которые можно собрать в домашних условиях, размещено на веб-сайте [www.turnpoint.net/wireless/has.html](http://www.turnpoint.net/wireless/has.html).



**Рис. 11.4.** Замаскированная узконаправленная антенна, корпусом для которой послужила упаковка от чипсов Pringles

Изготовить самодельную антенну можно достаточно просто и быстро, причем для этого не требуются особые технические познания. Всенаправленные антенны, напротив, требуют значительно больших навыков и затрат труда. Если только вы не занимались в прошлом радиолюбительством, советуем вам сразу приобретать всенаправленную антенну промышленного производства.

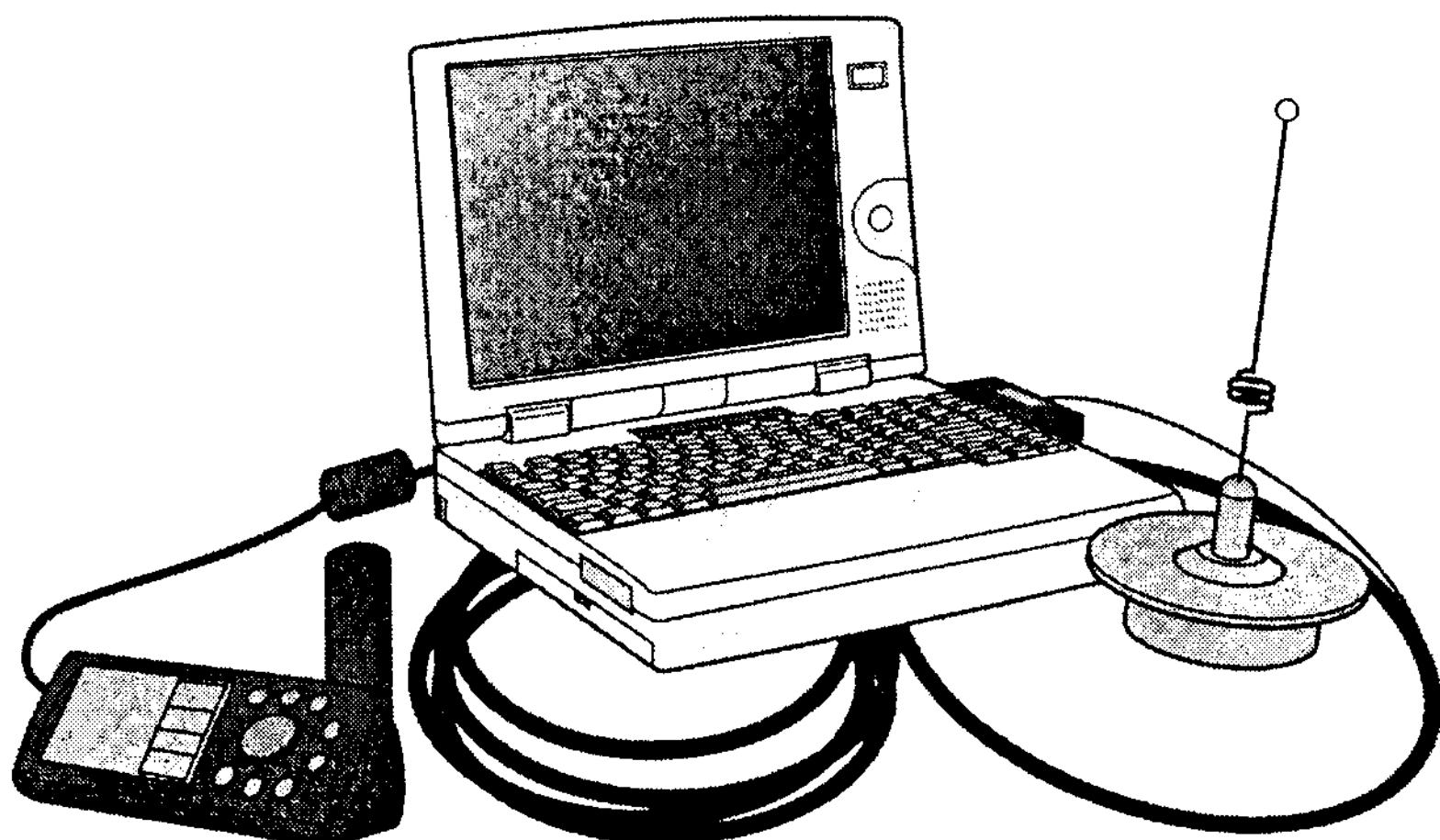
**МОНТАЖ АНТЕННЫ.** Раздобыв антенну, ее необходимо соответствующим образом установить. Если вы намерены использовать ее на транспортном средстве, вам надо обойти проблему экранирования радиоволн корпусом автомобиля и влияния электромагнитных помех. С другой стороны, антenna не должна быть жестко зафиксирована на случай, если понадобится быстро избавиться от нее, как от улики. «Искатели сетей» обычно используют антенны с магнитным креплением, протягивая шнур через открытое окно либо вентиляционные отверстия в крыше машины. Возможно также выведение кабеля через заднюю дверь машины или багажное отделение, что продлит срок службы кабеля благодаря большему размеру щели для его прокладки. Только будьте осторожны, чтобы не защемить антенный кабель дверью либо окном. Повреждение кабеля может ухудшить передачу сигнала, сведя на нет все преимущества от использования внешней антенны.

**УСТРОЙСТВА ГЛОБАЛЬНОГО ПОЗИЦИОНИРОВАНИЯ (GPS).** Программа NetStumbler и другие утилиты, предназначенные для обнаружения беспроводных сетей, могут взаимодействовать с устройствами глобального позиционирования (GPS). Устройство GPS обычно выглядит как небольшой приборчик с дисплеем, отображающим широту и долготу вашего местоположения. Для взаимодействия с компьютером и другими устройствами (см. рис. 11.5) в GPS используется протокол передачи строк ASCII NMEA 0183. В первую очередь устройства глобального позиционирования получили распространение в морской навигации, и Национальная ассоциация морской электроники разработала стандарты для работы с автопилотами и другим навигационным оборудованием.

При помощи собственного кабеля (тип которого может зависеть от производителя) GPS подключается к последовательному порту ноутбука. Поскольку USB медленно вытесняет устройства, подключаемые к последовательным портам, некоторые из новейших ноутбуков не имеют последовательного порта. Производители GPS также переходят на выпуск приборов, подключаемых через USB-интерфейс, поэтому, если в вашем ноутбуке отсутствует разъем для подключения СОМ-устройств, вам понадобится специальный переходник от USB к последовательному порту.

Итак, имея в наличии модуль GPS, подключенный к вашему мобильному компьютеру, а также утилиту NetStumbler (или другую подобную программу), вы сможете записывать точные координаты обнаруженных вами беспроводных сетей. Эта информация впоследствии может быть экспортирована на электронную карту, на которой вы визуально увидите местоположение различных сетей. В зависимости от того, используется или нет в

обнаруженной сети шифрование при помощи WEP-ключей, сеть будет обозначаться на карте различными значками, что позволит упростить и ускорить процесс выбора потенциальных целей.



**Рис. 11.5.** Устройство GPS Garmin III+, подключенное к ноутбуку Toshiba Libretto, полностью готово к поиску беспроводных сетей

Двумя основными производителями устройств глобального позиционирования являются фирмы Garmin и Magellan. Обе компании предлагают базовые модели GPS по цене менее \$100. Особенной популярностью среди шпионов беспроводных сетей пользуется серия GPS Garmin eTrex благодаря своему малому размеру.

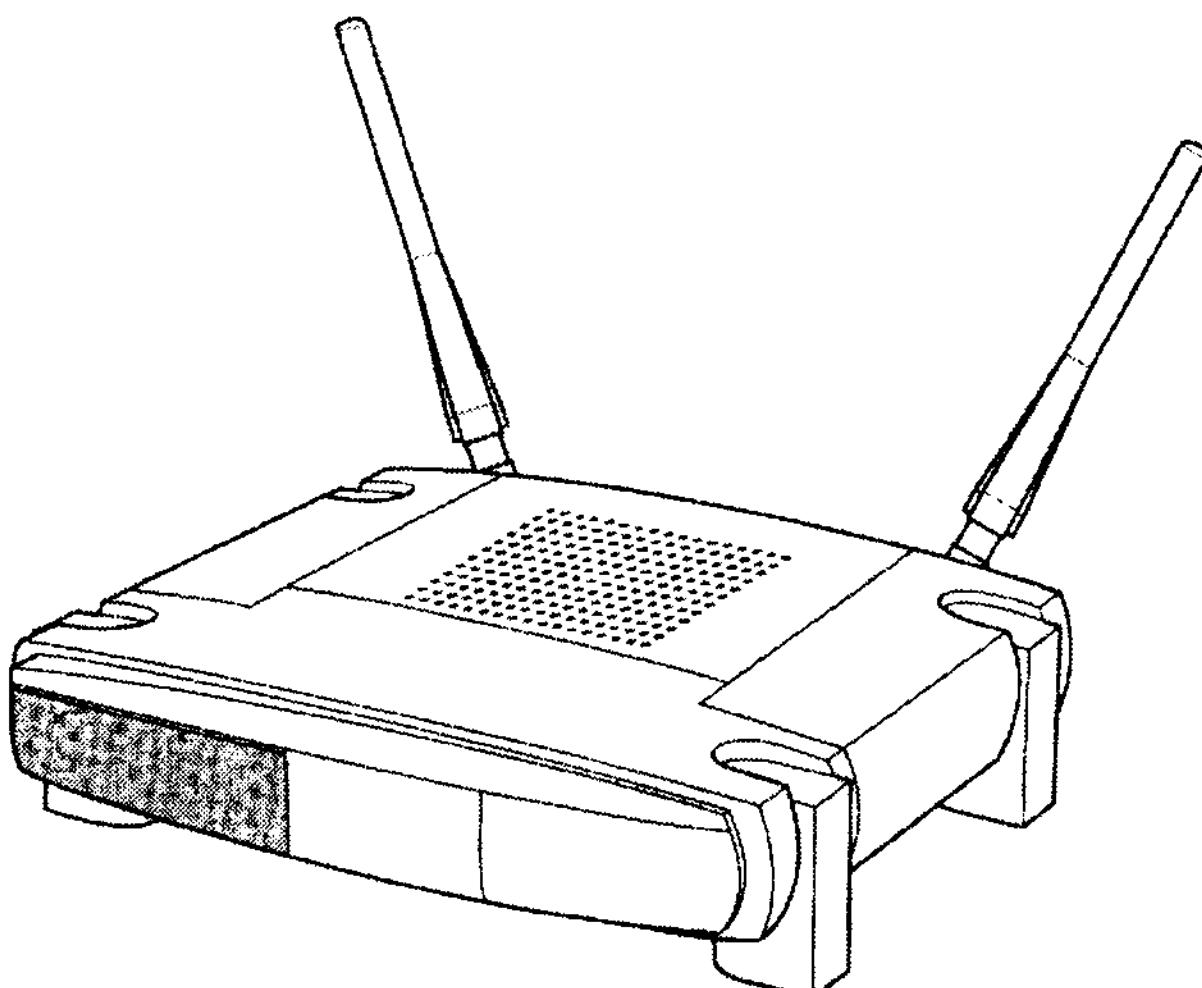
Но самым незаметным устройством GPS по праву считается прибор в виде компьютерной мыши под названием Sapphire GPS Mouse. Это устройство предназначено только для совместной работы с ноутбуком или КПК. Оно не отличается такой универсальностью, как обычный GPS, не подходит для наземной или водной навигации, поскольку не обладает дисплеем либо кнопками управления. Однако, имея размер всего 5 сантиметров, оно идеально подходит для скрытого применения.

**БАЗОВЫЕ СТАНЦИИ.** Хотя большая часть вышеперечисленных устройств неплохо подойдет для мобильного шпионажа, серьезный шпион может использовать в этих целях стандартные базовые станции для беспроводных сетей (рис. 11.6). Существует несколько вариантов реализации такого подхода.

Если вы обладаете физическим доступом к зданию, вы можете тайно установить вашу собственную базовую станцию в радиусе действия целевой сети, получив таким образом удаленный доступ к ней. К примеру, шпион может спрятать подключение передатчика базовой станции в сетевом разветвителе, размещенном рядом с окном. Затем, выйдя за пределы

здания и установив направленную антенну, начать прослушивание корпоративной сети при помощи программ перехвата сетевых пакетов.

Еще один прием, связанный с использованием базовых станций, основан на включении в состав беспроводной сети второй базовой станции с идентичными настройками для наблюдения за проходящим через нее трафиком. К примеру, шпион может установить базовую станцию между компьютером клиента и реальной базовой станцией. Поскольку фальшивая базовая станция будет находиться ближе, чем реальная, клиентский ПК будет стараться подключиться именно к ближайшей базовой станции. Шпиону понадобится прибегнуть к помощи программы перехвата сетевых пакетов для записи проходящего трафика. Еще один способ применения промежуточных базовых станций заключается в атаке типа «отказ в обслуживании», направленной против главной базовой станции, в результате чего управление беспроводной сетью перейдет к вашей базовой станции. (Сейчас на рынке начинают появляться утилиты, специально предназначенные для проведения атак типа «отказа в обслуживании» для беспроводных сетей. Например, на выставке Black Hat в Лас-Вегасе в 2002 году была представлена целая коллекция утилит под названием Air-Jack.)



**Рис. 11.6.** Базовая станция от компании Linksys, которую можно использовать параллельно с основной либо в качестве промежуточной станции для атак со второй базовой станцией

**САМОЛЕТЫ, ПОЕЗДА И АВТОМОБИЛИ.** Если только вы не передвигаетесь пешком, вам необходимо место, откуда вы будете осуществлять наблюдение. Если вы оказались задействованы в беспроводном шпионаже, вам либо придется заниматься мобильной разведкой, либо настроить фиксированную станцию для ведения наблюдения.

Мобильная разведка и есть то, что обозначают термином war driving. Вы ищете беспроводные сети. Перед вами могут стоять конкретные цели, например, выяснить, используется ли в этом здании беспроводная ЛВС, или же вы надеетесь исключительно на случай, разыскивая незащищенную беспроводную сеть для атаки.

Как и при любом виде шпионажа, ключевое качество для обозначения ваших действий – «незаметный». Оно касается вас и вашего транспортного средства, которое должно затеряться среди других автомобилей. Хотя свободолюбивый «искатель сети» ничего так не любит, как поспорить о законности сканирования беспроводных сетей с подозрительным полицейским, заставившим его выйти из машины, успех самого дела состоит именно в незаметности. Вы и ваша машина не должны привлекать нежелательного внимания.

При проведении мобильной разведки вы можете действовать как в одиночку, так и с партнером. Если вы работаете самостоятельно, поместите ноутбук на сиденье пассажира либо на пол. Полоска резины либо kleenka на сиденье позволит зафиксировать положение ноутбука. «Искатели сетей» любят оперативно следить за информацией об обнаруживаемых сетях. Но каким бы сильным ни было подобное искушение, для вас же будет лучше, если вы закроете крышку ноутбука, убедившись, что нужное программное обеспечение запущено и работает. Вы сможете просмотреть результаты разведки после окончания операции. Ваше постоянное отвлечение на дисплей во время езды может заметить простой обыватель либо подозрительный полицейский. По крайней мере, оно увеличивает ваши шансы попасть в дорожное происшествие.

Исключение составляет случай, когда у вас имеется партнер: он (или она) может постоянно следить за ноутбуком и сообщать вам текущую информацию. Если вы мужчина, возмите на заметку прием, используемый профессионалами в сфере разведки, и подберите себе партнера противоположного пола. Пара обычно привлекает меньше внимания, чем два мужчины в машине, а идеальным, не вызывающим подозрений, вариантом является использование женщины с ребенком. По ходу разведки ваш пассажир может делать заметки о возможных целевых объектах письменно либо начитывая их на диктофон.

Перед тем как отправиться на поиск сетей, потратьте некоторое время на изучение дорожных карт и проведите рекогносцировку на местности, чтобы четко представлять себе, с чем вы можете столкнуться в ходе операции. Вам не следует бесцельно слоняться вокруг да около – вы должны заранее определить маршрут поездки.

Какое время лучше всего подходит для работы «искателей сетей»? Это зависит от целевого объекта. В некоторых компаниях базовые станции могут отключаться после 17:00, делая обнаружение беспроводной сети в нерабочие часы невозможным. С другой стороны, если на целевом объекте всерьез обеспокоены вопросами безопасности, то в течение дня может осуществляться постоянный мониторинг обращений со стороны таких утилит, как NetStumbler. В то же время, так как большинство «искате-

лей сетей» любят ездить по ночам, учтите, что экран ноутбука может подсвечивать изнутри интерьер автомобиля, делая вас очень заметными в темноте.

Главное правило наблюдения в данном случае – содержать ваше транспортное средство в полном порядке (чтобы полицейский не мог придраться к перегоревшей фаре) и не нарушать правила дорожного движения. В полиции любят использовать дорожные нарушения в качестве предлога для проведения более тщательного расследования ваших подозрительных действий. Что если представитель правоохранительных органов застукает вас во время проведения разведывательного рейда? Подавляющее большинство полицейских не отличаются высоким уровнем компьютерной грамотности и, возможно, никогда даже не слышали о таком занятии, как *war driving*. Ведите себя учиво, демонстрируя свою готовность к сотрудничеству, однако не забудьте заранее продумать правдоподобное объяснение ваших действий. Поясните, что вы занимаетесь исследованием мощности радиосигнала для школьного проекта либо что работаете в качестве консультанта, что не так уж далеко от истины. Покажите ему экран компьютера, GPS и начните рассказывать о чувствительности и коэффициенте усиления антенны, о внесении помех в радиодиапазон микроволновыми печами, о соотношении сигнал/шум и других технических деталях, обычно повергающих в сон среднестатистического обывателя. Заявление о том, что вы являетесь консультантом по безопасности, действующим по заказу клиента для обнаружения беспроводных сетей, – не самый лучший ответ. Многие копы, услышав слово «безопасность», сразу навострят уши – таковы реалии нашего времени после событий 11 сентября.

Второй тип беспроводного шпионажа подразумевает использование фиксированной прослушивающей станции. Она может находиться внутри офисного комплекса, либо в качестве такой станции вы можете использовать собственный автомобиль. После обнаружения интересующей вас беспроводной ЛВС, вы можете воспользоваться программой – сетевым монитором для перехвата незашифрованных пакетов данных с целью их последующего изучения или же зашифрованных пакетов для расшифровки WEP-ключа. Используя в качестве дежурной станции машину, не сидите в ней часами, делая вид, что читаете газету, иначе, говоря шпионским языком, вас «попалят». Лучше настроить все ваше наблюдательное оборудование, припарковавшись неподалеку от нужного объекта, и на несколько часов отправиться на прогулку.

При организации дежурного поста наблюдения, который будет находиться без присмотра, необходимо учитывать следующие аспекты:

- Ваше транспортное средство не должно выделяться среди других автомобилей на парковке (это значит, что не нужно вешать на бампер наклейку *war driver*).
- Наблюдательное оборудование не должно бросаться в глаза (имеется в виду ноутбук). Это нужно не только для того, чтобы вас не заподозрили в шпионаже, но и для того, чтобы не спровоцировать

на кражу обычных воров. Можно поместить ноутбук в багажник либо вести наблюдение из микроавтобуса или фургона. Микроавтобус или автоприцеп с занавесками идеально подходят на эту роль – за занавеской может находиться направленная антенна, ориентированная на офисное здание.

- Вам нужен ноутбук с достаточно большим временем автономной работы. Для увеличения периода автономной работы вместо обычных применяемых в ноутбуке батарей можно использовать свинцовые аккумуляторы с таким же вольтажом либо подключить ноутбук к солнечным батареям.

Если дежурная станция находится слишком далеко от объекта наблюдения, то ее работе могут помешать неблагоприятные погодные условия, такие как снег, дождь или туман, которые ослабляют сигнал беспроводных сетей стандарта 802.11b. Поэтому для удаленного мониторинга беспроводных сетей лучше выбирать дни с хорошей погодой.

Не ограничивайте вашу фантазию рамками автомобилей, грузовиков и фургонов. На самом деле практически любое транспортное средство может использоваться для этих целей. Известны случаи наблюдения за беспроводными сетями с лодок (на реках, каналах и в городских портах). В Европе для этих целей применяются даже поезда и велосипеды.

Такое занятие, как war driving, встречается даже на самолетах. В августе 2002 года в сети Интернет появилась информация о двух случаях использования самолетов для обнаружения беспроводных сетей в Австралии и США. Австралийская команда сообщила об обнаружении более 95 беспроводных ЛВС в ходе проведения полетов на 500-метровой высоте над городом Перт. Американцы, в свою очередь, потратили 1,5 часа, летая над Сан-Диего на высоте от 500 до 800 метров со скоростью менее 200 км/ч, успев обнаружить за это время 437 базовых станций. Собранная ими статистика говорит сама за себя. В 60% беспроводных ЛВС SSID по умолчанию не менялся, и только в 23% случаев использовалось WEP-шифрование.

## ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Обычно для поиска электронных «жучков» используется анализатор спектра – больше вам ничего не нужно. Но как обстоят дела с беспроводными сетями? У вас имеется ноутбук со встроенной сетевой картой, антенной и GPS, однако вам необходимо программное обеспечение, чтобы связать между собой все эти устройства для поиска беспроводных сетей и их проверки на уязвимость (конечно, вы ни в коем случае не собираетесь заниматься нелегальным шпионажем). Вам повезло, что в число фанатов беспроводных технологий попал целый ряд опытных программистов, создавших богатый арсенал средств для обнаружения и наблюдения за беспроводными сетями. Существуют программы, предназначенные для работы под Windows, Linux, BSD, Mac и ОС для КПК.

В целом все программные средства можно поделить на три категории:

- **Средства обнаружения**, просто сообщающие о наличии поблизости беспроводной сети.
- **Сетевые мониторы**, предназначенные для перехвата передаваемых данных для дальнейшего изучения.
- **Навигационные средства**, отображающие местоположение локальной сети.

Некоторые из этих средств очень сложны в использовании, однако, даже если вы являетесь шпионом с ограниченными техническими навыками, вы все равно без труда отыщете программу, которая подойдет именно вам. При этом вам не обязательно иметь в своем распоряжении бюджет Управления национальной безопасности, так как большинство таких программ распространяются совершенно бесплатно.

Далее мы вкратце обсудим некоторые наиболее популярные программные утилиты. Более полный перечень существующих программ для беспроводного шпионажа размещен на официальном веб-сайте данной книги <http://www.wiley.com/legacy/combooks/mcnamara/links.html>.

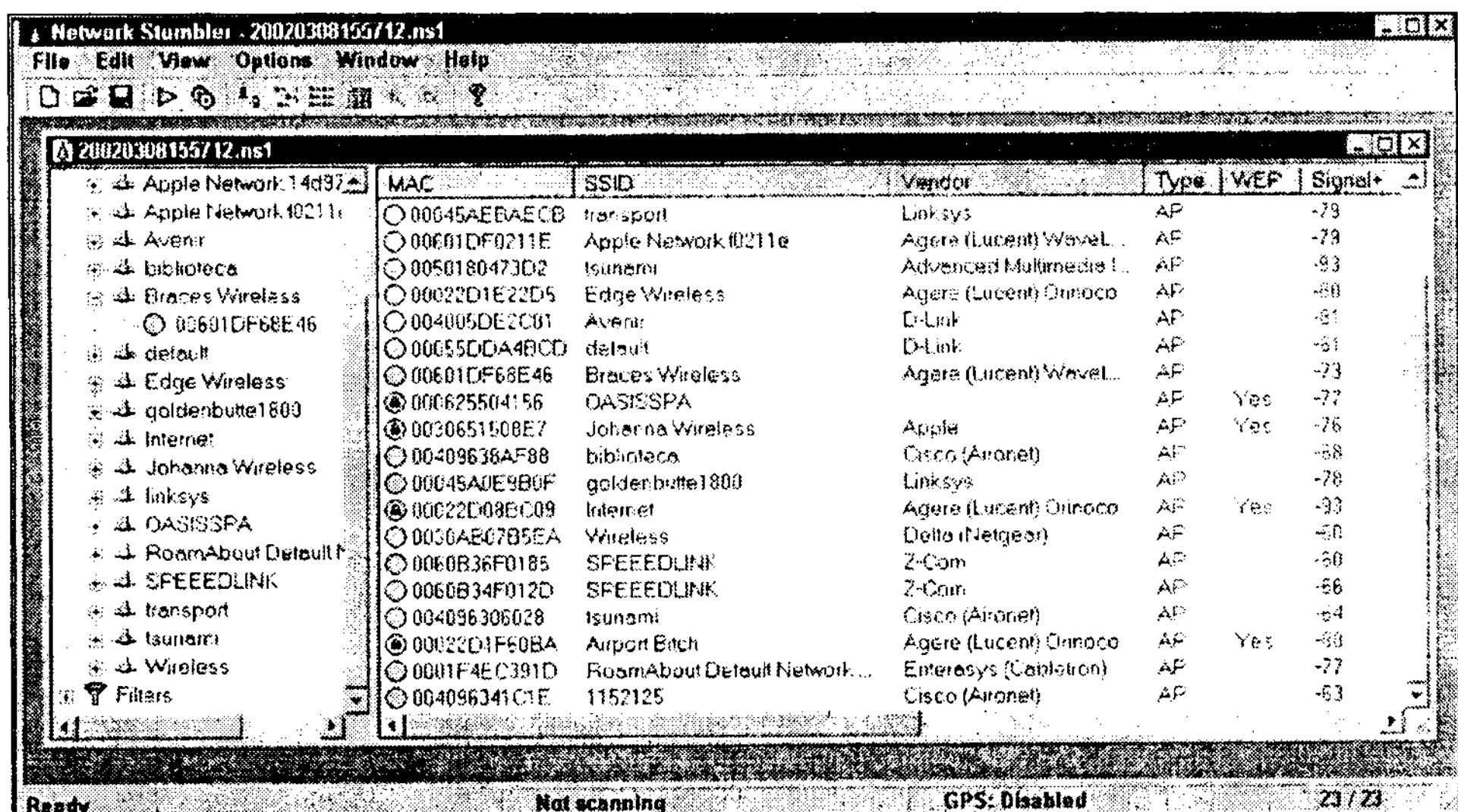
**NETSTUMBLER.** Программа Network Stumbler, чаще называемая NetStumbler (рис. 11.7), представляет собой удобную в использовании утилиту под Windows, которой не в последнюю очередь обязано своей популярностью такое занятие, как war driving. Написанная Мариусом Милнером, сотрудником компании по разработке беспроводных сетей Avaya, программа NetStumbler осуществляет поиск близлежащих базовых станций. Со временем программа NetStumbler, первый релиз которой увидел свет в мае 2001 года, превратилась в сложное с точки зрения реализации и одновременно необычайно простое в использовании средство для обнаружения беспроводных ЛВС.

NetStumbler передает пробный сигнал один раз в секунду. Не следует забывать об этом, поскольку NetStumbler выполняет активное сканирование и оставляет свою подпись в передаваемом пробном сигнале. В случае получения ответа от базовой станции, NetStumbler записывает идентификатор SSID и другую информацию. Программа NetStumbler не относится к сетевым мониторам, поскольку она не умеет сохранять и анализировать другие пакеты, передаваемые по беспроводной сети стандарта 802.11b.

При обнаружении базовой станции подается звуковой сигнал, после чего информация о ней заносится в список. Слева от MAC-адреса базовой станции и идентификатора SSID отображается небольшой кружок, цвет которого означает мощностью сигнала. Если поверх кружка изображен замок, следовательно, в данной сети включено WEP-шифрование. Если к ноутбуку подключен GPS-модуль, тогда, помимо прочего, могут записываться координаты точки, в которой была обнаружена базовая станция (но не координаты самой базовой станции, как вы могли бы подумать).

Программа NetStumbler предназначена для работы с сетевыми интерфейсными картами на микросхемах Hermes, таких как ORiNOCO, Avaya или Toshiba. В Windows XP NetStumbler может также работать с сетевыми картами Cisco или Prism-2, хотя их официальная поддержка программой отсутствует.

Помимо версии NetStumbler под Windows, Милнером была написана версия для КПК, например, Compaq iPAQ.



**Рис. 11.7.** Окно программы NetStumbler, в котором отображаются сведения об обнаруженных базовых станциях, включая мощность сигнала

Популярность программы NetStumbler привела к появлению в Интернете целой субкультуры. Вы можете найти разнообразнейшие форумы по вопросам «поиска сетей», последние версии программы, а также присланные пользователями базы данных, которые хранят данные о более чем 25 000 беспроводных сетях. Название этого программного продукта даже превратилось в синоним термина war driving, и теперь словом stumbing также обозначается поиск беспроводных сетей.



Самый последний релиз программы NetStumbler, равно как и последние обсуждения по этой теме, вы всегда можете найти на сайте [www.netstumbler.com](http://www.netstumbler.com). Кроме того, Мариус Милнер поддерживает собственный сайт по адресу [www.stumbler.net](http://www.stumbler.net).

Вообще-то, программа NetStumbler не являлась основным проектом Милнера, поэтому он уделял работе над ней только свое свободное время. Эта программа была отнесена им к категории так называемого Beggar-

Ware (попрошайничающего ПО), и он предложил тем пользователям, которым понравились результаты работы этой программы, перечислять ему деньги.

**KISMET.** Утилита Kismet для обнаружения беспроводных сетей предлагается вниманию тех, кто предпочитает работать с ОС Linux. Хотя NetStumbler пользуется большей популярностью и известностью, свободно распространяемая по принципу открытого кода утилита Kismet отличается лучшей эффективностью в плане обнаружения беспроводных ЛВС.

В отличие от программы NetStumbler, выполняющей активное сканирование, программа Kismet позволяет пассивно перехватывать передаваемые по беспроводной сети 802.11b пакеты данных и управляющую информацию. Фактически Kismet представляет собой программу перехвата сетевых пакетов. Поскольку она действует пассивно, ее невозможно обнаружить, и, в отличие от NetStumbler, эта программа может обнаруживать даже те базовые станции, в которых была отключена опция передачи SSID.

The screenshot shows the Kismet application interface. At the top, there's a terminal-like window with the command `dragom@gir.lan.nerv-un.net:/home/dragom`. Below it is a main pane titled "Networks (Autofit)". This pane contains a table with columns: Name, T, W, Ch, Packts, Flags, Info, and Elapsd. The table lists various wireless networks with their details. At the bottom of the main pane, there's a "Status" section with a list of recent network detections. The "Elapsd" column shows the time since the last detection, such as "000203".

	Name	T	W	Ch	Packts	Flags	Info	Elapsd
+	St Francis	G	N	07	324	0.0.0.0	Ntwrks	
	VBWOUND	A	Y	11	48	0.0.0.0		22
+	Centhud-POK	G	N	06	339	0.0.0.0	Packets	
	<no ssid>	A	N	01	1508	U3		6148
	cvretail	A	N	11	1091	0.0.0.0	Cryptd	
+	IBM-POK	G	Y	00	432	0.0.0.0		386
	pserwar003	A	Y	07	56	0.0.0.0		Weak
	linksys	A	Y	06	155	0.0.0.0		0
	<no ssid>	A	Y	11	175	0.0.0.0	Noise	
	tsunami3624t	A	N	06	4	0.0.0.0		0
	<no ssid>	A	Y	06	58	0.0.0.0	Discrd	
	default	A	N	11	284	0.0.0.0		1448
	arlington	A	N	06	15	0.0.0.0		
	linksys	A	Y	06	91	0.0.0.0		
	LuoHomeNet	A	Y	06	1107	0.0.0.0		
	linksys	A	N	02	107	0.0.0.0		
!	CPT_Wireless	A	N	01	170	0.0.0.0		
!	WLAN	A	N	11	22	0.0.0.0		

**Status**

- Detected new network "WavelAN Network" bssid 00:02:20:22:86:C1 WEP N Ch 10 @ 11.00 mbit
- Detected new network "WLAN" bssid 00:90:D1:00:D9:57 WEP N Ch 11 @ 11.00 mbit
- Detected new network "CPT\_Wireless" bssid 00:02:2D:0D:D4:C0 WEP N Ch 1 @ 11.00 mbit
- Detected new network "linksys" bssid 00:04:5A:D0:56:0F WEP N Ch 2 @ 11.00 mbit

**Рис. 11.8.** Окно программы Kismet со списком обнаруженных базовых станций. Kismet имеет текстовый интерфейс, поэтому выглядит не столь привлекательно, как, например, NetStumbler, что, однако, с лихвой компенсируется ее разнообразными возможностями

Программа Kismet также обладает рядом мощных и полезных функций, таких как перехват пакетов для дальнейшего анализа в Ethereal или tcpdump, запись в журнал, совместимый с форматом AirSnort, экспорт данных в навигационные системы, а также определение диапазона IP-адресов, используемых данной беспроводной сетью. Существуют даже версии Kismet для КПК iPAQ и Zaurus под управлением Linux. Изначально программа Kismet предназначалась для работы с картами Prism-2, однако сейчас можно найти «заплаты» и для работы с сетевыми картами Hermes или Aironet.



Вы можете загрузить последние версии программы Kismet, получить дополнительную информацию по ее возможностям, а также инструкции по установке на сайте [www.kismetwireless.net](http://www.kismetwireless.net).

Почему же, несмотря на свои широкие возможности, программа Kismet не приобрела такого широкого распространения, как NetStumbler? Все дело в удобстве установки и использования. Для того чтобы установить NetStumbler под Windows, требуются считанные секунды, а чтобы установить Kismet, вам потребуется вначале ее откомпилировать и связать с рядом пакетов, не все из которых входят в стандартный дистрибутив Linux. Поэтому для настройки и запуска программы Kismet необходим намного больший уровень технической грамотности.

Но, несмотря на сложность работ по установке, если вы всерьез занимаетесь беспроводным шпионажем, вам стоит потратить время на изучение программы Kismet, поскольку взамен вы получите расширенные (по сравнению с NetStumbler) возможности.

**КОММЕРЧЕСКИЕ И БЕСПЛАТНЫЕ СЕТЕВЫЕ МОНИТОРЫ.** Программы перехвата сетевых пакетов, называемые на жаргоне снiffeрами (sniffer) или сетевыми мониторами, предназначены, как следует из названия, для перехвата и записи пакетов, передаваемых по сети. Первоначально сетевые мониторы применялись администраторами и техническими специалистами для разрешения проблем в сети, поскольку с их помощью можно было проанализировать содержимое отдельных пакетов и выяснить причины того или иного отказа.

В то же время шпионы применяют программы перехвата сетевых пакетов для того, чтобы получить доступ к именам учетных записей, паролям и другой передаваемой по сети конфиденциальной информации. Сохранив определенный объем данных, вы можете заняться анализом содержимого сетевых пакетов в поисках чего-нибудь интересного.

Для эффективного использования подобных программ необходимо обладать средним уровнем техническим познаний. Они не так просты и интуитивно понятны, как NetStumbler, поэтому вам, к примеру, понадобится знание структуры пакетов в различных протоколах, чтобы суметь разобраться с их содержимым. Если вы активно занимаетесь беспроводным шпионажем, рекомендуем вам научиться обращаться с программами

перехвата сетевых пакетов, поскольку они предоставляют мощные функциональные возможности в плане кражи конфиденциальной информации.

На рынке представлен целый ряд коммерческих и бесплатных программ перехвата сетевых пакетов для беспроводных ЛВС. Вначале рассмотрим коммерческие утилиты:

- **AiroPeek NX** – это сетевой монитор под Windows от компании WildPackets, предназначенный для работы с беспроводными сетями. Программа умеет перехватывать и одновременно расшифровывать сетевые пакеты (зашифрованные при помощи WEP-ключей). Учтите при этом, что сама программа не позволяет взламывать WEP-ключи, – о корректном ключе вам придется позаботиться заблаговременно. Более подробно узнать о программе AiroPeek можно на сайте [www.wildpackets.com/products/airopeek\\_nx](http://www.wildpackets.com/products/airopeek_nx).
- **Sniffer Wireless** – это еще одна программа перехвата сетевых пакетов от компании Network Associates. Хотя она не умеет декодировать сетевые пакеты «на лету» (вам придется вначале остановить процесс перехвата), эта программа позволяет расшифровывать огромное количество сетевых протоколов. В нее также встроены функции, связанные с безопасностью сетей, например, выявление промежуточных базовых станций. Семейство продуктов Sniffer существует на рынке уже достаточное время, и эти программы часто используются в корпоративных сетях. За детальной информацией по семейству продуктов Sniffer обращайтесь на веб-сайт [www.sniffer.com](http://www.sniffer.com).

Коммерческие программы перехвата сетевых пакетов позиционируются на рынке в первую очередь как утилиты системных администраторов, которым необходимо решать возникающие в сети проблемы. Эти программы обладают множеством функций, которые вряд ли понадобятся обычному шпиону, заинтересованному поиском только определенной информации, и поэтому они имеют соответствующую цену. Готовьтесь к тому, что вам придется выложить от 4000 до 20 000 долларов за подобную программу.

Чаще всего коммерческие программы сетевого мониторинга слишком «тяжелы» для шпионских целей, поэтому, если у вас возникла такая необходимость, займитесь поиском бесплатно распространяемых утилит на необъятных просторах сети Интернет.

В распоряжении пользователей Linux имеется целый ряд свободно распространяемых по принципу открытого кода утилит, включая Kismet, Ethereal (эта программа обсуждалась в главе 10), позволяющую перехватывать и отображать пакеты стандарта 802.11b в «сыром» виде, MogNet (<http://www.node99.org/projects/mognet/>), написанную на Java, AirTraf (<http://airtraf.sourceforge.net>) и Wellenreiter (<http://www.wellenreiter.net>).

## Шпионский инструментарий: действительно ли сетевые мониторы — это реальная угроза?

Являются ли сетевые мониторы (они же программы перехвата сетевых пакетов) реальной или же чисто теоретической угрозой? Поскольку они действуют пассивно (работая только на прием), очень трудно говорить о том, как часто злоумышленниками проводятся подобные операции. Коммерческие предприятия могут и не догадываться о том, что за их сетью наблюдают, и даже в случае раскрытия фактов шпионажа стараются избежать огласки из-за боязни очернить себя перед клиентами.

Весной 2002 года магазины по продаже электроники Best Buy и Home Depot попали в выпуски новостей после того, как стало известно о случаях перехвата данных из беспроводных сетей этих магазинов. «Искатели сетей» с соответствующим оборудованием смогли подключиться к беспроводной сети, работающей с базой данных, и осуществлять мониторинг транзакций с наличными деньгами. Владельцы магазинов по продаже электроники сразу же заявили о том, что все бреши в системе защиты их беспроводных сетей были ликвидированы, и никаких конфиденциальных данных по их клиентам украдено не было. По отчетам же «искателей сетей» перехватить конфиденциальные сведения, например по кредитным карточкам, из беспроводной сети магазина по-прежнему не составляет труда.

Вы должны понимать, что программы сетевого мониторинга беспроводных сетей не выводят информацию по учетным записям пользователей, их пароли, имена кредитных карточек и другую ценную информацию автоматически. Весь сетевой трафик сохраняется, и хотя вы можете настроить фильтрацию сетевых пакетов, вам все равно придется заняться изучением пакетов вручную, чтобы найти крупицы важной информации среди кучи бесполезных данных.

Действительно, сетевые мониторы представляют собой вполне реальную угрозу, но для их эффективного использования в целях шпионажа требуется собрать большой объем данных (поскольку, по статистике, ценная информация составляет весьма небольшой процент от общего объема сетевого трафика). Кроме того, работа шпиона требует немалого терпения для скрупулезного изучения всех собранных данных в поисках стоящей информации.



Если вы хотите узнать о других программах сетевого мониторинга, предназначенных не только для ОС Linux, посетите веб-сайт [www.personaltelco.net/index.cgi/WirelessSniffer](http://www.personaltelco.net/index.cgi/WirelessSniffer).

К несчастью для пользователей Windows, на данный момент мы не можем перечислить приличных бесплатных программ сетевого мониторинга. Вам придется установить на ваш ПК Linux либо обратиться к коммерческим продуктам.

**AIRSNORT.** Программа AirSnort под Linux предназначена для пассивного мониторинга передаваемых по беспроводной сети зашифрованных данных, с целью расшифровки WEP-ключа. Чтобы расшифровать ключ, в программе AirSnort нужно проанализировать от 5 до 10 миллионов зашифрованных сетевых пакетов (приблизительно от 100 Мб до 1 Гб данных). В зависимости от загруженности сети это может занять от нескольких дней до нескольких недель. Как и в случае с программой Kismet, исполняемый код программы вам придется компилировать самостоятельно – такой вариант вряд ли подойдет для шпионов, привыкших к операционной системе Windows и не обладающих большими познаниями в Linux. Получить более подробную информацию о программе и загрузить ее исходные коды можно на сайте <http://airsnort.shmoo.com>.

**MAPPPOINT.** Программа Microsoft MapPoint (рис. 11.9), хотя и не относится к утилитам для беспроводного шпионажа, подобно другим навигационным программам, пользуется популярностью благодаря возможностям визуализации местоположения беспроводных сетей. Собранные GPS-устройством координаты импортируются из NetStumbler или других программ в MapPoint, в которой их местоположение накладывается на карту местности.

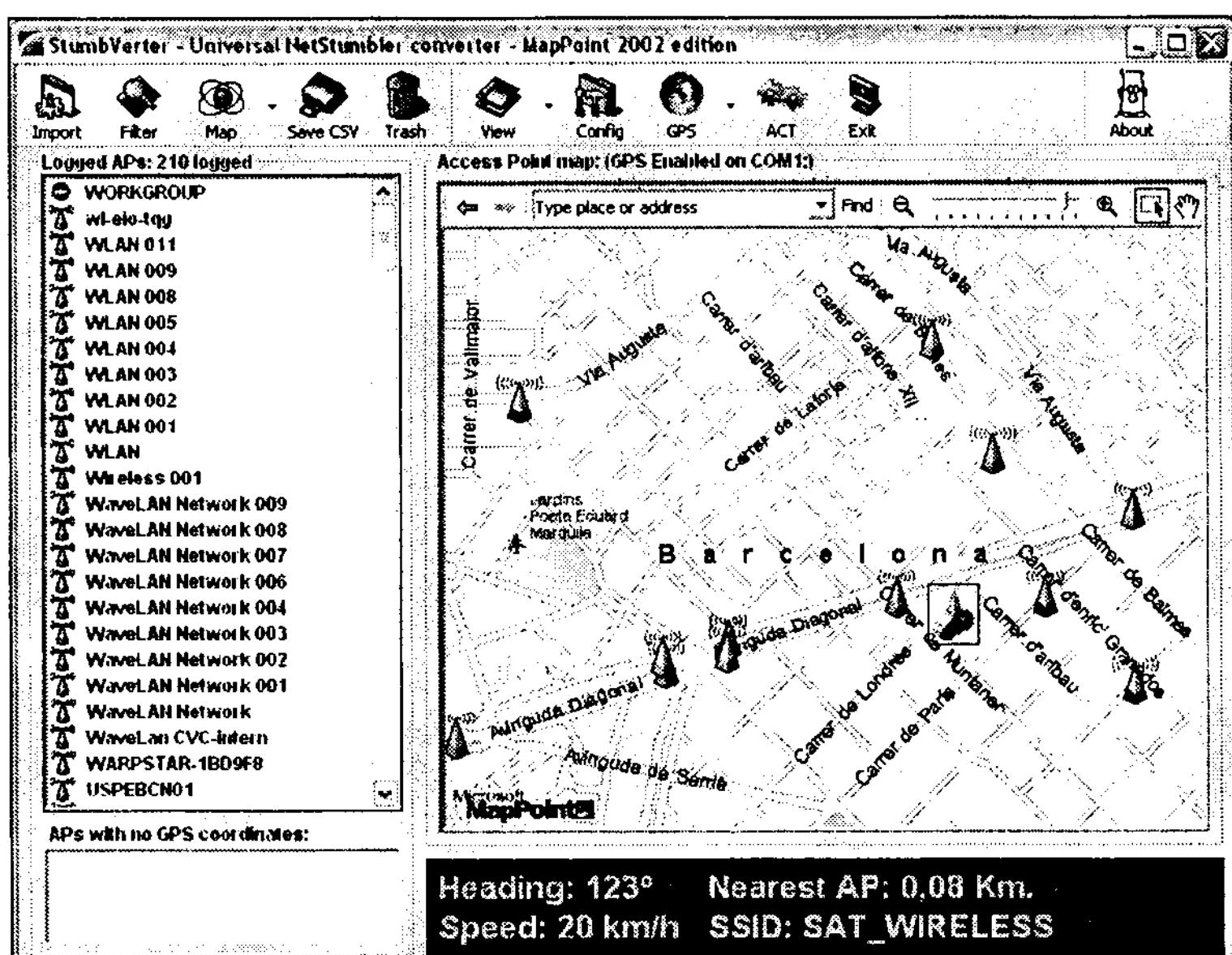


Рис. 11.9. Конвертирование данных из NetStumbler в MapPoint 2002 при помощи утилиты StumbVerter

Свободно распространяемая программа StumbVerter (которую вы можете найти на сайте [www.sonar-security.com](http://www.sonar-security.com)) позволяет импортировать файлы отчетов NetStumbler в MapPoint. Базовые станции с отключенной опцией WEP-шифрования отображаются на карте в виде зеленых значков, а защищенные беспроводные ЛВС с включенным WEP-шифрованием – в виде красных значков. Щелкнув по значку объекта, вы можете просмотреть по нему дополнительную информацию, включая SSID, MAC-адрес и мощность сигнала.

**WINDOWS XP.** Хотя некоторые критикуют Windows XP за присутствие в ней встроенного шпионского программного обеспечения («spyware»), собирающего информацию о пользователе, в то же время в состав этой операционной системы входит программное обеспечение, позволяющее выступать в роли шпиона вам самим. По умолчанию, обнаружив сигнал SSID, пришедший от базовой станции беспроводной ЛВС, Windows XP автоматически настраивает сетевую интерфейсную карту на тот же SSID для подключения к только что обнаруженной сети. Замечательная возможность для шпиона без технического образования, увлеченного поиском незащищенных беспроводных сетей. Итак, за кем вы хотите понаблюдать сегодня?

## Контрмеры

Заниматься поиском «жучков» относительно несложно. Вы их находите и избавляетесь от них (или же, в крайнем случае, сообщаете вашему клиенту о ваших находках, если тот намерен организовать кампанию по дезинформации неизвестного шпиона). Однако в случае с беспроводными сетями ситуация усложняется, поскольку, если вы продемонстрируете клиенту уязвимость сети, он захочет услышать от вас советы о том, как себя обезопасить. Изучив все слабые места в системе защиты беспроводных сетей стандарта 802.11b и средства их использования, вы начинаете думать, была ли вообще так уж хороша идея попытать счастья в бизнесе, связанном с обеспечением компьютерной безопасности.

Мужайтесь! Несмотря на массу известных уязвимых мест беспроводных технологий, вы все-таки в состоянии укрепить безопасность сети и оградить ее от потенциальных шпионов. В то же время не существует одного магического рецепта, который бы позволил прикрыть одним махом все бреши в системе безопасности. Вам необходимо применять многоуровневый подход для обеспечения должной защиты системы, используя одни контрмеры поверх других.

## Мониторинг вашей собственной сети

Раздобудьте себе копии программ NetStumbler и Kismet, чтобы увидеть то, что видит шпион, курсируя вокруг офиса вашего клиента. Пройдитесь

пешком либо подъедьте на машине с ноутбуком и небольшой антенной, чтобы воочию убедиться, какая информация может оказаться доступной для посторонних. Благодаря простоте установки и малой стоимости аппаратного и программного обеспечения, сетевые администраторы имеют возможность в буквальном смысле заниматься шпионажем внутренних беспроводных сетей, которые были настроены сотрудниками без авторизации. Не полагайтесь в этом деле исключительно на программу NetStumbler, поскольку ее возможности ограничены обнаружением только тех базовых станций, которые передают в эфир свой SSID. Сетевые мониторы, такие как Kismet, позволяют находить даже те базовые станции, которые не под силу NetStumbler, – среди них могут оказаться именно те сети, которые вас больше всего интересуют.

## Правильное размещение антенны

Антенна базовой станции должна быть повернута таким образом, чтобы распространение радиоволн за пределы здания было минимальным. Сигнал от базовых станций, размещенных возле окна или на внешней стене, может быть перехвачен снаружи при помощи направленной антенны. Исследуя возможности по обнаружению беспроводных сетей, Шипли пришел к выводу, что при помощи направленной антенны с некоторого возвышения можно идентифицировать беспроводную сеть на расстоянии более десятка миль. Поэтому желательно оптимизировать размещение базовой станции так, чтобы обеспечить максимальное покрытие помещений офиса и в то же время снизить уровень паразитного сигнала, выходящего за пределы здания, чтобы лишить шпионов возможности обнаружить вашу сеть.

### Контрмеры: AirMagnet

AirMagnet представляет собой программу управления беспроводными ЛВС, предназначенную для запуска на КПК. Эта программа поставляется в комплекте со специальной беспроводной картой. Среди функциональных возможностей программы: обнаружение промежуточных базовых станций и клиентов, идентификация атак типа «отказа в обслуживании», поиск базовых станций, выдающих себя за других, обнаружение ненастроенных базовых станций, а также перехват и декодирование сетевых пакетов в режиме реального времени. Стоимость AirMagnet составляет \$2495 плюс стоимость КПК. Помимо выполнения вполне законных операций, AirMagnet может применяться и в целях тайного шпионажа. Если вы захотите больше узнать об этой программе, зайдите на сайт [www.airmagnet.com](http://www.airmagnet.com).

## Контрмеры: дорогая, это тебе

В июне 2002 года компания Science Applications International Corporation (SAIC) по заказу правительства начала работу над проектом создания фальшивых беспроводных сетей (*honeypots*) для привлечения хакеров. Эти сети проектировались специально для привлечения потенциальных хакеров с целью изучения их методов. Эксперимент по защите информации, передаваемой по беспроводным сетям, проводился в секретном месте в Вашингтоне, округ Колумбия. В ходе эксперимента были использованы пять базовых станций Cisco и серия сетевых компьютеров с известными уязвимыми местами. С помощью всенаправленной антенны даже был увеличен радиус действия беспроводной сети для привлечения злоумышленников издалека. Чтобы зафиксировать все попытки подключения к сети, использовалось специальное программное обеспечение, в том числе система обнаружения вторжения.

Консультант компании KMPG организовал подобную беспроводную сеть возле своей лондонской штаб-квартиры, чтобы подсчитать частоту визитов со стороны «искателей сетей» и количество попыток активных сетевых вторжений.

Подобные «мнимые» сети могут быть организованы в корпорациях с высоким риском шпионажа, для того чтобы следить за попытками проникновения в систему. С ростом интереса к вопросу безопасности беспроводных ЛВС в ближайшее время следует ожидать появления целого ряда коммерческих и бесплатных утилит для создания и мониторинга «мнимых» беспроводных сетей.

Если предположить, что в дальнейшем символика war driving будет развиваться такими же темпами, то, скорее всего, среди стандартных символов для обозначения беспроводных сетей очень скоро должен появиться знак «фальшивая сеть».

## Обнаружение средств поиска беспроводных ЛВС

Благодаря популяризации стандарта 802.11b, в системы обнаружения вторжений (IDS) начали встраивать функции обнаружения пробных проникновений и атак со стороны хакеров в беспроводных сетях. Система IDS не позволяет выявить присутствие пассивного сетевого монитора, однако она в состоянии обнаружить более активные атаки, например, когда взломщик проникает в сеть.

Как мы уже говорили, программа NetStumbler выполняет активное сканирование, поэтому ее работу можно обнаружить с помощью такой утилиты, как NSSpyglass под Windows. Более подробно об этой программе вы

можете узнать на сайте <http://home.attbi.com/~digitalmatrix/nsspyglass/>\*. Новая компания под названием AirDefense предлагает еще один гибридный подход с использованием как аппаратного, так и программного обеспечения. Система AirDefense состоит из набора размещенных в пространстве датчиков радиосигнала, которые анализируют сетевой трафик для получения несанкционированного доступа, читают пакеты и пытаются воспользоваться уязвимыми местами в системе защиты базовых станций. В этих датчиках используются специальные алгоритмы и база данных, содержащая информацию об этой беспроводной сети, что позволяет обнаруживать и анализировать любые вносимые в сеть изменения с дальнейшим уведомлением администратора о возможных рисках. Получить детальную информацию об этой системе вы можете на сайте [www.airdefense.net](http://www.airdefense.net).

## Средства одурачивания шпионов

Классический армейский пример того, как можно одурачить врага, заключался в создании на радаре фальшивых целей (нескольких сотен вместо одной или двух реальных). Группа Black Alchemy разработала утилиту под названием Fake AP, позволяющую одурачивать шпионов, занимающихся поиском беспроводных сетей. Fake AP передает ложную информацию для NetStumbler и других подобных программ, заставляя их думать, что в окрестной местности находятся тысячи базовых станций. Таким образом, определить, какая из этих станций является настоящей, становится далеко не тривиальной задачей.

Программа Fake AP предназначена для работы на Linux-платформах, а загрузить ее можно с сайта [www.blackalchemy.to](http://www.blackalchemy.to).

### Контрмеры: использовать ли WEP

Между 31 августа и 7 сентября 2002 года «искатели сетей» со всего мира приняли участие в Первом всемирном сканировании беспроводных сетей. В ходе этой акции все собранные протоколы NetStumbler отправлялись для обработки на центральный сервер. В Северной Америке было обнаружено 9102 беспроводных ЛВС, в 70% которых не использовалась защита при помощи WEP-шифрования. Эти данные подтверждают результаты других исследований, в которых показатель незащищенных сетей (с отключенным WEP-шифрованием) колебался от 60% до 80%.

Поэтому, если вам не безразлична ваша безопасность, используйте WEP.

\* Утилита NSSpyglass доступна для загрузки по адресу <http://www.michigan-wireless.org/tools/>. – Прим. ред.

## Включение WEP-шифрования

Хотя мы и убедились, что WEP-шифрование не обеспечивает полной защиты, оно дает базовый уровень надежности ЛВС и может служить дополнением к вашим контрмерам. Помните, что WEP-шифрование иногда понижает сетевое исполнение до уровня шифрованных и дешифрованных пакетов данных. Низкая скорость в обмен на лучшую защиту.

## Регулярная смена WEP-ключей

После включения WEP-шифрования вы обязательно должны сменить заданный по умолчанию WEP-ключ, поскольку подобные ключи широко известны, так же как используемые производителями по умолчанию пароли и SSID. После этого вы должны достаточно регулярно менять значения ключей. Хотя WEP-ключ можно взломать, однако утилитам, таким как, например, AirSnort, для этого потребуется проанализировать достаточно большой объем информации. Если у вас высокая загруженность сети, то ключ следует менять еженедельно. Если же сетевая активность в вашей компании низкая, ключ достаточно менять раз в месяц. С точки зрения решения административных задач в большой организации для этого потребуется немало времени, поскольку администратору понадобится заменить ключи на всех клиентских компьютерах. Как и в случае применения любых других контрмер, прежде всего вам следует взвесить потенциальную угрозу и затраты, необходимые для обеспечения безопасности.

## Аутентификация MAC-адресов

В большинстве базовых станций для работы с сетью используются списки авторизованных MAC-адресов. Таким образом, если к сети попытается обратиться сетевая интерфейсная карта, MAC-адрес которой отсутствует в этом списке, то в доступе ей будет отказано. Теоретически это отличная контрмера. Однако при помощи программ перехвата сетевых пакетов вы можете быстро выяснить MAC-адреса всех клиентов и самой базовой станции, после чего легко фальсифицировать этот адрес. Кроме того, если шпион обладает физическим доступом к ноутбуку клиента либо хотя бы к его сетевой интерфейсной карте (взяв ее на время из оставленного без присмотра компьютера), аутентификация при помощи MAC-адресов становится бесполезной. И наконец, подобные контрмеры пригодны лишь для небольших сетей, так как в большой корпорации постоянно следить за актуальностью существующего списка MAC-адресов практически нереально.

## Изменение SSID

Некоторые администраторы сразу же изменяют SSID базовой станции, что, однако, мало что дает в плане безопасности, поскольку такие утилиты, как NetStumbler, принимают измененный SSID и даже позволяют определить тип базовой станции. Если вы решили изменить SSID, то придумайте

что-нибудь такое, что не привлечет излишнего внимания со стороны шпионов. К примеру, название SSID RD\_LAB слишком много говорит о цели.

Не надейтесь, что, заменив SSID базовой станции на идентификатор по умолчанию другого производителя, вы сможете ввести в заблуждение потенциального шпиона. Теоретически наблюдатель может попытаться воспользоваться известными уязвимыми местами базовой станции Cisco, поскольку сеть имеет SSID «tsunami», хотя на самом деле используется оборудование компании D-Link. Обычно тактика «одурачивания» шпионов дает неплохой результат, но в данном случае она не пройдет. Дело в том, что утилиты вроде NetStumbler для определения производителя оборудования анализируют передаваемые MAC-адреса. Например, первая часть MAC-адреса 00055D-A6F60C говорит о том, что данное оборудование было произведено компанией D-Link Systems. Даже если SSID сети будет «tsunami», число 00055D однозначно определяет производителя – компанию D-Link.

Если постоянная передача сигнала SSID в эфир отключена, определить SSID можно при помощи программы перехвата сетевых пакетов, и, если в сети не включена опция WEP-шифрования, шпион может использовать известный идентификатор SSID для подключения к сети. Макс Мозер, автор утилиты Wellenreiter для Linux, советует вам придерживаться следующей тактики. SSID может иметь длину до 34 символов и содержать непечатаемые символы (например, ASCII 7 (звуковой сигнал) или ASCII 9 (символ табуляции)). Используйте подобные символы в SSID, поскольку это может ввести в заблуждение различные сканеры и сетевые мониторы, которые будут некорректно отображать данный идентификатор.

## Отключение функции передачи SSID

Во многих базовых станциях имеется возможность отключения передачи SSID в эфир. Если передача идентификатора SSID будет отключена, такие программы, как NetStumbler, не смогут обнаружить сеть и вывести SSID. Кроме того, в этом случае компьютеры под управлением Windows XP также не смогут автоматически подключаться к сети.

Но даже эту контрмеру нельзя назвать «защитой от дурака». При загрузке компьютера или (в случае с ноутбуком) его перемещении в зоне покрытия беспроводной сети, отправляется кадр ассоциации. В этих кадрах всегда содержится идентификатор SSID, который может быть легко перехвачен шпионом при помощи программы сетевого мониторинга.

## Изменение пароля по умолчанию базовой станции

Когда шпион видит, что в сети используется SSID по умолчанию, он может попытаться воспользоваться паролем по умолчанию для подключения к базовой станции. Если ему повезет, он сможет перенастроить беспроводную сеть, создав еще одну брешь в системе безопасности. Поэтому, кроме случаев крайней необходимости, вам следует всегда отключать функции удаленного администрирования.

## Применяйте статические IP-адреса

Для того чтобы клиент мог обращаться к различным сетевым ресурсам, ему должен быть присвоен определенный IP-адрес. Протокол динамического определения адресов (DHCP) позволяет автоматически назначать активному клиенту IP-адрес. Протокол DHCP часто используется для облегчения жизни администратора. К сожалению, он одновременно облегчает жизнь шпионам беспроводных сетей, которые с легкостью получают доступ к сети после автоматического присвоения им IP-адреса. Если же отключить DHCP, вам придется вручную назначать IP-адреса каждому клиенту беспроводной сети. Однако и это не гарантирует полной защиты, поскольку выяснить IP-адрес компьютера и впоследствии использовать его не составляет труда.

## Размещайте базовые станции за пределами брандмауэра

Из-за огромного количества известных ошибок системы безопасности стандарта 802.11b беспроводные сети всегда следует рассматривать в качестве не заслуживающих доверия соединений. По этой причине брандмауэр должен изолировать базовую станцию от основной сети. При соблюдении данной стратегии, даже если шпиону удастся получить несанкционированный доступ к базовой станции, оставшаяся часть сети будет под защитой брандмауэра.

## Применение виртуальных частных сетей

Виртуальные частные сети (VPN) используются для создания частных сетей, например, офисных ЛВС, через общедоступные линии связи, например, через Интернет. Весь обмен информацией в VPN шифруется намного надежнее, чем в беспроводных ЛВС с WEP-ключом. Применение виртуальных частных сетей является, вероятно, наиболее эффективной мерой укрепления безопасности вашей беспроводной ЛВС.



За более подробной информацией о виртуальных частных сетях, обращайтесь к главе 10.

## Не рассчитывайте на расстояние как меру безопасности

Многие администраторы полагают, что рекламируемый ограниченный радиус действия беспроводных сетей стандарта 802.11b сам по себе является защитной мерой, и не считают нужным обращать внимание на странные автомобили с антеннами, поставленные на служебной парковке.

Напомним вам, что Питу Шипли удалось подключиться к одной из сетей в западном Сан-Франциско с холма над Калифорнийским университетом в Беркли, находясь на расстоянии 15 миль от объекта.

## Отключайте базовую станцию

Выключайте базовую станцию, когда она не используется. Если беспроводная сеть нужна вам только в рабочие часы, отключайте ее на ночь. Если у вас имеется четкий график работы, вы даже можете настроить базовую станцию на автоматическое включение в начале рабочего дня и на вечернее отключение. Иногда такие простейшие контрмеры бывают весьма действенны.

## Заключение

Угроза шпионажа для беспроводных сетей имеет вполне реальные черты. За прошедшие несколько лет «искатели сетей» (люди, занимающиеся так называемым *war driving*) успели продемонстрировать незащищенность и уязвимость подавляющего большинства беспроводных ЛВС. И все же, несмотря на постоянное обсуждение вопросов безопасности в средствах массовой информации, пользователи и администраторы сетей продолжают применять настройки оборудования по умолчанию, оставляя открытыми двери для сетевых шпионов.

Хотя наиболее уязвимым местом в плане обеспечения безопасности всегда будет оставаться человеческий фактор, в технической сфере в будущем можно ожидать сдвигов в укреплении безопасности беспроводных сетей. Поскольку все слабые места в системе защиты современного стандарта 802.11b хорошо изучены, в последующих ревизиях стандарта они должны быть исправлены.

Находящийся в настоящее время на заключительной стадии разработки стандарт 802.11i должен прийти на смену шифрованию WEP. Торгово-промышленная группа Wi-Fi Alliance ([www.wi-fi.org](http://www.wi-fi.org)) представила внутреннюю спецификацию безопасности (в качестве переходного этапа к стандарту 802.11i) под названием WPA (Wi-Fi Protected Access), в котором исправлены многие ошибки WEP\*. Стандарт аутентификации сетевых портов 802.1x разрабатывается для укрепления безопасности больших корпоративных сетей при помощи сервера службы аутентификации удаленных абонентов (RADIUS – Remote Authentication Dial-In User Service).

\* Этот стандарт был сертифицирован еще в июне 2003 года, а к началу 2004 года продукты с поддержкой WPA появились в ассортименте всех основных производителей сетевого оборудования. – Прим. перев.

В заключение следует отметить, что беспроводные технологии еще просто не достигли зрелости в плане безопасности и в настоящее время проходят те же самые этапы в развитии систем защиты, которые в свое время проходили другие методы и технологии. Следует понимать, что в будущем никто не застрахован от обнаружения новых уязвимых мест и методов их использования. Если вы являетесь системным администратором или работаете в службе поддержки беспроводных сетей, вам придется постоянно быть начеку в ближайшие несколько лет, следя за всеми новостями в плане безопасности.

## Глава 12

# Офисное оборудование

«Я знаю, что вы работаете на ЦРУ...»

War, “Why Can’t We Be Friends?” *Why Can’t We Be Friends*

Шпионаж в сфере высоких технологий не ограничивается персональными компьютерами. Информация может быть получена и с другой офисной или персональной электронной техники. Многие люди, уделяя значительное внимание укреплению компьютерной безопасности, игнорируют другие возможные пути утечки конфиденциальных данных. В этой главе мы поговорим о том, какая информация может быть собрана с офисного оборудования, средств связи, пользовательских электронных устройств, а затем коснемся вопроса контрмер, которые помогли бы вам защитить себя от шпионов. В данной главе вы сможете расслабиться, поскольку мы не станем заставлять вас играть роль шпиона, как в предыдущих главах, а предложим вам просто сесть, отдохнуть и послушать информацию о том, как осуществлять шпионаж за электронными устройствами.

## Офисное оборудование

Давным-давно, когда наша жизнь была намного проще, шпионам приходилось рассчитывать только на обрывки бумажек или отпечатки на красящей ленте печатной машинки для определения намерений объекта. Современное сложное офисное оборудование может быть таким же небезопасным в плане сохранности информации, как и давно отжившая свой век печатная машинка. Любое устройство, при помощи которого вы работаете с важной и конфиденциальной информацией, может рассматриваться как потенциально уязвимое место, которым может воспользоваться шпион. К офисным устройствам, которые представляют наибольшую угрозу в плане утечки информации, относятся факсы и машины для уничтожения бумаг.

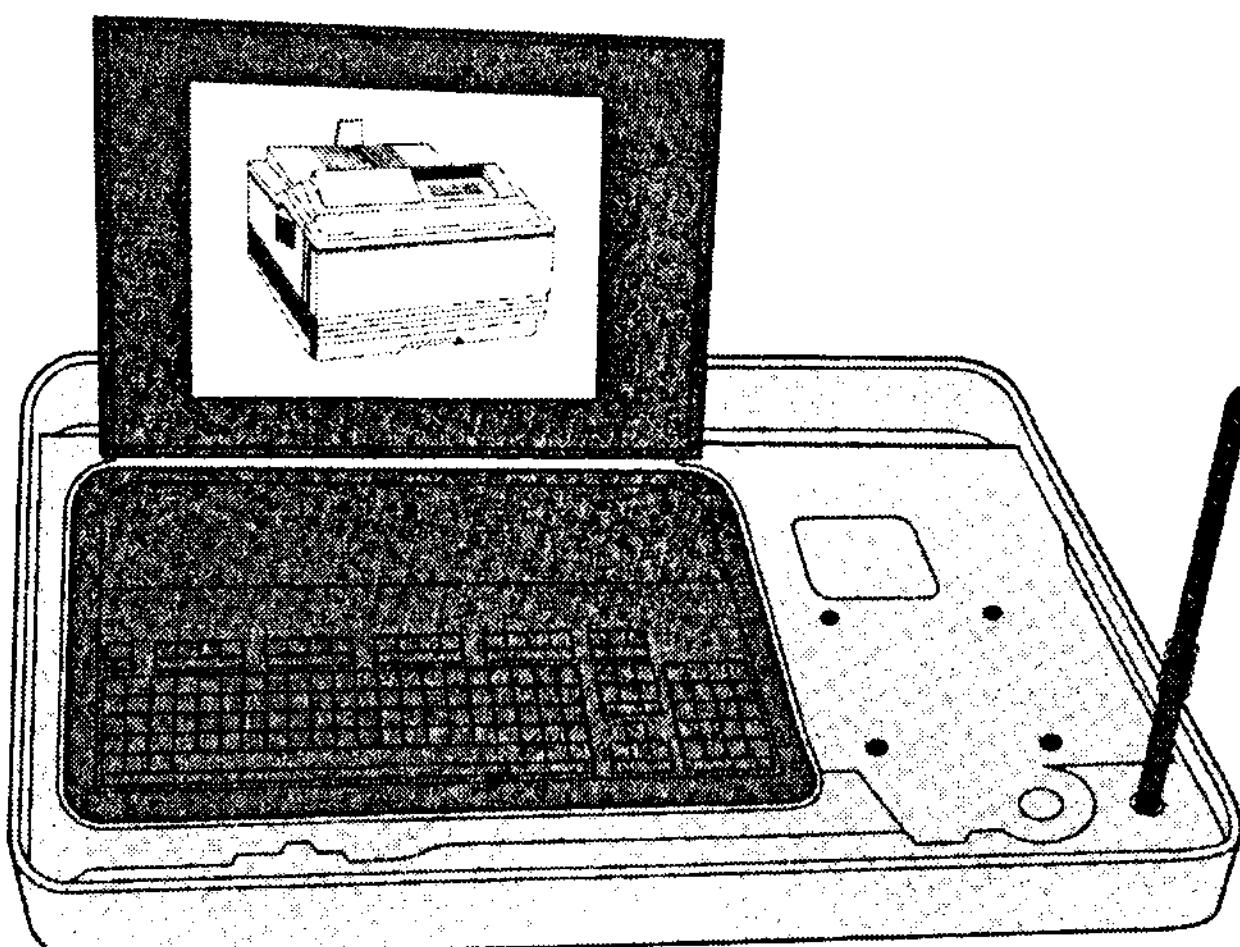
### Факсы

До появления электронной почты для быстрой передачи документов на большие расстояния использовался факс. Хотя электронная почта, наличие сканеров и FTP несколько приуменьшили значимость такого устройства,

как факс, его продолжают достаточно широко использовать дома, в офисах и госучреждениях. Поскольку через факс нередко проходят конфиденциальные документы, то именно это устройство представляет для шпиона наибольший интерес.

Итак, при работе с факсом вы должны учитывать следующие моменты в плане безопасности:

- **Перехват информации.** Факсы используют низкую скорость передачи и хорошо документированный протокол передачи данных в незашифрованном виде. По этой причине передаваемую по факсу информацию достаточно легко перехватить и просмотреть. Промышленные устройства для перехвата факсимильных сообщений имеются в распоряжении правительственные служб не первый год (см. рис. 12.1). Даже если наблюдатель не имеет доступа ни к одному из таких устройств (поскольку продажа подобного оборудования в США ограничена), он всегда может подключиться к телефонной линии и сделать запись переданной информации на цифровую аудиопленку (DAT). Затем шпиону останется только проиграть эту запись для другого факса, заставив его поверить, что данные были переданы с другого устройства.



**Рис. 12.1.** Портативное устройство мониторинга факсов, выпускаемое британской компанией Eskan Electronics ([www.eskan.com](http://www.eskan.com))

- **Рулоны копировальной бумаги.** Во многих факсах для печати документов используется копировальная бумага (такая же, как и в электронных печатных машинках). После приема и распечатки факса на этом рулоне остается изображение, идентичное распечатанному. Использованный рулон копировальной бумаги может быть извлечен шпионом либо сотрудником группы

технического обслуживания, после чего на рулоне можно будет увидеть копии всех принятых факсом документов в негативе. (Этот же способ может быть применен по отношению к печатным машинкам и матричным принтерам.)

- **Журналы факса.** Многие факсы обладают функцией хранения входящих и исходящих посланий с указанием даты, времени, количества страниц и телефонного номера. Поэтому, имея физический доступ к факсу, шпион может просмотреть документы и установить связь между ними.
- **Входящие и исходящие сообщения.** Больше всего вы рискуете тогда, когда входящее факсимильное сообщение находится на всеобщем обозрении до тех пор, пока получатель его не заберет. В случае с исходящими сообщениями возможна ошибочная отправка факса другому абоненту из-за неправильного соединения. В принципе многие факсы можно настроить таким образом, чтобы они тайно отсылали копию всех исходящих сообщений на определенный номер.

Дабы оградить себя от шпионских посягательств при использовании факса, советуем вам прибегнуть к следующим контрмерам:

- **Воспользоваться устройством шифрования сообщений.** Устройство, подключаемое между факсом и телефонной линией, осуществляет шифрование передаваемой информации. Для нормальной работы вам необходимо наличие двух устройств: одного на факсе, с которого отправляются документы, а другого на машине, на которую эти документы принимаются (помимо создания дополнительного препятствия на пути шпиона, это оборудование защитит вас от ошибочной установки соединения с номером, на котором отсутствует аппарат для шифрования и дешифрования). Для обеспечения максимального уровня защиты примите оборудование со стойкими алгоритмами шифрования.
- **Не применять факсы с копировальной бумагой.** Факсы с жидкими чернилами или тонером не позволяют восстановить точную копию документов в отличие от факсов, использующих копировальную бумагу. Если в вашем факсе применяется копировальная бумага, постарайтесь ограничить доступ к факсу посторонних лиц, а использованные рулоны сжигайте.
- **Не посылать по факсу конфиденциальные документы.** Доставка курьером обойдется вам несколько дороже, но при этом вы выиграете в безопасности. В качестве альтернативы можем предложить вам воспользоваться такой программой, как WinFax Pro фирмы Symantec, чтобы отсканировать серию документов, сохранить файл на вашем жестком диске, зашифровать его при помощи утилиты PGP и отправить по электронной почте получателю.

## Тактика: копировальный аппарат с «сюрпризом»

В одном из номеров журнала *Popular Science* за 1996 год была опубликована интересная статья о том, как ЦРУ использовало копировальную машину в целях шпионажа с начала 1960-х. Статья, факты из которой подтверждены другими независимыми источниками, подробно описывает, как государственное разведывательное управление договорилось с компанией Xerox о разработке миниатюрной камеры, которую можно было бы разместить внутри копировальной машины. Целью разведчиков являлось посольство Советского Союза в Вашингтоне, округ Колумбия.

Команда разработчиков из компании Xerox модифицировала камеру для домашней киносъемки, добавив в нее специальный фоточувствительный элемент, который активировал камеру при снятии копии с документа. Затем камера была спрятана среди других деталей ксерокса. Технические работники компании Xerox установили камеру в Советском посольстве во время проведения планового технического обслуживания копировального аппарата в 1963 году. При последующих вызовах службы технического обслуживания они выполняли извлечение и замену пленки из камеры на новую. Эта операция оказалась настолько успешной, что подобные камеры были установлены в копировальных аппаратах по всему миру.

Нет никаких причин полагать, что подобные устройства наблюдения не могут использоваться и по сей день, причем не только в копировальных аппаратах, но и в факсах, сканерах и машинах для уничтожения бумаги. С появлением цифровых фотокамер и развитием беспроводных технологий связи всегда улыбающемуся сотруднику компании Xerox даже не придется наносить вам регулярные визиты после тайной установки устройства.

## Машины для уничтожения бумаги

Любимое занятие шпионов и взломщиков – искать выброшенные документы в корзине для бумаг. «Dumpster diving»\* позволяет обнаруживать конфиденциальную информацию самого различного рода, которую небрежные сотрудники просто смяли и выбросили в корзину. Ключевой мерой защиты в данном случае является использование машин для уничтожения бумаг (shredder), делающих невозможным прочтение информации на бумаге. (В связи с возросшей популярностью таких носителей информации, как

\* То есть копание в мусорных корзинах, от названия фирмы Dumpster, выпускающей большие контейнеры для мусора. – Прим. перев.

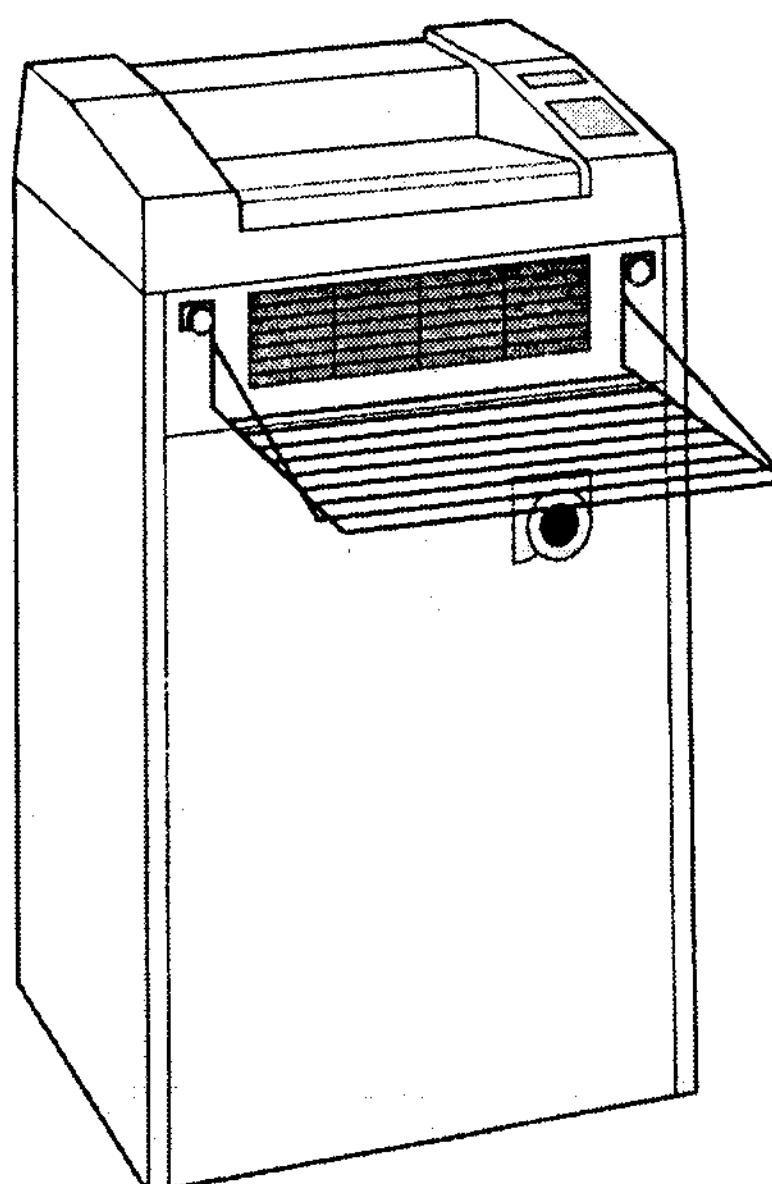
CD и DVD, в последнее время на рынке начали появляться специальные устройства для уничтожения таких носителей, доступные отдельно либо в комплекте с машиной для уничтожения бумаг.)

Продажа машин для уничтожения бумаг и предоставление услуг службами, занимающимися уничтожением секретных документов, сейчас превращается в крупный бизнес. По приблизительным оценкам, в Соединенных Штатах машины для уничтожения бумаг в корпорациях и государственных учреждениях ежегодно измельчают около пяти миллионов тон бумажных документов. Значительно увеличилась и продажа машин для уничтожения бумаг, ориентированных на домашнее использование, поскольку общественное мнение обеспокоено тем, что извлеченные из корзины обрывки бумагек могут использоваться для кражи личной информации.

Существует множество способов уничтожения документов: вы можете их резать, сминать, разрывать и измельчать любыми средствами, однако что касается уничтожения офисных документов, то здесь обычно применяется два метода:

- **Разрезание на полосы.** Этот метод применяется в недорогих машинах для уничтожения бумаг, которые разрезают документы на узкие полосы шириной от 4 до 13 мм. Такие машины не подходят для уничтожения конфиденциальных документов, поскольку из полосок такой ширины достаточно легко можно реконструировать исходный документ. Классический пример – захват посольства США в Иране в 1979 году. Сотни документов, отнесенных к разряду секретных, были восстановлены в результате скрупулезной работы, а затем опубликованы в виде собрания из 23 томов под названием «Документы из логова шпионов» (посетите, к примеру, сайт [www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB21/](http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB21/)). В оправдание сотрудников посольства и ЦРУ следует отметить, что они рассчитывали на достаточное количество времени для сжигания разрезанных документов в соответствии с инструкцией, однако посольство было захвачено намного быстрее, чем они ожидали. Еще один недостаток такого типа машин для уничтожения бумаг – получаемый объем отходов. Один кубический метр бумаг может занимать в измельченном виде все десять кубометров.
- **Поперечная нарезка.** Машины для уничтожения бумаг, в которых используется поперечная нарезка документов, более надежны в плане безопасности, чем машины предыдущего типа, поскольку в них осуществляется разрезание документов сначала в одном, а затем в другом направлении, в результате чего получаются мелкие обрезки, напоминающие конфетти, восстановить какую-либо информацию с которых становится, мягко говоря, затруднительно. Обычно чем дороже стоит такой аппарат, тем быстрее он работает и тем мельче нарезка. Как правило, размер клочков бумаги после нарезки составляет от 4×65 мм до 0,8×13 мм.

Главное правило, которым следует руководствоваться при выборе машины для уничтожения бумаг, – чем меньше кусочки, на которые разрезаются документы, тем выше надежность защиты ваших документов. В соответствии с требованиями Министерства обороны конфиденциальные, секретные и совершенно секретные документы должны быть измельчены на кусочки размером не более  $0,8 \times 13$  мм (за более подробной информацией по правилам уничтожения секретных документов обращайтесь к документам Программы безопасности информации Министерства сухопутных сил: AR 380-5, приложение K, которые размещены в Интернете по адресу <http://ia.gordon.army.mil/iaso/Army/AR%20380-5/AppendixI-K.htm>). В настоящее время на рынке начинают появляться новые машины для уничтожения бумаг, соответствующие спецификации NSA/CSS #02-01, которые позволяют разрезать документы на кусочки не более  $1 \times 4$  мм. Однако стоимость устройств даже нижней ценовой группы, соответствующих государственным стандартам безопасности, составляет не менее \$800. (Надеюсь, вы понимаете, что в посольствах будут использоваться не те машины за \$20 для уничтожения бумаг, которые можно приобрести в магазине за углом?) Машины для уничтожения бумаг, соответствующие госстандарту США, производят следующие фирмы: Dahle (рис.12.2), Intimus, Olympia и Security Engineered Machinery.



**Рис. 12.2.** Машина для уничтожения бумаг Dahle 20634 EC, соответствующая стандартам NSA (размер фрагментов после порезки –  $1 \times 4$  мм)

Но действительно ли вам так уж необходимы машины для уничтожения бумаг, соответствующие стандартам Министерства обороны и Управления национальной безопасности? Вначале вы должны определить наиболее вероятную угрозу и ее источник (мы уже говорили об этом в главе 1). Определенно, вам нужно приобретать модель с поперечной нарезкой, а не машину для уничтожения бумаг с разрезанием на обычные полоски; и уже затем, посчитав, сколько бумаг вы собираетесь уничтожать ежедневно, и, исходя из таких характеристик, как размер и количество одновременно обрабатываемых листов, выберите наиболее подходящую модель.

Если вам нужна полная гарантия защиты вашей конфиденциальной информации, после измельчения в машине для уничтожения бумаг сожгите либо спустите в туалет полученные обрезки. Хотя эту меру можно считать избыточной для большинства обывателей, однако, если вы имеете дело с информацией государственной важности (или, по крайней мере, вам так кажется), это достаточно распространенный и эффективный метод.

### **Шпионский инструментарий: ПО для восстановления документов**

Хотя восстановление разрезанного документа вручную требует много времени и терпения, существуют предположения, что разведуправления и правоохранительные органы научились автоматизировать процесс восстановления измельченных документов.

В конце 1990-х компания Wakefield Integrated Technologies начала рекламную кампанию своего программного продукта под названием Unshredder, который работал вместе со сканером, используемым для сканирования фрагментов бумаги. После сканирования всех обрезков приложение при помощи специального алгоритма подбирало фрагменты, пытаясь восстановить исходный документ.

Компания Wakefield поддерживала собственный веб-сайт по адресу [unshredder.com](http://unshredder.com), на котором активно рекламировался данный продукт, однако и сама компания, и ее сайт исчезли год спустя\*. К сожалению, нам остается только гадать, то ли технология оказалась несовершенной, то ли этот сайт являлся мистификацией, то ли некое государственное управление приобрело продукт и саму технологию.

(Кэвин Мюррей из компании Murray and Associates, уважаемая личность в бизнесе, связанном с контршпионажем, разместил некоторые рекламные материалы по данному программному продукту на своем сайте <http://www.spybusters.com/pdf/UNshredder.pdf>.)

\* Однако домен unshredder.com остается зарегистрированным. – Прим. ред.

# Средства связи

Информация, передаваемая при помощи средств связи (таких, как обычные и сотовые телефоны, пейджеры, голосовая почта), также может быть перехвачена удаленно (путем подслушивания) либо локально, если шпион обладает физическим доступом к устройству. Средства связи традиционно являются самым слабым звеном в большинстве систем безопасности (люди слишком любят поговорить), и эта их слабость активно используется шпионами с соответствующим техническим оборудованием. С другой стороны, если вы предполагаете, что кто-то может подслушивать ваш разговор, воспользуйтесь целым рядом электронных контрмер, призванных обеспечить безопасность вашего общения.

## Телефоны

Практика подслушивания телефонных переговоров берет свое начало почти с момента изобретения самого телефона в конце XIX века. Шпионы, полицейские, ревнивые супруги прибегали к самым различным способам, начиная от использования параллельного телефона и до установки «жучков», предназначенных для записи переговоров. Вплоть до 1960-х годов «жучки» для прослушивания телефонных разговоров и аудионаблюдения в помещении мог заказать по почте практически любой человек. В 1960-е годы законы о производстве и применении приборов для аудионаблюдения были ужесточены, и с тех пор легально приобрести их могут только представители государственных управлений и правоохранительных органов в соответствии с судебным ордером. В то же время реально мало что было сделано для остановки шпионажа, поскольку некоторые законы довольно трудно привести в исполнение, и, в частности, подслушивание телефонных переговоров до сих пор остается весомой угрозой. Обсуждение деталей телефонного шпионажа, технологий аудионаблюдения и защитных контрмер выходит за рамки данной книги. Если вас интересует эта сторона шпионажа, начните с посещения веб-сайта Марти Кайзера, размещенного по адресу [www.martykaiser.com](http://www.martykaiser.com). Кайзер стал легендой в шпионском бизнесе, разработав с 1960-х годов огромное количество интересных приборов для различных правительственные учреждений с трехбуквенными названиями (ФБР, ЦРУ и др.).

В целом наблюдение за телефонными линиями может быть организовано двумя различными способами:

- **При помощи устройств для прослушивания.** Как правило, подобные устройства подключаются к телефонной линии. Главное преимущество от их использования – не нужен физический доступ к телефонному аппарату (вам не придется организовывать рискованные тайные проникновения), поскольку такие приборы могут быть установлены за несколько километров от цели. Многие санкционированные судом операции по подслушиванию

телефонных переговоров могут проводиться на территории АТС, что делает их обнаружение практически невозможным. (В «шпионских магазинах» продаются относительно недорогие устройства для обнаружения «жучков», которые работают только с основными типами подслушивающих устройств и практически бесполезны против серьезно настроенного противника.)

- **При помощи «жучков».** Если шпион обладает физическим доступом к телефону, он может установить подслушивающее устройство внутри телефонной трубки. Такие «жучки» могут записывать не только телефонные переговоры, но и вообще любые другие звуки в помещении, пока трубка лежит на рычаге. (Предостережения для офис-менеджеров: некоторые устройства громкоговорящий связи, не требуя модификации, могут передавать радиосигнал на расстояние в несколько сотен футов.)

Хотя для защиты от прослушивания телефонных переговоров разработан ряд высокотехнологичных контрмер (о которых мы поговорим в ближайшем будущем), более надежной защиты, чем держать рот на замке и воздерживаться от обсуждения по телефону конфиденциальных тем, не существует.



Телефонные «жучки» промышленного производства и другое оборудование, предназначенное для скрытого аудионаблюдения, считается незаконным в США, и его могут применять только представители правоохранительных органов и правительственные учреждений. (Хотя существуют такие компании, как Ramsey Electronics – [www.ramseykits.com](http://www.ramseykits.com), абсолютно законно выпускающие конструкторы, из которых можно собрать прибор для аудионаблюдения. В процессе сборки вам должна помочь книга Уинстона Аррингтона «Как услышать это», размещенная на сайте [www.covertbug.com](http://www.covertbug.com), в которой описываются способы создания самодельных подслушивающих устройств.) Чтобы составить представление о том, какие товары легально доступны для правоохранительных органов (и нелегально для всех остальных), зайдите на веб-сайт английского производителя шпионского оборудования Lorraine Electronics по адресу [www.lorraine.co.uk](http://www.lorraine.co.uk).

## БЕЗОПАСНЫЕ ТЕЛЕФОНЫ

Один из способов защиты от телефонного шпионажа – использование безопасных телефонов. Приборы для шифрования голосовых данных существуют еще с середины 60-х годов прошлого века. Наиболее широко используются так называемые безопасные телефоны STU (Secure Telephone Unit). Подобные устройства впервые появились в 1970-х, и сейчас выпущено уже третье поколение таких телефонов (STU-III). Телефон STU-III на вид ничем не отличается от обычного настольного телефона (рис. 12.3) и работает по тому же принципу, не считая поддержки безопасного общения с тем, у кого также имеется телефон STU-III.



**Рис. 12.3.** Плакат, призывающий соблюдать безопасность переговоров, на котором изображен обычный телефон STU-III и увеличенный криптографический ключ CIK KSD-64A, предназначенный для организации безопасных переговоров

Алгоритм работы безопасного телефона следующий. Вы звоните на другой телефон STU-III по обычной телефонной линии. Затем говорите вашему абоненту: «Переходим на безопасный режим». После этого вы оба должны вставить специальный криптографический ключ (CIK – Crypto Ignition Key) и нажать на своих телефонах кнопки Secure Voice, в результате чего аудиоданные начнут передаваться в зашифрованном виде. Даже если шпион занимается прослушиванием телефонной линии, он не сможет записать ничего, кроме псевдослучайного шума, или, в некоторых случаях, абсолютно неразборчивых металлических голосов. После удаления ключа разговор будет продолжен в обычном незашифрованном виде. (Каждый раз при вставке CIK-ключа телефон автоматически переходит в разряд секретной техники, с которой могут работать только пользователи, имеющие специальный допуск на применение STU-III. Как только CIK-ключ будет удален, телефон превращается в обычное несекретное, хотя и очень дорогое, средство переговоров: стоимость телефона STU-III нынешнего поколения составляет около 3000 долларов.)

Перебежчики из иностранных разведывательных служб утверждают: телефоны STU-III очень эффективны в плане защиты от прослушивания.

Тем не менее многие важные разведданные могут быть получены из незашифрованных фрагментов переговоров.



Более подробно узнать о телефонах STU-III можно из руководства пользователя, выпущенного Министерством обороны для своих сотрудников (ищите его в Интернете по адресу <http://koeln.ccc.de/archive/doku/stu3.pdf>). Подробное описание телефонов STU-III (включая фотографии) и других используемых правительством средств связи можно найти на сайте [www.tscm.com/stu.html](http://www.tscm.com/stu.html).

Вы не сможете приобрести телефон STU-III на ближайшем радиорынке, хотя существуют разновидности аппаратов с менее стойким алгоритмом шифрования, доступные широкой публике. Если же вы являетесь среднестатистическим гражданином, желающим защитить свою частную жизнь, у вас тоже есть для этого вполне реальные возможности.

Многие «шпионские магазины» продают устройства, обеспечивающие шифрование телефонных переговоров, не давая возможности подслушать вас. Вам понадобится, как минимум, два таких устройства: одно должно быть у вас, а другое у вашего абонента, с которым вы хотите безопасно общаться. Простейшие устройства шифрования применяют технологию инвертирования частоты для искажения речи (соответственно восстановить оригинальную речь при помощи недорогой аппаратуры не менее просто). Более дорогие устройства (стоимостью от 1500 долларов), ориентированные на применение отдельными частными лицами и корпорациями, которые нуждаются в безопасных средствах связи, используют более стойкие алгоритмы шифрования.

В 1999 году некая компания под названием Starium Incorporated заявила о скором появлении оборудования для безопасных телефонных переговоров, ориентированного на рядового потребителя. Разработанное в содружестве с известным специалистом по криптографии Эриком Блоссом небольшое устройство по розничной цене менее 100 долларов могло подключаться к любому телефону, обеспечивая высокую безопасность переговоров за счет использования стойких алгоритмов шифрования (см. сайт [www.starium.com/pics.htm](http://www.starium.com/pics.htm)). Это устройство так никогда и не увидело свет, а судьба самой компании к концу 2002 года оказалась под вопросом, хотя разговоры о возможности повторной попытки прорыва на рынок не угасали.

Существует также безопасный протокол передачи голосовых данных через Интернет (VoIP – Voice over Internet Protocol), который должен стать альтернативой старым телефонным сетям. Большинство приложений для работы с голосовыми данными через Интернет являются незащищенными, мы же назовем вам два приложения, поддерживающих шифрование данных, которые лишают шпионов возможности подслушать вас.

- Speak Freely – бесплатная утилита, распространяемая по принципу открытого кода. Она была разработана Брайаном С. Вайлзом и Джоном Уолкером. Программа может работать под

операционными системами Windows и Linux. Загрузить утилиту можно с веб-сайта <http://speak-freely.sourceforge.net/>.

- **PGPfone** – первоначально была написана под Apple Macintosh, а уже впоследствии портирована в Windows. Написанная Филом Циммерманом и Уилом Прайсом, с приобретением PGP Incorporated компанией Network Associates (NAI) в 1997 году эта утилита превратилась в коммерческий продукт. Однако, поскольку компании NAI не удалось продвинуть этот продукт на рынок, в конце концов Циммерман выложил исходные коды программы на всеобщее обозрение. Найти программу можно в Интернете по адресу [www.pgp.org/products/pgpfone/](http://www.pgp.org/products/pgpfone/).

## Шпионский инструментарий: декодеры DTMF

Жизненно необходимым инструментом для людей, занимающихся телефонным шпионажем, являются декодеры DTMF (Dual Tone Multi-Frequency – тональный набор с разделением частот). Как известно, при нажатии любой цифровой клавиши на панели телефона, работающего в тоновом режиме, генерируется уникальный тон. Декодер DTMF анализирует этот тон и записывает цифровую клавишу, которая была нажата.

Если у вас имеется аудиозапись нажатия последовательности цифровых клавиш, вы можете обработать ее в декодере DTMF, чтобы узнать набранный номер. Это может пригодиться для выяснения телефонных номеров, по которым звонил объект, и паролей к службам голосовой почты.

В сети Интернет существует масса доступного недорогого коммерческого аппаратного и программного обеспечения для DTMF-наблюдения. За более подробной информацией обращайтесь к поисковым серверам (задавая в строке поиска «DTMF decoder»).

## ТЕЛЕФОННЫЙ ШПИОНАЖ

Телефонный шпионаж подразумевает получение информации не только из телефонных разговоров. Обладая физическим доступом к телефону, вы можете собирать сведения из следующих источников:

- **Определители номера.** Во время ответа на звонок вы можете видеть номер телефона звонящего и, если это было предварительно задано пользователем, даже его имя. Автономные либо встроенные определители номера очень удобны тем, что позволяют сохранять журнал входящих звонков (принятые и непринятые вызовы). Поэтому, если вы не будете своевременно удалять номера входящих звонков из памяти определителя номера,

любое лицо, имеющее доступ к вашему телефону, сможет уз-нать, кто и когда вам звонил. (Кстати, существует множество способов обмануть определитель номера. На сайте [www.artof-hacking.com](http://www.artof-hacking.com) вы можете найти немало информации по этому вопросу.)

- **Последний набранный номер.** Во многих телефонах существует функция повтора последнего набранного номера. Это очень удобно, когда возникает необходимость дозвониться на занятый телефонный номер, поскольку избавляет вас от повторного набора одних и тех же цифр, однако, если к вашему телефону получит физический доступ шпион, он легко сможет выяснить, кому вы звонили последнему. К тому же при тональном наборе номера сигнал может быть декодирован при помощи устройства DTMF, помещенного вблизи телефонной трубки.
- **Функции быстрого набора.** Предварительно заданные телефонные номера нужны для быстрого вызова людей, с которыми вы чаще всего общаетесь. Зная эти номера, шпион может определить ваш круг делового и личного общения.

## Сотовые телефоны

Сотовые телефоны еще менее надежны в плане безопасности, чем обычные настольные телефоны. Поскольку сотовые телефоны передают сигнал в виде радиоволн, при помощи соответствующего оборудования вы можете перехватывать телефонные переговоры непосредственно из радиоэфира, что не требует ни подключения к телефонному проводу, ни организации тайного проникновения для установки «жучка». К тому же такую пассивную разновидность шпионажа чрезвычайно трудно обнаружить и предотвратить.

Перед тем как начать обсуждение темы использования сотовых телефонов в целях шпионажа, важно сформулировать для себя общее понимание принципов работы данной технологии.

## ТЕХНОЛОГИЯ СОТОВОЙ СВЯЗИ

Сотовыми телефоны называются потому, что их работа основана на динамическом позиционировании внутри одной из совокупности взаимосвязанных «сот». Каждая «сота» имеет базовую станцию (здание с соответствующим радиооборудованием и антенной), обеспечивающую определенный радиус покрытия.

Управление «сotами» осуществляется из центрального телефонного узла. Этот узел отвечает за все телефонные переговоры по мобильной связи и управляет базовыми станциями в регионе.

Каждый сотовый телефон (телефонная трубка) имеет электронный серийный номер (ESN) и мобильный идентификационный номер (MIN), которые уникально идентифицируют данный телефон. Когда ваш телефон

находится во включенном состоянии, эта информация, как и другие сведения, необходимые для аутентификации, проверочная информация и данные о местонахождении, передаются между вашим телефоном и базовой станцией, в зоне покрытия которой вы находитесь в данный момент, а также центральным офисом. Если во время разговора вы подходите к границе покрытия, базовая станция анализирует мощность сигнала от телефона, и если сигнал у соседней базовой станции становится сильнее, то при помощи центрального телефонного узла ваш телефон перенастраивается на работу с другой базовой станцией.

Большинство людей думает, что все сотовые телефоны работают одинаково, хотя на практике применяются совершенно разные системы сотовой связи, использующие различные технологии и протоколы передачи данных. Наибольшей популярностью на сегодняшний день пользуются следующие стандарты:

- **AMPS** (Advanced Mobile Phone System – Усовершенствованная система мобильной радиотелефонной связи) – этот стандарт использовался в первых мобильных телефонах. Для него характерна передача данных в аналоговом виде, в результате чего разговоры легко могут быть подслушаны при помощи обычного полицейского сканера радиочастот. В 1990-х годах правительство США запретило производителям в США выпускать радиосканеры для частотного диапазона, используемого в сотовой связи. Тем не менее в сети Интернет вы можете найти детальные описания и схемы переделки таких сканеров для прослушивания заблокированного диапазона частот. Следует учитывать, что хотя аналоговые переговоры APMS могут быть легко перехвачены при помощи модифицированных сканеров, при использовании цифровой связи это становится невозможным.
- **TDMA (IS-136)**. Телефоны, работающие по стандарту множественного доступа с временным разделением (Time Division Multiple Access), используют цифровое вещание в диапазоне, пересекающемся с частотами, используемыми чрезмерно любопытными радиолюбителями. Прослушивать мобильные переговоры стандарта TDMA вы можете при помощи промышленного оборудования для тестирования TDMA-телефонов.
- **GSM**. Как и в случае с телефонами стандарта TDMA, для прослушивания мобильных телефонов, работающих с глобальной системой мобильной связи\*, вам понадобится специальное тестовое оборудование. GSM-телефоны обеспечивают дополнительную защиту путем шифрования передаваемых данных по алгоритму A5.

---

\* Global System for Mobile communications – стандарт сотовой связи в Европе. – Прим. перев.

- **CDMA (IS-95 или 1xRTT).** В стандарте CDMA (Code Division Multiple Access – Множественный доступ с кодовым разделением каналов) используется цифровая передача сигнала в широком диапазоне частот, что чрезвычайно осложняет задачу отслеживания звонков. В некоторых телефонах, таких как, например, Qualcomm QSec-800, аттестованном Управлением национальной безопасности, используется встроенная система стойкого шифрования, покрытие, соответствующие стандартам TEMPEST, и конструктив, защищающий от несанкционированного вскрытия (посетите веб-сайт [www.qualcomm.com/gov-sys/pdf/qsec800datasheet.pdf](http://www.qualcomm.com/gov-sys/pdf/qsec800datasheet.pdf)).



Более подробно о стандартах TEMPEST и электромагнитном шпионаже вы прочтете в главе 13.

Как бы там ни было, все существующие технологии мобильной связи, в той или иной мере подвержены прослушиванию. Звонки по сотовому телефону могут быть перехвачены в режиме реального времени в случае наблюдения за определенной частотой, с последующим выполнением демодуляции сигнала. Если вы работаете на правоохранительные органы и располагаете судебным ордером, то вы можете установить следящее оборудование непосредственно на центральном телефонном узле.

Если вы полагаете, что у кого-то достаточно ресурсов для организации против вас операции по шпионажу, ни в коем случае не считайте разговоры по мобильному телефону безопасными. Старый аналоговый сотовый телефон означает, что почти наверняка ваши переговоры прослушиваются целым рядом окрестных энтузиастов-радиолюбителей при помощи сканеров. Использование цифрового телефона хотя и защищает вас от наблюдения с помощью сканеров радиочастот, но ваши переговоры все равно могут быть перехвачены представителями правоохранительных органов или правительства – теми, кто имеет соответствующую подготовку и техническое оборудование.

Говоря о контрмерах, следует заметить, что в распоряжении правительства и военных имеются некоторые хитрые технологии обеспечения безопасности беспроводной связи и устройства, предназначенные для этой цели, о которых вы можете прочитать на сайте военных информационных технологий [www.mit-kmi.com](http://www.mit-kmi.com). Однако если вы не работаете на правительство, но при этом пользуетесь мобильной связью стандарта GSM, советуем вам подумать над приобретением немецкого телефона TopSec, в котором реализована устойчивая система шифрования. Сам телефон базируется на популярной модели Siemens S35i. Однако не надейтесь приобрести этот телефон бесплатно при подключении к оператору мобильной связи – вам придется выложить за него почти 3000 долларов, а ведь для безопасного общения с другим человеком вам понадобится, по крайней мере, два телефона.



Настольные беспроводные телефоны (называемые иногда радиотелефонами) не менее уязвимы для телефонного шпионажа. Во многих моделях используется передача аналогового сигнала, который может быть перехвачен при помощи радиосканера. В США разрешено производство радиосканеров, предназначенных для частот, используемых беспроводными телефонами (и так называемыми радионянями), хотя прослушивание телефонных переговоров с помощью таких устройств все равно считается незаконным. Таким образом, беспроводной телефон, работающий в диапазоне 2,4 ГГц еще более небезопасен в плане прослушивания, чем обычный проводной настольный аппарат.

## Тактика: прослушивание сотовых телефонов и шифрование

Представители компаний мобильной связи любят утверждать, что цифровые телефоны не так-то легко подслушать. По сравнению с более старыми аналоговыми телефонами это, конечно, справедливо, но в принципе шпиону не нужны денежные ресурсы, которыми располагает правительство, или судебный ордер, чтобы организовать прослушивание вашего мобильного телефона.

Предположим, у вашей жертвы имеется телефон стандарта GSM, переговоры по которому вас очень сильно интересуют (но вы не работаете в правоохранительных органах, имеющих доступ к промышленным устройствам мониторинга). Для начала вам понадобится «набор для цифрового тестирования радиоэфира». Это диагностическое оборудование, производимое такими компаниями, как Agilent и Racal Instruments, предназначено специально для разрешения проблем с мобильными телефонами и сетями. Подобные устройства позволяют вести наблюдение за голосовым и SMS-трафиком, а стоят не более 10 000 долларов.

Но даже при условии, что вы сможете перехватить цифровой сигнал, что вы будете делать с шифрованием передаваемой информации? К счастью для перехватчика, серия «A» алгоритмов шифрования, используемая для шифрования переговоров стандарта GSM, со временем показала свою низкую надежность. Перечислим обнаруженные слабые места в шифровании голосовых данных, о которых известно с конца 1990-х годов:

- **A5/1.** Если вам удастся записать первые две минуты разговора, использовавшийся при шифровании ключ A5/1 может быть раскрыт менее чем за секунду при помощи обычного настольного ПК.

- **A5/2.** Алгоритм A5/2 еще менее надежен, чем предыдущий алгоритм для шифрования голосовых данных, и легко может быть взломан в режиме реального времени.
- **A3 и A8.** A3 – алгоритм аутентификации, разработанный для предотвращения телефонного клонирования, и A8 – алгоритм генерации ключей для обеспечения безопасности переговоров. Оба могут быть взломаны в течение 8 часов.

В июле 2002 года был представлен новый алгоритм шифрования мобильной связи стандарта GSM – A5/3. Что ж, время покажет, насколько надежной окажется новая схема шифрования для безопасности мобильной связи.

Ходят слухи, что государственные разведывательные управление по обе стороны океана специально поддерживают шифрование мобильной связи на уровне, достаточном для того, чтобы гражданам было затруднительно подслушать друг друга, и в то же время недостаточном для того, чтобы защититься от прослушивания со стороны правоохранительных органов и правительства.

## ОПРЕДЕЛЕНИЕ ВАШЕГО МЕСТОПОЛОЖЕНИЯ

Итак, вас могут подслушать. Но это еще не самое худшее: как быть с тем, что при помощи мобильного телефона можно определить ваше местоположение? Для того чтобы вычислить, где вы находитесь, достаточно измерить время, требуемое на прохождение сигнала от вас до ближайших базовых станций, либо определить направление сигнала при помощи двух соседних базовых станций и затем, методом триангуляции, вычислить координаты телефона. Данная методика уже применялась для поиска и спасения потерявшихся во время снежных бурь автомобилистов. Кроме того, эта же технология используется правоохранительными органами и в ходе уголовных расследований. В 1995 году ФБР воспользовалось устройством под названием Triggerfish, произведенным компанией Harris Communications, для того чтобы выследить самого разыскиваемого на тот момент взломщика Кэвина Митника по сделанному им звонку с мобильного телефона из своих апартаментов в г. Роли, штат Северная Каролина.

В ближайшее время задача отслеживания местоположения мобильных телефонов для правительства и правоохранительных органов должна будет упроститься. Если вы звоните в службу спасения 911 со стационарного телефона, диспетчер сразу видит адрес, с которого вы звоните. Федеральная комиссия по средствам связи (FCC) готовит новую систему под названием Enhanced 911 (E-911), внедрение которой в системы мобильной связи должно будет произойти в 2005 году. В новые мобильные телефоны будут встраиваться устройства GPS, а в существующих системах

мобильной связи начнут применяться сложные триангуляционные методы расчета для определения местоположения телефона. Для методов триангуляции, основанных на получении информации от сети базовых станций, в соответствии с пересмотренными правилами FCC, погрешность определения координат на земной поверхности не должна будет превышать 100 метров в 67% случаев и 300 метров в 95% от общего количества случаев. Местоположение владельцев мобильных телефонов со встроенным устройствами GPS, которые характеризуются большей точностью и надежностью, можно будет вычислить с точностью до 50 метров в 67% случаев и со 150-метровой точностью в 95% случаев.

## ДОКАЗАТЕЛЬСТВА, ХРАНИМЫЕ НА МОБИЛЬНЫХ ТЕЛЕФОНАХ

Заполучив в свои руки сотовый телефон, вы можете собрать много полезной информации и доказательств различного типа. (Если вы работник полиции и в результате задержания изъяли мобильный телефон подозреваемого, не отдавайте его в хранилище доказательств на длительное время. На некоторых моделях телефонов при полной разрядке батареи теряется адресная книга и другие хранимые на телефоне данные.)

Любой владелец мобильного телефона, хоть немного смыслящий в вопросах безопасности, обязательно использует блокировку телефона при помощи пин-кода. Конечно, это зависит от модели телефона, но обычно такая защита вызывает лишь небольшую заминку в действиях опытного шпиона. В сети Интернет можно найти множество информационных источников по способам разблокирования популярных моделей мобильных телефонов: шпиону в этом случае нужно будет только набрать защищую в памяти запасную последовательность цифр для разблокировки телефона (чтобы убедиться, насколько это просто, посетите веб-сайт [www.cellphoneshack.com](http://www.cellphoneshack.com)).

После разблокировки телефона вы можете проанализировать следующую информацию:

- **Адресная книга.** В большинстве мобильных телефонов имеется адресная книга для хранения телефонных номеров. Это чрезвычайно удобно для быстрого набора номеров друзей, членов семьи, деловых партнеров, к тому же вам не придется носить за собой бумажную записную книжку. Офицеры полиции просто обожают адресные книги в мобильных телефонах, поскольку, получив судебный ордер, они могут изучать содержимое этой книги, сопоставляя абонентов с соучастниками подозреваемого. Это средство предоставляет широкие возможности в плане установки взаимосвязей в криминальных расследованиях.
- **Журнал звонков.** Многие телефоны позволяют хранить журнал входящих и исходящих звонков, включая номер телефона абонента, а также дату и время вызова.
- **Интернет.** В последние годы мобильные телефоны начали интегрировать в себя функции отправки электронной почты и

посещения Интернета. Таким образом, те же разновидности доказательств, которые могут быть получены с обычного компьютера, теперь можно встретить и на мобильном телефоне с поддержкой Интернета. А наиболее ценным источником доказательств можно считать сохраненные в памяти телефона сообщения электронной почты и SMS.

- **Функции КПК.** В настоящее время наблюдается тенденция появления в мобильных телефонах многих функций, характерных для карманных ПК. В этом случае источником информации могут послужить встроенные календари, организеры, адресные книги и т. д.

## Автоответчики и голосовая почта

Сегодня автоответчики и услуги голосовой почты превратились в важную часть нашей деловой и личной жизни. Неудивительно, что эти устройства и службы занимают важные позиции в списке потенциальных целей шпиона, поскольку они могут содержать весьма ценную информацию, и в то же время сами пользователи часто не принимают их в качестве серьезного источника угрозы.

Практически все системы голосовой почты и автоответчики разрешают пользователям проверять содержимое пришедших сообщений удаленно. Если шпион сможет узнать пароль пользователя для удаленного подключения, он будет иметь возможность прослушивать и выборочно стирать оставленные жертве сообщения.

Получить доступ к системам голосовой почты и автоответчикам можно следующими способами:

- **«Лобовая атака».** Данная разновидность атаки подразумевает перебор всех возможных комбинаций цифр, из которых может состоять пароль. Обычный автоответчик с паролем из трех цифр заставит вас выбирать из 1000 возможных комбинаций. Коммерческие системы голосовой почты имеют более длинные пароли (до 15 цифр). Очевидно, что атака «в лоб» может занять много времени. Однако в помощь шпиону существуют различные устройства и сценарии, позволяющие автоматизировать процесс подбора пароля, так что вам не потребуется набирать возможные пароли вручную на клавиатуре.
- **Атака при помощи словаря.** В рамках этой атаки перебираются наиболее вероятные цифровые комбинации (например: 12345, последовательность цифр на клавиатуре, составляющая букву «U» или «Z», цифры в почтовом индексе, даты дней рождения, юбилеев либо коды социального страхования).
- **Использование приемов социотехники.** Вы можете просто спросить пароль (придумав предварительно убедительную историю, почему это так необходимо).

- **Посредством физического доступа.** Если шпион сможет получить доступ в помещение, где находится телефон либо автоответчик, он может поискать пароль, записанный где-то рядом с устройством.

## АВТООТВЕТЧИКИ

Обычные автоответчики, используемые дома и на малых предприятиях, служат для шпиона легкой добычей, поскольку чаще всего в них применяются пароли, состоящие из двух-трех цифр, что делает использование таких устройств делом ненадежным. Пароль, состоящий из двух цифр, можно подобрать за пять минут. А, получив удаленный доступ к вашему автоответчику, шпион без труда сможет прослушивать либо удалять любые оставленные вам сообщения. Кроме того, у некоторых моделей имеются функции включения микрофона, с помощью которой можно услышать все, что происходит в комнате\*. Причем некоторые автоответчики ожидают только ввода корректной последовательности цифр, а не определенного пароля. К примеру, чтобы подобрать пароль из двух цифр, для подобного автоответчика достаточно набрать одну из следующих цифровых последовательностей:

00112233445566778899135790246803692581471593704948382726160517395062  
840852963074197531864209876543210  
12345678987654321257924686429731474193366994488552277539596372582838  
491817161511026203040506070809001

## ГОЛОСОВАЯ ПОЧТА

Услуги голосовой почты, предоставляемые телефонными компаниями, являются такими же незащищенными, как и автоответчики. Хотя в голосовой почте и применяются дополнительные меры безопасности, такие как более длинный пароль и блокировка учетной записи после нескольких попыток неправильного ввода пароля, некоторые из существующих функций предоставляют шпиону грандиозные возможности по получению доступа к информации. Прямые телефонные номера, которые может применять пользователь для получения удаленного доступа к информации (без необходимости набирать добавочный номер), предоставляют шпиону возможность использовать один и тот же телефонный номер для получения доступа ко многим почтовым ящикам. Кроме того, корпоративные системы голосовой почты часто связаны с внутриофисными АТС, поэтому, проникнув в систему, шпион может воспользоваться офисной АТС, дабы не разглашать свой истинный номер.

Как правило, каждая система голосовой почты обладает своими уникальными характеристиками (например, приветствием), позволяющими определить, с каким типом системы работает пользователь, и соответст-

\* Даже когда трубка лежит на рычаге. – *Прим. перев.*

но воспользоваться при этом известными слабыми местами данной системы (команды и пароли по умолчанию для некоторых популярных служб голосовой почты можно найти в Интернете).

Теперь поговорим о контрмерах. Для того чтобы уменьшить шансы злоумышленников на получение несанкционированного доступа к вашей информации, хранимой на системах голосовой почты либо автоответчиках, вам необходимо придерживаться следующих простых правил:

- Выбирать цифровой пароль максимально возможной длины, который может быть задан на данном устройстве или в данном сервисе.
- Если такая функция поддерживается системой голосовой почты, настройте систему на блокировку подключения после определенного количества неудачных попыток.
- Никогда не храните на автоответчике либо в службе голосовой почты конфиденциальную информацию. Это означает, что не следует передавать сообщения с конфиденциальной информацией при помощи услуг голосовой почты, а при получении таких сообщений от ваших коллег не стоит хранить эту информацию в системе.



Стефан Барнс (известный также как «M4phr1k») из консалтинговой фирмы в сфере безопасности Foundstone собрал коллекцию статей по проникновению и защите от проникновения для внутриофисных АТС и безопасности услуг голосовой почты на своей веб-странице по адресу [www.m4phr1k.com](http://www.m4phr1k.com). Еще два интересных документа по безопасности голосовой почты, написанных Джо Грандом (известным также под псевдонимом Kingpin) можно найти на сайте компании @Stake. Первый из них, под названием «Советы по безопасности автоответчиков», размещен на вебстранице [www.atstake.com/research/advisories/1998/ansmach.txt](http://www.atstake.com/research/advisories/1998/ansmach.txt), второй, называющийся «Взлом систем голосовой почты», ищите по адресу [www.atstake.com/research/reports/acrobat/compromising\\_voice\\_messaging.pdf](http://www.atstake.com/research/reports/acrobat/compromising_voice_messaging.pdf).

## Пейджеры

Хотя пейджеры в ближайшее время, судя по всему, ожидает судьба динозавров, поскольку им на смену приходят мобильные телефоны с поддержкой услуг SMS и электронной почты, однако даже пейджеры иногда все еще используют в качестве источника информации и доказательств.

Традиционные пейджеры позволяют только принимать сообщения, тогда как в более новых моделях, таких как Research in Motion (RIM) BlackBerry, поддерживаются функции и приема, и отправки. Как и у других средств связи, перехватить пейджерные данные можно непосредственно из беспроводного трафика либо прочитать сохраненные сообщения, заполучив само устройство.

Правоохранительные органы должны иметь судебный ордер, предъявляемый компании по предоставлению услуг связи, чтобы прочитать текст сообщений, которые были отправлены определенной жертве, шпионы же могут перехватывать трафик при помощи недорогого аппаратного и программного обеспечения. (Несанкционированный перехват пейджерных сообщений карается несколькими федеральными и окружными законами, но, как и в случае с прослушивание переговоров по беспроводным средствам связи, обнаружить такие нарушения из-за пассивности перехвата чрезвычайно трудно.)

По сути, пейджер представляет собой радиоприемник, принимающий сообщения, поступающие от компании по предоставлению услуг связи. Эти сообщения передаются в аналоговом виде при помощи протокола POCSAG (Post Office Code Standardization Advisory Group) или фирменного протокола Flex компании Motorola. Каждый пейджер обладает электронным идентификационным кодом, длина которого обычно составляет 7...8 символов. Пейджер постоянно следит за поступающим потоком сообщений, и как только обнаружит в нем сообщение, адресованное абоненту с данным идентификационным номером, пейджер декодирует информацию в буквенно-цифровой вид и отображает ее на своем небольшом LCD-дисплее.

Передаваемые в аналоговом виде пейджерные сообщения не шифруются, поэтому если вы сможете декодировать сам протокол, то без труда прочтете послание (исключение составляют пейджеры RIM BlackBerry: в них используется цифровой протокол передачи данных, поддерживающий шифрование DES с тройной длиной ключа). Для прослушивания традиционных пейджеров вам понадобится:

- **ПК под управлением Windows.**
- **Радиосканер для перехвата сигнала в диапазоне частот, используемых пейджерами.** Вам не понадобится никакого специфического оборудования – вполне достаточно будет обычного полицейского сканера. Подобный радиосканер, состоящий из селекторной микросхемы, позволяет отфильтровывать аудиосигнал для прослушивания его через наушники или динамик. К сожалению, отфильтрованный аудиосигнал не подходит для декодирования пейджерных сообщений. Вам придется модифицировать сканер, удалив селекторную микросхему, чтобы разрешить передачу интерфейсному устройству необработанных данных. (Можно найти схемы переделки для большинства моделей сканеров, ну а если вы не сильны в работе паяльником, то вам могут сделать это на заказ.)
- **Интерфейс частотной манипуляции.** Для того чтобы отобразить текстовое сообщение на дисплее, пейджер должен преобразовать аналоговый сигнал в цифровой вид. Это осуществляется через специальный интерфейс частотной манипуляции. В таком случае, входные данные с селекторной микросхемы сканера

отправляются на интерфейс частотной манипуляции, где аудио-сигнал преобразуется в цифровую форму. (Существует программное обеспечение, которое позволяет выполнять декодирование сообщений без дополнительного интерфейсного оборудования – при помощи обычной звуковой карты. Тем не менее если вам необходимо проводить серьезный мониторинг трафика, то без такого устройства вам не обойтись.)

- **Программное обеспечение.** Программное обеспечение принимает данные от интерфейсного устройства частотной манипуляции и отображает их на компьютере. Некоторые бесплатные и условно-бесплатные утилиты позволяют перехватывать сообщения, предназначенные конкретному абоненту, имеющие отправленные время и дату отправки, и сохранять все полученные сообщения в текстовый файл. Среди наиболее популярных утилит для работы с пейджерами (доступных в сети Интернет) можно назвать PDW и WinFlex.

При помощи специального программного обеспечения можно создать «клон» пейджера, на который будут приходить все те же сообщения, которые были отправлены настоящему абоненту. Компании по обслуживанию пейджеров предоставляют подобные устройства представителям правоохранительных органов, обладающим ордером на перехват сообщений подозреваемого. (Промышленные и самодельные устройства для перехвата пейджерных сообщений могут использоваться только при наличии соответствующего судебного ордера.)

Помните о том, что переданные на пейджер сообщения могут быть также перехвачены непосредственно при их отправке. Если телефон, с которого было отправлено сообщение, прослушивается, то можно выполнить отбор звонков на номер пейджера. Если же сообщение было отправлено с веб-сайта либо посредством услуг электронной почты, можно также определить адрес отправителя.

Наилучшая контратака в плане защиты информации, передаваемой посредством пейджера, – понимать, что конфиденциальность обмена информацией в данной службе не гарантирована. Вы можете, конечно, обмануть следящих за вами шпионов, используя условные коды (наркодельцы делают это постоянно). Однако подстановочные шифры достаточно легко взломать, впрочем, как и подобрать более сложные цифровые коды путем анализа трафика (при условии достаточного объема передаваемой информации). Вероятно, наиболее эффективный прием для защиты передаваемых на пейджер сообщений – использование карманного ПК для запуска утилит со стойкими алгоритмами шифрования, такими как IDEA, 3DES или AES, для шифрования сообщений перед их отправкой. Получатель же, в свою очередь, приняв зашифрованное сообщение, вводит его в КПК и затем расшифровывает при помощи предварительно заданного пароля. Хотя этот прием требует времени и не лишен недостатков, но при условии использования надежного пароля данный подход можно считать весьма эффективным.



В Интернете можно найти массу информации по декодированию пейджерных сообщений. Задайте на каком-нибудь поисковом сервере (наш любимый поисковик – Google) строчку «POCSAG decoder» – и вперед. Для начинающих советуем посетить веб-сайт Майка ZL3TMB, на котором размещен список программ для декодирования пейджерных сообщений (<http://homepages.ihug.co.nz/~Sbarnes/pocsag/software.html>). А если у вас имеются технические наклонности, зайдите на сайт Либора Улсака, где можно найти электронные схемы самодельного декодера пейджерных сообщений ([www.applet.cz/~ulcak/4\\_level\\_fsk\\_interface.htm](http://www.applet.cz/~ulcak/4_level_fsk_interface.htm)).

Помимо перехвата сообщений из эфира вы можете извлечь полезную информацию, имея физический доступ к устройству:

- содержимое не удаленных и сохранных сообщений;
- когда и откуда были отправлены хранимые сообщения (с электронного почтового ящика, веб-сайта или телефона);
- цифровые данные (номера телефонов и коды).

Проводить изучение современных пейджеров, поддерживающих двухстороннюю связь, например того же RIM BlackBerry (который, по сути, представляет собой гибрид между пейджером и беспроводным КПК), намного сложнее. Майкл Бернет написал на эту тему отличную статью под названием «Судебная экспертиза беспроводных устройств RIM (BlackBerry)» (ее можно найти по адресу [www.rh-law.com/ediscovery/Blackberry.pdf](http://www.rh-law.com/ediscovery/Blackberry.pdf)), в которой обсуждаются некоторые проблемы и технологии сбора доказательств с устройства BlackBerry.

## Персональные электронные устройства

Если с компьютерным шпионажем и проведением судебных экспертиз компьютерной техники все было более менее понятно – вы ищете информацию на жестком и гибких дисках компьютера и любых других находящихся рядом цифровых носителях информации, то с появлением персональных электронных устройств ситуация осложнилась. Популярные сегодня КПК требуют иного подхода к поиску информации. Кроме того, теперь данные могут быть спрятаны в таких электронных устройствах, которые изначально не предназначались для этих целей (а использовались для хранения фотографий, проигрывания музыкальных файлов либо записи телевизионных шоу). Технически грамотные пользователи могут записать секретную информацию на одном из этих устройств, что может пройти незамеченным во время обыска. В результате перед лицом правоохранительных органов и судебных экспертов встает целый ряд трудно решаемых задач,

требующих от них углубления своих знаний и совершенствования технических навыков, причем не только в плане компьютерной техники. Необходимо также разрабатывать новые средства и способы экспертного изучения цифровых доказательств, собранных с различных персональных электронных устройств.

## КПК

Необычайную популярность в последнее время завоевали карманные ПК (КПК). Это обусловлено их широкими возможностями в плане хранения информации: контактные данные, расписание встреч, финансовые записи, таблицы и текстовые документы, которые вы всегда можете взять с собой. По самым приблизительным оценкам, за последние пять лет было продано более 20 000 000 КПК.

Как и следовало ожидать, КПК превратились в любимый объект охоты шпионов. Благодаря своему малому размеру подобные устройства могут быть легко потеряны или украдены. В отчете Gartner Group за январь 2002 года сообщалось о пропаже за предшествующий год более чем 250 000 КПК и мобильных телефонов только в аэропортах. Опубликованное в конце 2001 года исследование компании Anderson Consulting содержит статистику, согласно которой от 10 до 15% всех мобильных телефонов и КПК, в конце концов, оказываются украденными или потерянными. Возможно, вы считаете, что устройство за несколько сотен долларов не является такой уж крупной потерей, однако, по оценкам той же компании, стоимость информации на каждом из таких КПК оценивается в пределах от \$10 000 до \$20 000. (Если вы являетесь владельцем КПК, попробуйте сами оценить ценность такой информации, как имена, адреса, телефоны, расписания встреч, архив электронных сообщений и другие файлы на устройстве.)

Давайте представим ситуацию, в которой некто оказался более заинтересован в информации, которая хранится на КПК, чем в самом устройстве. Доступ к хранимой на нем информации может быть получен несколькими способами:

- **В результате несоблюдения пользователем мер безопасности.** В большинстве КПК имеется функция аутентификации пользователя при помощи пароля для защиты данных, однако многие владельцы КПК не используют эту возможность, что делает хранимую на нем информацию легкой добычей шпиона.
- **Благодаря низкой надежности шифрования.** Даже при использовании встроенной системы аутентификации ее надежность оставляет желать лучшего. К примеру, документы, отмеченные как «private» в Palm OS на самом деле шифруются, как оказывается, при помощи простейшего алгоритма XOR, который можно взломать в течение нескольких секунд (см. рекомендации на веб-сайте [www.atstake.com/research/advisories/2000/a092600-1.txt](http://www.atstake.com/research/advisories/2000/a092600-1.txt)).

- **С использованием уязвимых мест процесса синхронизации.** Синхронизацией называется процесс обмена данными между настольным и карманным ПК. Обмен данными может осуществляться при помощи кабеля либо специального устройства, подключаемого к параллельному порту или USB. В процессе синхронизации на жестком диске обычно создается резервная копия данных с КПК. Таким образом, любое лицо, имеющее доступ к компьютеру, с помощью которого проводилась синхронизация, может изучить данные (и даже выяснить пароль к КПК) либо загрузить информацию с компьютера на похожую модель КПК. Доступ к КПК может быть получен удаленно, через инфракрасный порт. Компания @Stake разработала утилиту под названием NotSync, предназначенную для КПК Palm ([www.atstake.com/research/advisories/2000/notsync.zip](http://www.atstake.com/research/advisories/2000/notsync.zip)), которая активизирует инфракрасный порт КПК и может обмениваться по нему информацией с другим КПК, заставляя второй КПК думать, что он обменивается информацией с настольным компьютером. Помимо всего прочего, эта утилита позволяет перехватывать пароль целевого КПК для его последующего декодирования.
- **Путем сохранения дампа памяти в файл.** Обладая физическим доступом к КПК, сравнительно легко можно сохранить дамп всей памяти КПК на жестком диске компьютера, после чего заняться поиском и анализом интересующей информации. Дамп памяти КПК под управлением Palm OS можно сохранить на жесткий диск компьютера при помощи такой утилиты, как pdd (<http://www.securiteam.com/tools/6V00K0U36C.html>).

Первичной контрмерой для защиты вашего КПК является осведомленность об угрозе. Оцените важность информации, хранимой на вашем КПК, и примите соответствующие меры против его утери или кражи. Стандартные средства безопасности, встроенные в КПК, недостаточны для обеспечения должной защиты от шпионов. Для сохранности информации рекомендуем воспользоваться утилитами шифрования сторонних разработчиков. Среди доступных утилит можно перечислить следующие:

- **PDA Defense.** Утилита, предназначенная для КПК Palm и Pocket PC, стоимостью \$29,95, которую можно заказать на сайте [www.pdadefense.com](http://www.pdadefense.com).
- **Sentry 2020.** Программа для Pocket PC стоимостью \$49,95. Подробности на сайте [www.softwinter.com/sentry\\_ce.html](http://www.softwinter.com/sentry_ce.html).
- **OnlyMe.** Приложение для обеспечения безопасности КПК Palm. Заказать его по цене в \$9,95 можно на веб-сайте [www.transzoa.com](http://www.transzoa.com).
- **TealLock.** Программа защиты информации для Palm-совместимых КПК. Стоимость персональной лицензии на нее составляет \$16,95, корпоративной – \$21,95. Подробности на сайте [www.teal-point.com/softlock.htm](http://www.teal-point.com/softlock.htm).



К концу 2002 года КПК Palm занимали лидирующую позицию в плане продаж (65% продаваемых в Соединенных Штатах карманных ПК), и хотя Pocket PC от компании Microsoft постепенно догоняет лидера, на сегодняшний день вероятность того, что вам придется иметь дело с некоторой разновидностью системы Palm, намного выше. Шпионам и судебным экспертам, которых интересуют сведения по системам Palm, советуем для начала почитать статью «pdd: запись содержимого памяти и судебная экспертиза КПК Palm OS», написанную Джо Грандом ([http://www.atstake.com/research/reports/acrobat/pdd\\_palm\\_forensics.pdf](http://www.atstake.com/research/reports/acrobat/pdd_palm_forensics.pdf)). Кроме того, обязательно посетите веб-сайт компании Paraben, являющейся разработчиком утилиты PDA Seizure, предназначеннной для изучения содержимого памяти Palm OS и Pocket PC. Стоимость программы составляет 199 долларов (компания также занимается продажей полного набора инструментов, включая кабели и адаптеры для сбора доказательств с 30 различных моделей КПК); более детальную информацию вы можете прочесть на сайте [www.paraben-forensics.com/pda.html](http://www.paraben-forensics.com/pda.html).

## Цифровые камеры

На современных цифровых камерах ценность могут представлять не только сделанные фотографии. В ходе изучения цифровой камеры в качестве улики не забывайте о следующих моментах:

- В файлы формата JPEG могут быть добавлены небольшие текстовые комментарии и даже аудиоинформация, поэтому некоторые камеры позволяют задавать комментарии после создания фотографии. Несмотря на ценность подобной информации (особенно в качестве доказательств), ее наличие нередко упускают из виду.
- Если на камере была включена функция добавления даты и времени, то эти значения можно будет увидеть на фотографиях. Кроме того, дату и время создания снимка можно узнать исходя из даты и времени создания файла изображения (если часы на камере были установлены правильно и не менялись преднамеренно).
- По умолчанию при присвоении имен цифровым фотографиям используется принцип сквозной нумерации. Поэтому, если файлы не переименовывались, вы можете выяснить, сколько всего фотографий было сделано и порядок съемки.
- Поскольку в цифровых фотокамерах изображения обычно записываются на флеш-картах, всегда следует проверять их содержимое, так как на них могут быть сохранены не только фотографии.

## Устройства GPS

Устройства GPS (Global Positioning System – Система глобального позиционирования) позволяют определить с помощью спутников ваши точные координаты на земной поверхности. Эта система, изначально разработанная для навигации пилотов, капитанов морских судов и путешественников, теперь применяется практически повсеместно: в автомобилях, КПК, ноутбуках и т. д. (Системы позиционирования помогают даже шпионам при определении места секретной встречи для обмена информацией. Осужденный за шпионаж Патрик Рэйган во время ареста имел при себе GPS Garmin III+.)

Если вы сами относитесь к владельцам устройства GPS, то по информации о точках маршрута и файлам журнала можно определить, где и когда вы были. За последние годы устройства GPS были значительно усовершенствованы – теперь они уменьшились в размерах, подешевели и могут работать автономно намного дольше. Функции «определения местоположения» получили распространение и в других цифровых устройствах, автомобилях, мобильной компьютерной технике. Каждый раз, когда информация о местоположении устройства передается в эфир либо сохраняется на самом устройстве, она может быть прочитана любым лицом, получившим доступ к устройству либо имеющим возможность перехватить информацию.

## Игровые приставки

Последнее поколение игровых приставок, таких как Microsoft Xbox и Sony PlayStation 2, прошло долгий путь развития со времен Pong и Atari 2600. Помимо более реалистичного звука и графики современные игровые приставки имеют встроенные жесткие диски и возможность подключения к сети Интернет. Вы можете заказать приставку PlayStation 2 с дополнительным набором периферии, включающим клавиатуру, программное обеспечение и жесткий диск, позволяющий превратить вашу игровую приставку в полноценный настольный компьютер под управлением Linux. Благодаря наличию расширенных возможностей и специального программного обеспечения, подобная приставка может быть приспособлена для хранения секретной информации, о присутствии которой никто даже и не догадается. (Советуем вам прочитать интересную статью на сайте [www.securityfocus.com/news/558](http://www.securityfocus.com/news/558), посвященную использованию игровых приставок в целях сетевого шпионажа.)

## MP3-плееры

Подобно игровым приставкам, в качестве хранилища конфиденциальной информации могут использоваться обычные портативные MP3-плееры. Флэш-память либо встроенные жесткие диски позволяют хранить от нескольких мегабайт до нескольких гигабайт музыки и любых других данных. Разыскивая улики, не упустите из виду устройство, имеющее вид

обычного радиоприемника или проигрывателя компакт-дисков. Если устройство поддерживает формат MP3, на нем может храниться не только музыка.

## Тактика: преследование при помощи GPS

Кони Адамс, жительница города Кеноша, штат Висконсин, долго не могла понять, что происходит. Куда бы она ни направлялась, за ней, как тень, следовал ее бывший бойфренд. Стоило ей оглянуться или посмотреть в зеркало заднего вида, и она видела его машину, едущую за ней по дороге на работу либо во время поездок по разным поручениям. Однажды он появился в баре, где она сама была в первый раз на свидании.

Занявшаяся расследованием этого дела полиция обнаружила, что ее бывший парень, Пол Сейдлер, установил устройство GPS в ее машине, между радиатором и печкой. При помощи этого прибора Сейдлер знал обо всех ее перемещениях. В январе 2003 года Сейдлер отказался признать себя виновным в таких уголовно наказуемых преступлениях, как преследование жертвы, проникновение со взломом, угрозу ее безопасности и нарушение общественного порядка.

Сейдлер использовал коммерческую систему от компании L.A.S. Systems ([www.landairsea.com](http://www.landairsea.com)). Оборудование стоимостью в \$695 позволяло передавать сигнал о местонахождении объекта по сети мобильной связи. С помощью данной системы вы могли отслеживать координаты объекта в режиме реального времени на карте города, отображаемой на экране вашего компьютера, либо получать сообщения о координатах объектах на свой мобильный телефон в виде коротких текстовых сообщений. Подобные AVL-устройства (Automatic Vehicle Location – средства автоматического определения местоположения транспортного средства) уже довольно давно используются для законного наблюдения за дальнобойщиками и в автопарках. В связи со снижением цен и увеличением доступности такого товара, приборы начали попадать в руки шпионов, детективов и одержимых преследователей.

Обнаружить устройства глобального позиционирования для автомобилистов легко, если, конечно, вам известно, где нужно искать. Поэтому, если вам необходимо действительно миниатюрное устройство, которое вы и сами бы не заметили, будучи на месте жертвы, обратитесь к военным документам по радиоразведке и радиопротиводействию. В декабрьском номере журнала Phrack за 2002 год (весьма занимательный журнал для электронных хакеров и взломщиков) была опубликована статья о том, как своими силами можно собрать постановщик помех для GPS. Схемы и инструкции по сборке можно найти на сайте [www.phrack.com/phrack/60/p60-0xd.txt](http://www.phrack.com/phrack/60/p60-0xd.txt).

## Цифровые видеомагнитофоны

Цифровые видеомагнитофоны, такие как TiVo, делают просмотр телевизора еще более приятным занятием, позволяя записывать несколько часов телевизионного эфира на жесткий диск. Вы можете записать целый сезон вашей любимой телепрограммы, не беспокоясь о видеопленке и т. п. (плюс возможность практически мгновенной перемотки рекламных роликов). В цифровых видеомагнитофонах TiVo в качестве операционной системы используется Linux, поэтому в принципе вы можете использовать недокументированные возможности видеомагнитофона в своих целях, включая копирование файлов с компьютера на видеомагнитофон (обратитесь к сборнику часто задаваемых вопросов по теме «Hacking the TiVo» – «Взлом TiVo» – на сайте [www.tivofaq.com/hack/faq.html](http://www.tivofaq.com/hack/faq.html)). Поскольку цифровой видеомагнитофон на вид очень похож на обычный видеомагнитофон или приемник спутниковых передач, шпион в поисках хранилищ цифровых данных может легко упустить его из виду.

## Заключение

Итак, очевидно, что компьютер является далеко не единственным устройством, которое может привлечь внимание шпиона, заинтересованного в поиске информации. Любое устройство, способное передавать или хранить информацию (в особенности в цифровом виде), так или иначе, уязвимо для атаки. Для повышения уровня безопасности проделайте следующие простые шаги:

1. Составьте список всех регулярно используемых вами устройств или служб, которые могут хранить или передавать данные.
2. Вычеркните из списка все устройства, кроме тех, на которых вы работаете с важной или конфиденциальной информацией.
3. Проанализируйте полученный список, разберитесь, в каком виде хранятся данные и как они передаются тем или иным устройством, насколько они защищены от подслушивания и может ли кто-нибудь удаленно или локально получить доступ к этой информации.
4. После определения наиболее уязвимых мест примите меры для повышения защищенности конфиденциальной информации (не забывайте о различии между возможной и вероятной угрозой и при этом постарайтесь не превратиться в параноика).

По мере того, как новые технологии все глубже проникают в повседневную личную и деловую жизнь человека (технологии удаленного доступа «IP

anywhere», приборы, позволяющие определять ваше местоположение, опознавательные знаки радиочастот, потребительские товары, связанные «внутренними сетями»), опасность шпионажа возрастает. Как только вы начинаете использовать новые технологии для хранения или передачи данных, помните, что функции обеспечения безопасности (даже если они присутствуют) далеки от совершенства на начальных этапах развития любой технологии, а за вашей спиной может находиться шпион, ожидающий возможности ухватиться за только что обнаруженное слабое место системы защиты.

## Глава 13

# Высший компьютерный шпионаж

«Они дали тебе номер и забрали у тебя имя».

Джонни Риверс, «Секретный агент»

В этой главе мы изучим некоторые приемы (в том числе и весьма экзотические) высшего пилотажа в сфере компьютерного шпионажа (простите за каламбур), которые активно применяются правительством, военными и другими организациями, задействованными в операциях по экономическому шпионажу высокого уровня (разумеется, поскольку вся эта информация изначально являлась секретной, иногда вам придется догадываться, о чем идет речь). Кроме того, мы обсудим ряд технологий, применяемых в сложных разведывательных операциях, реализация которых, однако, не требует больших денежных затрат. Мы рассмотрим ситуацию с точки зрения жертвы, и если вы не сделали ничего такого, что способно привлечь внимание могущественной и хорошо финансируемой организации, вам не придется ставить большинство из перечисленных ниже методов на первые места в списке возможных угроз.

## ТЕМPEST – перехват электромагнитного излучения

Кодовое слово TEMPEST используется для описания секретного перечня стандартов по ограничению побочного электромагнитного излучения, исходящего от электронного оборудования (многие устройства излучают электромагнитные волны, с помощью которых можно скомпрометировать данные, поэтому в отношении защитных мер шпионы и детективы используют термин «безопасность излучения»). Микросхемы, мониторы, принтеры и другие электронные устройства излучают электромагнитные волны в окружающее пространство либо передают побочные сигналы по проводникам, таким как, например, провода электросети или металлические трубы. В качестве примера можно привести помеху, появляющуюся на экране телевизора при включении какого-либо кухонного электроприбора.



Множество пользователей пытались придать термину TEMPEST осмысленную расшифровку (например, Transient ElectroMagnetic Pulse Emanation STandard – стандарт побочного импульсного электромагнитного излучения). Однако правительство заявило, что это кодовое слово, используемое для обозначения стандартов, было выбрано без какого-либо подтекста.

В 50-х годах XX века правительство было всерьез обеспокоено возможностью перехвата побочного электромагнитного излучения (ЭМИ), по которому могла быть восстановлена исходная информация. Конечно, вряд ли кому-то будет любопытно электромагнитное излучение от миксера, а вот электромагнитные импульсы, испускаемые устройствами шифрования, очень даже могут заинтересовать шпионов. Если записать это электромагнитное излучение, интерпретировать, а затем воссоздать на аналогичном устройстве, можно без проблем восстановить содержание зашифрованного послания. Исследования показали, что перехват электромагнитного излучения возможен и на расстоянии, ответом на что стала разработка программы стандартов TEMPEST.

Целью данной программы являлось введение стандартов, которые бы снизили шансы на «утечку» электромагнитного излучения от устройств, используемых для обработки, передачи либо хранения конфиденциальной и секретной информации. Для защиты от возможного мониторинга электромагнитного излучения правительственные организации и их подрядчики используют только те компьютеры и периферийное оборудование (принтеры, сканеры, накопители на магнитной ленте, мышь и т. п.), которые соответствует стандартам TEMPEST. Такая защита обычно организуется за счет установки экранирующего оборудования (иногда экранируется целая комната или даже здание) при помощи меди или других токопроводящих материалов.

В Соединенных Штатах консультации, тестирования по вопросам, связанным со стандартами TEMPEST, а также производство оборудования, сертифициированного на соответствие данному набору стандартов, представляет собой солидный бизнес с годовым оборотом около миллиарда долларов. (Экономисты, однако, не спешат с применением оборудования TEMPEST. Покупать подобные устройства – удовольствие не из дешевых, поэтому был разработан менее строгий стандарт под названием ZONE. Этот стандарт не обеспечивает такого уровня защиты, как TEMPEST, но и стоимость оборудования, соответствующего этому стандарту, ниже, причем он вполне подходит в ситуациях, когда вы работаете с данными не самого высшего уровня секретности.)

Соединенные Штаты (а если быть конкретнее, Управление национальной безопасности) и их союзники упрямо хранят молчание относительно стандартов TEMPEST, чтобы сохранить в тайне от своих противников способы обеспечения должного уровня защиты. Цель такой политики очевидна: противники не могут обеспечить необходимую степень защиты и тем облегчают задачу «хорошим» шпионам по наблюдению за ними. Тем

не менее после первого упоминания о комплексе правительственные стандартов TEMPEST на несекретном брифинге в 1965 году загнать джина назад в кувшин оказалось уже невозможно, и теперь иностранные правительства, имеющие лишь самое приблизительное представление об электромагнитном шпионаже, спешат применить целую серию базовых контрмер для защиты своей информации.

Один немаловажный момент, касающийся стандартов TEMPEST (по принципу «безопасность через непонятность»), связан с тем, что только правительственные организации и их подрядчики (как правило, в оборонной промышленности) получают выгоду от использования стандартов. Все остальные американские корпорации, не имеющие соответствующей категории допуска, не могут обеспечить полноценной защиты конфиденциальной информации от электромагнитного шпионажа. Поскольку развитие стандартов происходило на фоне холодной войны, экономическому шпионажу уделялось мало внимания, а из-за секретности стандартов TEMPEST крупные американские компании оставались уязвимыми к шпионским операциям со стороны иностранных разведывательных управлений.

Когда-то стандарты TEMPEST были окутаны мраком тайны, сейчас же ситуация проясняется. Проанализировав общедоступные источники информации, включая ряд документов, представленных широкой общественности на основе Закона о свободе информации, сообразительный гражданин может составить общую картину того, что собой представляют эти стандарты. Но, несмотря на множество доступных широкой общественности сведений, стандарты TEMPEST, которым скоро исполнится 50 лет, по-прежнему остаются засекреченными.

## Мониторинг побочного излучения: реальность или фантастика?

Если существуют такие стандарты по предотвращению перехвата побочного электромагнитного излучения, как TEMPEST, насколько же реальной является угроза расшифровки информации, полученной таким способом? Если вы интересовались компьютерной безопасностью либо хотя бы иногда смотрите боевики и шпионские фильмы, то вам должна показаться знакомой следующая ситуация.

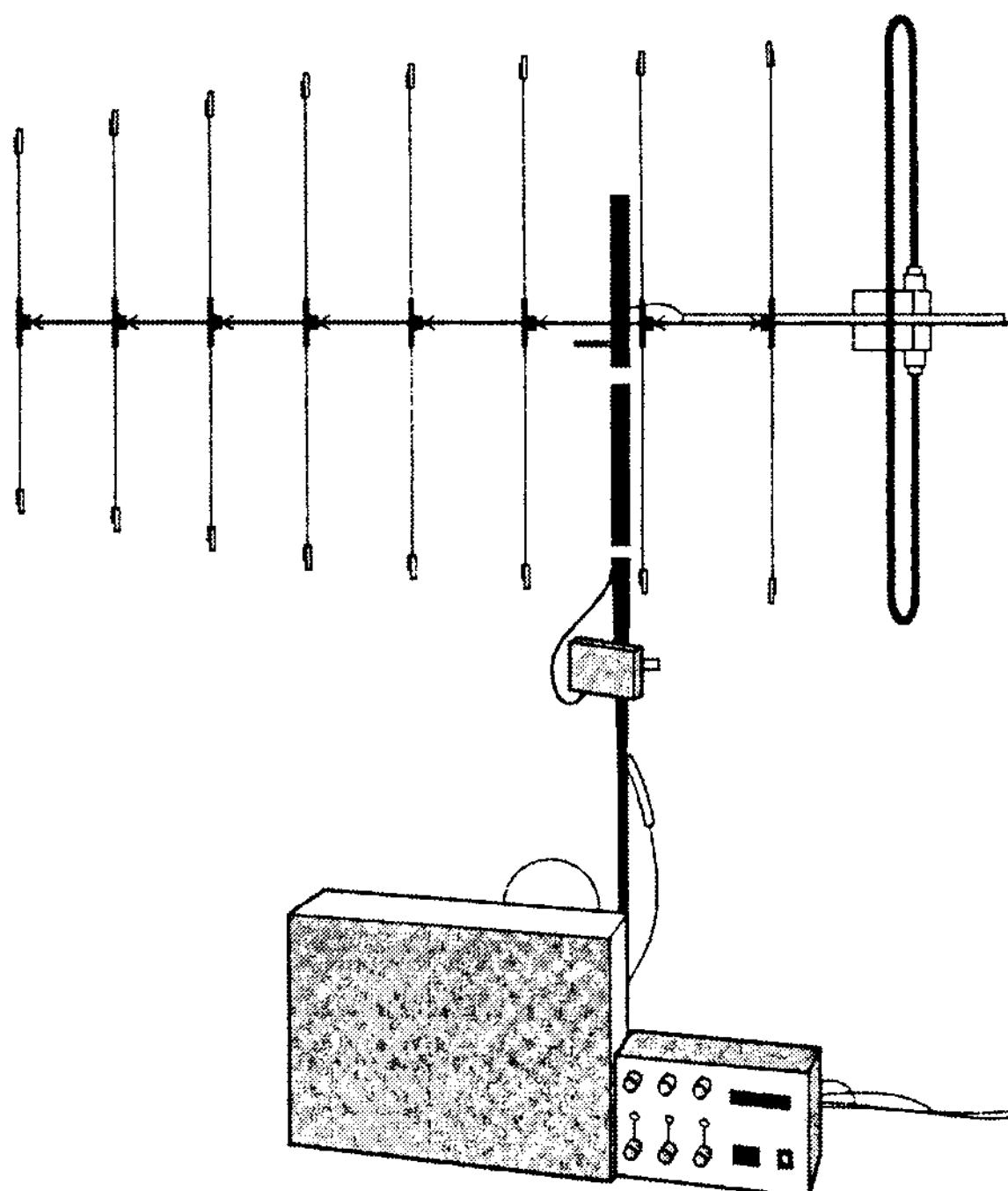
*На улице в темноте паркуется фургон без окон. Внутри, за панелью из стекловолокна, размещена антенна. Она направлена на окно офиса на третьем этаже. В это время директор компании составляет общую стратегию конкурентной борьбы, даже не подозревая, что все, что отображается на его мониторе, перехватывается, записывается и выводится на дисплей расположенного снаружи фургона.*

С точки зрения шпиона, это идеальный вариант развития событий: пассивный мониторинг, который невозможно обнаружить. Но, прежде чем приступить к обсуждению реальности описанной ситуации, изложим

общую информацию по данному вопросу. Поскольку у большинства наших читателей отсутствует необходимый допуск для работы с секретными документами, нам придется проанализировать общедоступные источники информации, дабы сделать обоснованные выводы о размерах угрозы мониторинга побочного излучения.

## КРАТКАЯ ПРЕДЫСТОРИЯ

Первые признаки того, что мониторинг электромагнитного излучения может представлять реальную угрозу, появились еще в 80-х годах XX века. В 1985 году немецкий инженер Вим ван Эк опубликовал статью под названием «Электромагнитное излучение от видеодисплеев: риск шпионажа?». В статье описывались способы наблюдения за видеотерминалами (предшественниками современных компьютерных мониторов) на расстоянии до 1 км при помощи сравнительно недорогого оборудования. (Увидевшая свет версия статьи была специально урезана, а для создания действительно рабочего устройства в приведенные схемы требовалось внести кое-какие изменения. Внешний вид подобного устройства продемонстрирован на рис. 13.1.)



**Рис. 13.1.** Оригинальное устройство мониторинга побочного излучения Вим ван Эка, позволяющее (при выполнении определенных условий) осуществлять наблюдение за видеотерминалами с расстояния до 1 км

Вскоре после опубликования статьи по британскому телевидению была показана серия разоблачительных репортажей, в которых репортеры ездили по Лондону с устройствами, напоминающими прибор ван Эка, осуществляя наблюдение за банками, адвокатскими конторами и Новым Скотленд-Ярдом. Специалисты в сфере обеспечения безопасности забеспокоились по поводу перспектив электронного шпионажа даже без проникновения в здание. Не меньшие волнения по этому поводу возникли у Управления национальной безопасности из-за того, что данная технология стала известна широкой общественности. Фирма Wang Research Laboratories (крупный производитель оборудования, соответствующего стандартам TEMPEST) собиралась продемонстрировать оборудование для электромагнитного наблюдения профессионалам в сфере безопасности, однако Управление национальной безопасности, сославшись на секретность, запретило проведение презентации. На конференции Interface'87 одна из известных компаний из Вашингтона, округ Колумбия, заявила о проведении презентации «Как обойти системы компьютерной безопасности», на которой также должна была проводиться демонстрация технологий наблюдения и перехвата побочного электромагнитного излучения (эмиссии), однако и эта выставка была отменена в последний момент по требованию Управления национальной безопасности. (Это резко контрастирует с подходом шведского правительства в 80-х, которое постоянно информировало коммерческие предприятия о возможной угрозе со стороны устройств мониторинга побочного излучения и даже опубликовало информационный буклет под названием «Утечка компьютерной информации», в котором разъяснялись потенциальные опасности и приводился список возможных контрмер.)

В конце 80-х в Соединенных Штатах появилось множество устройств, подобных прибору ван Эка, начали продаваться схемы создания собственных устройств сомнительного вида и эффективности. Развитие подобных устройств продолжалось и в начале 90-х, были даже проведены фальсифицированные телевизионные демонстрации устройств мониторинга TEMPEST и продажи мошеннического оборудования. (Такое впечатление, что, когда речь заходит об оборудовании, соответствующем стандартам TEMPEST, средства массовой информации по каким-то причинам делаются страшно наивными и не проявляют должного усердия, чтобы проверить имеющуюся информацию.)

Постоянная шумиха вокруг устройств мониторинга побочного излучения электронных приборов привела к возникновению множества ошибочных суждений о стандартах TEMPEST. Популярно, например, мнение, что практически любой радиотехник, посетив магазин радиотоваров и выложив 100 долларов, сможет построить устройство для мониторинга электромагнитного излучения, позволяющее воссоздавать информацию (возможно, это и удалось бы сделать со старыми видеотерминалами, но отнюдь не с современными компьютерными мониторами).

Хотя по поводу расшифровки информации на основе перехваченного побочного электромагнитного излучения в лабораторных условиях опубликовано немало статей, на сегодняшний день ничего не известно о существовании устройств мониторинга, которые были бы применимы в полевых условиях.

Несмотря на интерес общественности к проблеме TEMPEST, на множество ярких индивидуальностей, имеющих опыт в электронной схемотехнике, а также популярность Интернета как средства распространения информации, пока что никто не решился опубликовать схемы для создания недорогих устройств мониторинга. Это говорит в пользу того, что мониторинг побочного излучения не является столь же тривиальной задачей, как, например, перехват трафика беспроводных сетей стандарта 802.11b, описанный в главе 11.



Хронологию ключевых событий в истории стандартов TEMPEST вы можете прочесть на веб-странице <http://cryptome.org/tempest-time.htm>.

## ПРАВИТЕЛЬСТВЕННЫЕ ПЕРСПЕКТИВЫ

Итак, теперь мы знаем, что мониторингу побочного излучения со стороны широкой общественности ничего не грозит, но как быть с организациями, финансируемыми правительством? Здесь, к сожалению, мы располагаем весьма скучными сведениями, что связано с секретностью стандартов TEMPEST, вызванной необходимостью защищать свои «источники и методы».

Достоверные правительственные сведения о том, насколько часто проводятся или проводились операции по мониторингу побочного излучения, отсутствуют. Известны отдельные анекдотичные случаи мониторинга, проводившегося в целях политического, военного и промышленного шпионажа, но никаких подробностей широкой общественности сообщено не было. К примеру, один из агентов ФБР, принимавший участие в коллективном обсуждении проблемы в Массачусетском технологическом университете, заявил, что мониторинг электромагнитного излучения может использоваться для расследования преступлений. Являлось ли это заявление соответствующим истине, популистским либо сознательной дезинформацией – мы не знаем.

Основной трудностью в отслеживании подобных случаев мониторинга является пассивность технологии наблюдения, удаленность от целевого объекта и сложность раскрытия преступления, если только вам не удастся поймать злоумышленника, пока с его рук еще не была смыта красная кровь (не самый удачный каламбур времен холодной войны). Даже если шпион все-таки пойман, скорее всего, об этом случае предпочтут промолчать, особенно когда речь идет об экономическом шпионаже. И правительство, и частные компании имеют большой опыт в деле сокрытия информации по безопасности.

И все же некоторые факты указывают на то, что риск мониторинга побочного излучения действительно существует – по крайней мере, со стороны иностранной разведки. Поскольку оборот в индустрии TEMPEST составляет более миллиарда долларов в год, то, скорее всего, угроза реально существует, в противном случае кому нужно все это защитное оборудование (хотя, возможно, мы стали свидетелями грандиозной аферы, ставшей источником обогащения ряда лиц).

Кроме того, как быть с различными упоминаниями об этой угрозе в несекретных правительственные и военных документах? Процитируем для примера одну из инструкций военно-морского флота, в которой обсуждался вопрос «перехвата побочного излучения»: «Иностранные правительства постоянно проводят операции против Соединенных Штатов с целью перехвата секретных переговоров и информации, проводя испытания с единственной целью – воспользоваться достижениями в сфере перехвата побочного ЭМИ».

Итак, опасность все-таки существует, но насколько она реальна? Несколько смягченная картина угрозы была представлена в 90-х годах серией отчетов и директив военных и разведывательных управлений, включая следующие:

- В 1991 году отчет главы ЦРУ потребовал от Разведывательного сообщества пересмотра внутренних стандартов TEMPEST, основываясь на реальности угрозы. Материалы отчета показывали, что сотни миллионов долларов были потрачены на защиту уязвимых мест, вероятность и возможность использования которых весьма низка. Этот отчет подтолкнул Разведывательное сообщество на пересмотр и послабление требований TEMPEST.
- В 1992 году Национальное разведывательное бюро (NRO – National Reconnaissance Office), секретное управление, задействованное в работе над проектом спутников-шпионов США, отменило использование стандартов TEMPEST в своей работе.
- В 1994 году объединенная Комиссия по безопасности представила министру обороны и главе ЦРУ отчет под названием «Переопределение безопасности». Комиссия заговорила о необходимости активного пересмотра программы TEMPEST, исходя из того, что угроза внутренней безопасности минимальна. Было предложено ограничить применение контрмер по программе TEMPEST только случаями проявления особой угрозы безопасности информации.

Можно утверждать, что со времен холодной войны, когда об опасности в плане мониторинга побочного электромагнитного излучения заговорили впервые, уровень угрозы использования этих уязвимых мест был слишком переоценен разведкой и военными. Однако после того как механизм был запущен, остановить его очень трудно.

## ВЫВОДЫ

Какие же мы можем сделать выводы в отношении реальности угрозы мониторинга побочного электромагнитного излучения? Основываясь на имеющейся информации, наши заключения будут следующими:

- Исследования ван Эка показали возможность перехвата побочного излучения от весьма примитивных видеотерминалов. Реконструировать же изображение на экране современного компьютерного монитора, тем более на расстоянии, на порядок сложнее, особенно если учесть наличие электромагнитного смога от встречающихся на каждом шагу электронных устройств, что может свести на нет все попытки выделить сигнал от интересующего вас монитора.
- Правительство не верит в угрозу мониторинга побочного излучения, проводимого иностранными разведками на территории США. За пределами страны, например, на территории посольств или военных баз Соединенных Штатов данная опасность представляется более реальной, поскольку иностранная разведка, находясь на своем поле, может задействовать все возможные средства.
- Разумеется, мониторинг побочного излучения не является столь уж распространенной шпионской технологией, как утверждают телевизионные шоу; реализовать данную методику намного сложнее, чем думает большинство обывателей. Если только ваш противник не имеет хорошего спонсора и не обладает доступом к сложному электронному оборудованию и услугам профессионалов в этой области, мониторинг побочного излучения можно ставить в самый конец списка потенциальных опасностей.

## Контрмеры по защите от мониторинга излучения

Рассматривая любой вид атаки, вы должны оценить затраты на реализацию контрмер и получаемые от них результаты. Разумный противник, очевидно, проанализирует альтернативы, выясняя, что проще и дешевле: самому шпиону проникнуть в здание под видом обслуживающего персонала для доступа к информации либо же организовать дорогостоящую техническую операцию для перехвата тех же самых данных? Хотя в случае некоторых «трудных» целей такой технический подход оправдан, традиционная техника сбора информации разведчиками, без сомнения, используется гораздо чаще.

Поскольку существуют менее дорогие и более эффективные способы перехвата информации, подавляющему большинству пользователей не нужно беспокоиться об опасности электромагнитного мониторинга. Если же у вас есть все основания считать данную угрозу реальной, но вы не обладаете соответствующим уровнем допуска к секретным стандартам, мы можем посоветовать вам прибегнуть к следующим контрмерам:

- **Приобретение оборудования, сертифицированного в соответствии со стандартами TEMPEST.** Это наиболее логичный шаг, если вы работаете в правительственной организации либо являетесь подрядчиком Министерства обороны. Учитывайте, что стоимость компьютеров и периферии, соответствующих стандартам TEMPEST, немалая, к тому же большинство производителей не продают такую технику частным лицам. Тем не менее в последнее время на рынке начинают появляться излишки оборудования TEMPEST, причем не по таким уж заоблачным ценам.
- **Использование архитектурных решений.** Еще дороже, чем специальное оборудование, сертифицированное по стандартам TEMPEST, обойдется вам экранирование целой комнаты или даже здания при помощи медной сетки и специальных окон, блокирующих передачу электромагнитных волн. Прочтите посвященный этому вопросу документ «Проектирование и дизайн – ЭМИ и защита помещений по стандартам TEMPEST», размещенный на сайте [www.usace.army.mil/inet/usace-docs/engineering-phlets/ep1110-3-2/toc.htm](http://www.usace.army.mil/inet/usace-docs/engineering-phlets/ep1110-3-2/toc.htm).
- **Применение стандартной технологии защиты от радиоволн и электромагнитных помех.** Хотя и немного устаревшая, написанная Гради Вордом инструкция по методам экранирования может применяться и сегодня. В ней описываются недорогие решения, которые можно реализовать своими силами. Найти эту инструкцию можно на веб-странице [www.eff.org/Privacy/Security/tempest\\_monitoring.article](http://www.eff.org/Privacy/Security/tempest_monitoring.article).
- **Использование специальных шрифтов.** Росс Андерсен и Маркус Кун обнаружили, что подавить побочное излучение можно путем использования специальным образом подобранных шрифтов. Их статью, посвященную этой теме, можно найти в сети Интернет по адресу [www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf](http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf). Немецкая компания Steganos GmbH ([www.steganos.com](http://www.steganos.com)) включила эти специальные шрифты в некоторые из своих продуктов, включая бесплатные приложения, подобные Блокноту в Windows.



Чтобы получить более подробную информацию по стандартам TEMPEST, собранную автором книги за последние шесть лет, посетите страничку «Полная неофициальная информация по стандартам TEMPEST» по адресу [www.eskimo.com/~joelm/tempest.html](http://www.eskimo.com/~joelm/tempest.html).

# Оптические стандарты TEMPEST – светодиоды и отраженный свет

В марте 2002 года Джо Лори опубликовал интригующую статью под названием «Оптические стандарты TEMPEST». Процитируем предисловие к ней: «Была открыта новая форма перехвата побочного излучения. Светодиодные индикаторы, размещенные на устройствах связи, при определенных условиях могут излучать модулированный оптический сигнал, напрямую связанный с передаваемой информацией. При этом злоумышленнику даже не потребуется физический доступ к устройству, поскольку он сможет удаленно перехватить все обрабатываемые устройством данные, включая исходный текст в системах шифрования информации. Эксперименты показали, что даже в реальных условиях данные могут быть перехвачены на значительном расстоянии. Таким образом, свою уязвимость продемонстрировали многие устройства, включая модемы и IP-маршрутизаторы».

В тот же день позднее появилась статья Маркуса Куна под названием «Риск оптического наблюдения за дисплеями ЭЛТ». Суть ее в том, что изображение на экране компьютерного монитора можно восстановить по отраженному от стен свету. В заключение Кун написал: «Информация, отображаемая на экране современных дисплеев с электронно-лучевой трубкой, может быть реконструирована по искаженному и даже диффузно отраженному свету при помощи доступных широкой общественности устройств, таких как фотоэлектронный умножитель и компьютер с достаточно быстрым АЦП (аналого-цифровым преобразователем)».

Знали ли правительственные разведывательные органы об этих уязвимых местах ранее – неизвестно. В любом случае проведение такого мониторинга требует наличия сложного оборудования, а простейшими, но эффективными контрмерами можно считать заклейку светодиодов черной электропроводной лентой и зашторивание окон при работе с конфиденциальной информацией (что, в общем-то, рекомендуется делать в любом случае).



Подробности по этим двум разновидностям атак можно прочесть в статье Лори, размещенной по адресу [http://applied-math.org/optical\\_tempest.pdf](http://applied-math.org/optical_tempest.pdf), и статье Куна на сайте [www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf](http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf).

## HIJACK и NONSTOP

Со стандартом TEMPEST связана пара других секретных стандартов под кодовыми названиями HIJACK и NONSTOP. Эти стандарты касаются наблюдения за криптографическими устройствами при помощи расположенных поблизости радиопередатчиков (мобильных телефонов, раций либо интеркома). На сегодняшний день мы располагаем весьма скучной информацией по этим двум стандартам, поскольку в отношении них секретность соблюдается гораздо строже, чем в отношении стандартов TEMPEST. Однако, собрав воедино разрозненные кусочки несекретной информации, мы попытаемся представить, что описывают эти кодовые слова.

Кодовое слово HIJACK относится к перехвату побочного излучения в результате передачи цифровых, а не электромагнитных сигналов. Такой способ получения доступа к защищенной информации напоминает атаки, направленные против оборудования, не сертифицированного в соответствии со стандартами TEMPEST, когда шпиону не требуется находиться рядом с наблюдаемым устройством. Для проведения подобного рода атак требуется доступ к линиям связи (проводным или беспроводным). Шпионы применяют антенны, приемники, устройства отображения, устройства записи и другое оборудование (специальные детекторные системы, которые, предположительно, являются чрезвычайно чувствительными, очень дорогими и встречаются очень редко). Кроме того, технические специалисты, работающие с этим спецоборудованием, должны иметь значительный опыт и соответствующие навыки.

Стандарт NONSTOP, очевидно, связан с перехватом побочного излучения от оборудования, работающего в радиочастотном диапазоне (радиции, мобильные телефоны, пейджеры, охранные системы, беспроводные телефоны и беспроводные сети; сюда не входят стандартные промышленные приемники AM/FM-сигнала), которое размещено вблизи с устройствами хранения секретной информации. Существуют даже специальные рекомендации по отключению подобных устройств радиочастотного диапазона либо их размещению на расстоянии от оборудования, на котором может храниться конфиденциальная информация (компьютеров или принтеров).

## ECHELON – глобальная система наблюдения

До сих пор все обсуждаемые нами методы и средства касались в основном сбора информации по отдельным объектам (компьютерам или сетям), однако на вооружении у правительства имеется намного более мощный инструмент глобального наблюдения под кодовым названием ECHELON.

ECHELON – это название экстенсивной программы наблюдения со стороны правительства, которая связана с перехватом различных видов информации по всему миру. На сегодняшний день в этой программе принимают участие правительства Соединенных Штатов, Великобритании, Канады, Австралии и Новой Зеландии. Хотя официальный старт проекту был дан в 1970-х годах, его концепция возникла в далеком 1948 году, когда пять стран-участниц подписали договор о сотрудничестве в плане разведки.

Считается, что в рамках программы ECHELON ежедневно осуществляется перехват трех миллиардов переговоров, включая почтовые сообщения, факсы, обмен файлами через Интернет, спутниковые передачи, телефонные звонки и телексы. По информации некоторых источников, программой ECHELON контролируется до 90% трафика в Интернете. (Если говорить о технической стороне вопроса, то термин ECHELON относится исключительно к перехвату спутникового сообщения, хотя его широко используют и для обозначения систем перехвата в целом.)

Секретность проекта ECHELON охраняется в течение многих лет, и правительство Соединенных Штатов не только отказывается от комментариев по этой теме, но и вообще не признает факт существования такого проекта. Когда речь заходит о секретных программах, нередко правительство занимает позицию страуса, спрятавшего голову в песок, полагая, что скрытие информации приведет к исчезновению проблемы самой по себе; иногда это можно оправдать требованиями секретности операции, но чаще ситуация выглядит несколько комично. Информация о проекте ECHELON известна в основном из уст доносчиков, из признаний правительств Австралии и Новой Зеландии, а также правительственные отчетов европейских стран по системам наблюдения. Возможно, что о данном проекте нам известна лишь малая толика от общего объема информации.

Управление национальной безопасности Соединенных Штатов играет главную роль в проведении программы ECHELON, за ним следует Штаб-квартира правительственных систем связи (GSHQ – Government Communications Head Quarter) в Великобритании, Управление связи оборонных войск Австралии (DSD – Defense Signals Directorate), канадская Организация по обеспечению безопасности систем связи (CSE – Communications Security Establishment), а также новозеландское правительственные бюро по обеспечению безопасности систем связи (GCSB – Government Communications Security Bureau). В некоторых случаях данные, собранные в рамках программы ECHELON, предоставляются правительствам дружественных стран.

ECHELON – это не единственная из глобальных программ наблюдения (хотя по сей день она является крупнейшей и наиболее совершенной). Другие страны, например Китай, Индия, Израиль, Франция, Германия, Пакистан и Россия, имеют достаточные ресурсы и опытные разведывательные службы для поддержки собственных проектов по перехвату информации в системах связи (особенно это касается Интернета).

## Принципы работы проекта ECHELON

Проект ECHELON использует «метод пылесоса», автоматически собирая информацию всех видов. Затем собранная информация обрабатывается при помощи серии мощных компьютерных приложений искусственного интеллекта. В перехваченном тексте или аудиозаписях осуществляется поиск ключевых слов. (К примеру, когда правительство проявляло интерес в отношении президента Северной Кореи, все сообщения, содержащие упоминание о Ким Йонг Иле, выделялись для дальнейшего анализа вручную.) В качестве ключевых слов могли фигурировать имена, адреса, номера телефонов, адреса электронной почты или даже фрагменты речи; предположительно, в некоторых случаях в рамках проекта ECHELON производилась идентификация личностей по голосам. Компьютерные системы, анализирующие все собираемые данные, называли словарями (DICTIONARY).

Необходимо понимать, что проект ECHELON сочетает в себе использование специального аппаратного обеспечения и работу экспертов в области разведки. Каждая страна, принимающая участие в проекте ECHELON, располагает своими наблюдательными системами и методами. Страны-участники проекта обмениваются информацией, собранной с помощью различных систем, причем, как правило, разведывательное управление одной страны имеет в своем распоряжении списки ключевых слов, приведших от разведуправлений других стран. К примеру, если в ходе автоматической обработки перехваченных сообщений австралийская станция наблюдения Управления связи оборонных войск обнаруживает ключевые слова, встречающиеся в списке Национального управления безопасности США, которые касаются ядерной программы Северной Кореи, данные будут автоматически пересланы Управлению национальной безопасности США по безопасной сети.

Перехват информации осуществляется различными способами. Для перехвата данных, передаваемых через коммерческие спутниковые системы связи, используется серия огромных антенн, расположенных по всему миру. Кроме перехвата сообщений с чужих спутников, в данном проекте задействована серия собственных орбитальных разведывательных спутников, предназначенных для перехвата данных, передаваемых по системам беспроводной связи на Земле. Затем спутники-шпионы отправляют собранную информацию в центры обработки США, Великобритании, Австралии и Германии.

Для наземного наблюдения (например, за телефонами и факсами) участники программы ECHELON могут заключать секретные договоры с телекоммуникационными компаниями о прослушивании переговоров при помощи специальных быстродействующих устройств мониторинга. Известно также об успехе совместного проекта военных и разведки по наблюдению за подводными кабелями передачи данных.

Однако, поскольку темой данной книги является компьютерный шпионаж, вернемся к заявлению о том, что за 90% трафика в Интернете

ведется наблюдение. Согласно статье Уэйн Мэдсен, проводившей журналистское расследование (до этого она работала в Управлении национальной безопасности США), а также документу о «Возможностях перехвата 2000» ([www.nrc.nl/W2/Lab/Echelon/ic2kreport.htm](http://www.nrc.nl/W2/Lab/Echelon/ic2kreport.htm)), к 1995 году специальное программное обеспечение для перехвата сетевого трафика было установлено Управлением национальной безопасности в девяти основных точках обмена трафиком (таблица 13.1). Точки обмена интернет-трафиком (Internet Exchange Points) представляют собой физическую сетевую инфраструктуру, предназначенную для поддержки сообщения между провайдерами услуг Интернета. А если вы контролируете все точки обмена трафиком, то вы контролируете всю передаваемую через Интернет информацию. (Сведения по существующим на данный момент точкам обмена интернет-трафиком можно найти на веб-сайте [www.ep.net/ep-main.html](http://www.ep.net/ep-main.html).)

**Таблица 13.1. Точки обмена интернет-трафиком (по состоянию на 1995 г.), за которыми, предположительно, ведется наблюдение со стороны Управления национальной безопасности**

Узел	Местоположение	Оператор	Назначение
FIX East	Колледж-Парк, Мэриленд	правительство США	обмен информацией федеральных органов по Интернету
FIX West	Маунтин Вью, Калифорния	правительство США	обмен информацией федеральных органов по Интернету
MAE East	Вашингтон, округ Колумбия	MCI	региональная сеть
New York NAP	Пенсакен, Нью-Джерси	Sprintlink	точка входа в сеть
SWAB	Вашингтон, округ Колумбия	PSInet/ Bell Atlantic	обходной канал для высокоскоростного доступа к сети в Вашингтоне
Chicago NAP	Чикаго, Иллинойс	Ameritech/ Bellcorp	точка входа в сеть
San Francisco NAP	Сан-Франциско, Калифорния	Pacific Bell	точка входа в сеть
MAE West	Сан-Хосе, Калифорния	MCI	региональная сеть
CIX	Санта Клара, Калифорния	CIX	биржа коммерческого информационного обмена

Пользователи компьютеров, страдающие паранойей в тяжелой форме (либо самые осведомленные в вопросах безопасности), уже давно считают, что Интернет находится под полным наблюдением. В знак протesta еще в 80-х годах XX века некоторые лица добавляли в конец невинных сообщений электронной почты либо групп новостей USENET такие слова и аббревиатуры, как КГБ, ЦРУ, плутоний, МОССАД и т. д. Эта полусерьезная-полушуточная затея достигла своего апогея 21 октября 1999 года, объявленного днем «борьбы с программой ECHELON», когда была организована попытка привлечь как можно больше людей к отправке зашифрованных сообщений и к добавлению в них провокационных слов. Задачей инициаторов атаки являлась «перегрузка» данными системы ECHELON, что привело бы к блокировке программы. Сомнительно, чтобы эта попытка увенчалась успехом, тем не менее она была повторена в 2001 году, результатом чего стало, по крайней мере, повышение осведомленности общественности об этой системе наблюдения.

В рамках программы ECHELON проводится не только пассивное наблюдение за передаваемой информацией, но и ее активный поиск. В течение четырех лет некоторое приложение-робот ежедневно посещало сайт Джона Янга cryptome.org, загружая все обновленные материалы. Этого робота нельзя отнести к невидимкам, поскольку его исходящий IP-адрес оказалось очень легко проследить до Управления национальной безопасности. Нетрудно предположить, что эти данные собирались системой ECHELON.

## ECHELON: дискуссии и контрмеры

Если бы не многочисленные источники, подтверждающие реальность существования проекта ECHELON, все разговоры об этой системе можно было бы посчитать порождением фантазии некоего одержимого поклонника теории заговоров. В данном случае это не так, и хотя ECHELON служит в основном целям обнаружения террористов и поиска оружия массового поражения, которым владеют экстремистские государства, секретность и впечатляющие возможности подобной наблюдательной программы беспокоят многих граждан. Правозащитников, не являющихся участниками проекта ECHELON, волнуют в первую очередь следующие моменты.

- Хотя изначально проект ECHELON разрабатывался для политического и военного наблюдения в годы холодной войны, существует информация, что в настоящее время эта программа используется и в целях экономического шпионажа. Известны случаи, когда американские корпорации неожиданно выигрывали прибыльные контракты у своих европейских конкурентов, – предполагается, что в этом им помогла информация, собранная проектом ECHELON.

- Соединенные Штаты и многие другие страны имеют законы, охраняющие право на частную жизнь, которые призваны защищать рядовых граждан от шпионажа со стороны собственного правительства и разведки. Тем не менее есть все основания подозревать, что проект ECHELON используется в том числе и для обхода этих ограничений. К примеру, Управление национальной безопасности США не имеет права просто так шпионить за своими гражданами из чистого любопытства, но, если Штаб-квартира правительственных систем связи Великобритании собрала в рамках проекта ECHELON данные об отдельных американских гражданах, эта информация может быть передана Управлению национальной безопасности, заинтересованному в предмете наблюдения. И никаких нарушений.
- Не существует контролирующих органов, которые могли бы предотвратить потенциальную угрозу злоупотреблений в рамках программы ECHELON. Газета Washington Post сообщила в декабре 1998 года, что Управление национальной безопасности призналось в том, что в их распоряжении имеется досье на принцессу уэльскую Диану, составленное по материалам перехваченных телефонных переговоров. Никаких разъяснений по поводу того, почему американская разведка располагает информацией о бывшем члене британской королевской семьи, не последовало.

Мы не намерены дискутировать с вами на тему: «Если мне нечего скрывать, то почему меня должен беспокоить проект ECHELON?» Приимем в качестве допущения, что вы являетесь защитником прав на неприкосновенность частной жизни, или вам все-таки есть что скрывать. Конечно, загрузка из Интернета трэйз-файлов не заставит ECHELON следить за вашими привычками в сфере файлообмена (хотя Американской ассоциации звукозаписывающих компаний эта ваша черта не понравилась бы). В рамках проекта ECHELON обрабатывается такое огромное количество информации, что, если только вы не являетесь отъявленным злодеем, данные о вас очень скоро затеряются в общей массе.

Кроме того, не забывайте, что проект ECHELON представляет собой всего лишь наблюдательную технологию, пусть достаточно сложную и могущественную, но которую, как и любую другую систему, так или иначе, можно обмануть. Перечислим основные контрмеры, которые помогут вам защитить свои данные от всевидящего ока проекта ECHELON:

- **Шифрование.** Очевидно, что если вы будете применять стойкие алгоритмы шифрования для передачи данных через Интернет, получить доступ к вашей информации будет достаточно сложно. В то же время учтите, что в рамках проекта ECHELON зашифрованным сообщениям уделяется особое внимание (значит, вам есть что скрывать). А если вы привлечете к себе внимание

правительственных организаций, то для взлома зашифрованных вами сообщений будут предприниматься многочисленные попытки. Даже если ваши сообщения не удастся взломать сейчас, они могут быть сохранены наряду с миллионом других зашифрованных сообщений для последующей расшифровки в будущем (в результате прорыва в области криптографических технологий, изобретения квантового компьютера, инопланетной технологии и т. п.).

### Тактика: США против Рейгана

Брайан Патрик Рейган работал в Национальном разведывательном бюро (NRO – National Reconnaissance Office) – организации, отвечающей за использование спутников-шпионов Соединенных Штатов. Вначале он был принят на должность мастер-сержанта ВВС, на которой Рейган имел доступ к информации под грифом «совершенно секретно» и даже еще более секретной информации. Уйдя в отставку в 2000 году, он продолжил работу с Национальным бюро разведки в качестве подрядчика компании TRW Incorporated, исчезнувшей в результате слияния с компанией Northrop Grumman.

Арестовали Рейгана 23 августа 2001 года по обвинению в попытке продажи секретной информации, включая спутниковые фотографии, таким странам, как Ирак, Ливия и Китай. Когда он был задержан в международном аэропорту Далласа во время посадки на рейс, отправлявшийся в Цюрих, агенты ФБР обнаружили при нем закодированные координаты мест дислокации ракет в Ираке и Китае, информацию о типе ракет и дату первого обнаружения ракет. Все эти данные, предположительно, были получены путем обработки спутниковых фотоснимков.

С изъятого у него дома ноутбука ФБР восстановило удаленные письма, адресованные в Ирак и Ливию, с предложениями о продаже секретной информации на сумму в 13 000 000 долларов. Эти письма начинались с фразы: «Я хочу совершить шпионаж против Соединенных Штатов».

Рейгана беспокоило внимание к своей персоне со стороны ФБР (а ему приходилось беспокоиться, поскольку агенты постоянно следовали за ним по пятам в общественные библиотеки, наблюдали за его перемещениями по сети Интернет и вели учет звонков в иностранные посольства), поэтому он решил воспользоваться скрытым каналом передачи информации при общении с иракцами.

К обвинению Рейгана была приложена копия письма, отправленного Саддаму Хусейну. В письме, в частности, присутствовал следующий фрагмент: «Мне от вас необходимо в первую очередь, чтобы вы внесли небольшие изменения на свою домашнюю страничку в качестве доказательства того, что наше общение не подстроено ФБР с целью загнать меня в ловушку. У меня есть распечатка вашей веб-страницы... Если вы внесете некоторые незаметные поправки (замените одно слово на другое, вставьте лишнюю запятую или же измените какое-либо число), я буду знать, что вы получили оба письма и согласны действовать по плану»\*. Письмо практически идентичного содержания было отправлено ливийскому лидеру Muammaru Kad-dafi.

В начале 2003 года началось рассмотрение дела Рейгана по обвинению в шпионаже. За последние 50 лет это был первый открытый суд над американским гражданином, обвиняемым в шпионаже. Уолкер, Поллард, Хансен, Эймс и другие не менее знаменитые шпионы пошли на компромисс с правительством в вопросе о признании себя виновными, поэтому их дела никогда не рассматривались в суде. Рейган же заявил, что он никогда не передавал секретную информацию иностранным властям и вся информация, которой он владел, была доступна широкой публике. Его признали виновным и в марте 2003 года вынесли вердикт о пожизненном заключении.

- **Скрытые каналы передачи данных.** Взамен шифрования, дабы не привлекать к себе лишнее внимание, вы можете использовать скрытые каналы передачи данных для проведения переговоров – это может быть выдача реального сообщения за спам либо вставка сообщения среди текста на какой-то веб-странице. Обвиняемый в шпионаже Патрик Рейган посоветовал иракцам внести изменения в их веб-сайт для передачи ему сообщения в случае, если они захотят приобрести американское вооружение и разведывательные секреты у него.
- **Отказ от использования современных технологий.** Если вы страдаете тяжелой паранойей в отношении проекта ECHELON и вам есть что скрывать, вернитесь к старым методам связи без использования компьютеров, телефонов или радио. Когда члены террористической группы Аль-Каида поняли всю разведывательную мощь Соединенных Штатов во время вторжения в Афганистан, они перестали использовать спутниковые телефоны и радио и вернулись к классическим способам доставки сообщений с помощью курьеров.

\* В переводе исправлены грамматические и стилистические ошибки оригинала, воспроизведенные автором в тексте книги. – Прим. ред.



Более подробно о проекте ECHELON вы можете узнать на веб-сайте американского Союза гражданских свобод (ACLU) по адресу [www.echelonwatch.org](http://www.echelonwatch.org) и из коллекции документов по проекту ECHELON на сайте <http://cryptome.org/cryptout.htm#Echelon>.

## Carnivore/DCS-1000

Система Carnivore (ныне известная под именем DCS-1000 – Digital Collection System – цифровая система сбора информации), которой владеет ФБР, предназначена для наблюдения за трафиком в сети Интернет. В отличие от «метода пылесоса», характерного для проекта ECHELON, система Carnivore собирает информацию только по целевым объектам.

Система Carnivore представляет собой усовершенствованную программу перехвата сетевых пакетов, разработанную специально для использования правоохранительными органами. Программа устанавливается на базовой станции провайдера услуг Интернета, к которому подключен интересующий правоохранительные органы объект, причем только после получения соответствующего судебного ордера. (ФБР утверждает, что система Carnivore используется только тогда, когда оборудование провайдера Интернета не подходит для выполнения подобного мониторинга, либо он отказывается идти на уступки, требуя предъявления судебного ордера на поиск определенной информации.) Эта система анализирует входящий и исходящий трафик, записывая данные, связанные с целевым объектом, согласно ордеру на прослушивание. Система Carnivore может выполнять запись содержимого либо работать только с устройствами регистрации IP-адресов:

- **Перехват содержимого сообщений.** В этом случае осуществляется сохранение всего сетевого трафика и электронной почты, поступающей с определенного IP-адреса или от определенного пользователя. Для получения ордера на такое прослушивание необходимы веские основания.
- **Отслеживание и регистрация IP-адресов и другой служебной информации.** В этом случае записывается только служебная информация, а не содержимое сообщений. В качестве примера приведем заголовки электронных писем (кроме темы), перечень посещавшихся веб-сайтов и FTP-серверов. Ордер на проведение операции такого уровня получить гораздо легче, чем разрешение на запись содержимого сообщений.

Впервые о системе Carnivore широкая общественность узнала летом 2000 года, причем все, что стало известно, базировалось на 600 страницах документов ФБР, обнародованных в соответствии с Законом о свободе информации и переданных Центру соблюдения прав на неприкосновенность

электронной информации (многие страницы документов подверглись перед опубликованием серьезному редактированию), и результатах независимой экспертизы Иллинского технологического института.

## Обзор системы Carnivore

Система Carnivore является частью набора инструментальных средств ФБР, предназначенных для проведения расследований под названием DragonWare Suite. Помимо системы Carnivore существуют такие программы, как CoolMiner и Packeteer. Packeteer позволяет обрабатывать выходные данные программы Carnivore и восстанавливать протоколы (такие, как SMTP или HTTP) из IP-пакетов. CoolMiner отвечает за подготовку статистических отчетов и преобразование информации, поступившей от регистраторов сетевых IP-адресов, в вид, пригодный для отображения в веб-браузере. (Утилиты пакета DragonWare представлены в виде библиотек DLL, написанных на языке C++, и графического интерфейса пользователя, разработанного на Visual Basic.)

Система Carnivore была разработана для ФБР сторонним подрядчиком, упоминание о котором было изъято из документов, обнародованных в соответствии с Законом о свободе информации, однако существуют неподтвержденные слухи по поводу того, что в разработке этого и других проектов для ФБР принимала участие компания Booz, Allen & Hamilton.

ФБР утверждает, что ничего зловещего в названии системы Carnivore (Динозавр) нет. В зависимости от того, к кому вы будете обращаться с вопросами по поводу происхождения этого названия, вы можете услышать различные ответы, начиная с того, что эта система «дает пищу (мясо) для расследований», и заканчивая образным описанием вроде: «Динозавр пережевывает всю информацию в сети, но съедает только то, что разрешено судебным ордером». Даже после переименования системы Carnivore в DCS-1000 ФБР продолжает утверждать, что смена названия никак не связана с негативной реакцией общественности на название Carnivore.

Использование системы Carnivore началось в 1999 году, но до ее появления существовали еще, по крайней мере, два подобных инструментальных средства. Предшественником Carnivore являлась программа Omnivore, которая предназначалась для систем Sun Solaris. Эта программа была разработана для мониторинга входящих и исходящих почтовых сообщений, распечатки содержимого посланий в режиме реального времени и архивации данных на восьмимиллиметровую магнитную ленту. Система Omnivore, впервые примененная в октябре 1997 года, пришла на смену другой программе, название которой так и осталось нераскрытым, — она была отнесена к секретным проектам.

Поскольку агентам ФБР не нравились системы Solaris, и они хотели работать с чем-нибудь попроще, под эгидой ФБР началась разработка проекта с кодовым названием «Phile Troenix». (Есть одна экзотическая пальма, которая носит название Phile Troenix, однако никто на самом деле не знает, чем руководствовалось ФБР и его подрядчики, присваивая

проекту такое имя.) Система Phiple Troenix, переименованная в конце концов, в Carnivore, предназначалась для работы на компьютерах под управлением Windows NT. На проект по переносу Omnivore на новую платформу и обучение персонала для работы с ней было выделено 800 000 долларов из бюджета.

В первой версии Carnivore было много ошибок, поэтому она явились поводом для разработки нового проекта «Enhanced Carnivore» в ноябре 1999 года. Согласно документам, обнародованным по Закону о свободе информации, в версии 2.0 и 3.0 планировалось добавление новых функций, таких как, например, прослушивание переговоров по протоколу передачи голосовых данных через Интернет.

Система Carnivore устанавливалась на компьютеры класса Pentium III под управлением Windows NT с сетевыми картами на 10/100 Мбит/с и приводами Iomega Jaz для записи перехваченных данных (привод закрывался на замок, чтобы не допустить несанкционированный доступ к Jaz-дискетам). Компьютер с установленной системой Carnivore подключался к сети провайдера услуг Интернета при помощи сетевого ответления Shomiti. Помимо операционной системы и наблюдательного ПО на компьютере была установлена копия программы pcAnywhere для обеспечения возможности удаленного доступа к компьютеру по телефонной линии для агентов ФБР.

Работой по установке и настройке системы занимались технические специалисты из ФБР, в их задачи входило задание IP-адреса или электронного почтового ящика подозреваемого, за которым нужно было вести наблюдение (могли быть также использованы различные фильтры). Система Carnivore осуществляла наблюдение за сетевым трафиком, сохраняя только те сетевые пакеты, которые были направлены с адреса (либо на него). Все остальные передаваемые по сети данные просто игнорировались.

Все перехваченные данные записывались на Jaz-диск емкостью 2 Гб. Этот диск регулярно извлекался из привода уполномоченным агентом, который ставил на нем дату и помещал в опечатанный контейнер, в соответствии с принципами ограничения круга лиц, имеющих доступ к уликам (об этих принципах мы говорили в главе 5). После этого проводилась экспертиза доказательств при помощи других утилит из пакета DragonWare с целью определения возможности использования их против подозреваемого.

После завершения наблюдения (обычно суд предоставляет 30-дневный срок на проведение подобного мониторинга) это оборудование должно быть удалено из сети провайдера услуг Интернета.

## Carnivore: дискуссии и контрмеры

Зашитников права на неприкасаемость частной жизни больше всего беспокоит то, что система Carnivore фактически имеет доступ ко всему входящему и исходящему сетевому трафику, включая трафик пользователей, не имеющих никакого отношения к расследуемому преступлению и не упоминаемых в судебном ордере.

Когда в 2000 году благодаря утечке информации общественности стало известно о существовании системы Carnivore, имел место всплеск публичной активности в связи с возможными нарушениями гражданских свобод. (ФБР удивил такой поворот событий, поскольку за предыдущий год бюро прибегало к использованию 20 установленных ими систем Carnivore всего несколько десятков раз.)

Из-за возникших дебатов ФБР разрешило провести независимое изучение системы Carnivore, выбрав для этих целей Иллинойский технологический институт. (Поборников права на неприкосновенность частной жизни не удовлетворил ход событий, поскольку само исследование прошло полтора месяца, а группа аналитиков состояла в основном из представителей правительства, включая лиц, работавших ранее в Министерстве юстиции, Управлении национальной безопасности и Министерстве обороны.)

Последняя редакция отчета увидела свет в декабре 2000 года, в результате чего покров секретности, окутывавший детали технической реализации проекта Carnivore, был сорван, и разговоры вокруг него постепенно начали утихать (этот отчет можно просмотреть на сайте [www.cdt.org/security/carnivore/001214carniv\\_final.pdf](http://www.cdt.org/security/carnivore/001214carniv_final.pdf)). Тем не менее система Carnivore повторно проявила себя весной 2002 года, когда выяснилось, что в ходе расследования террористической деятельности перехватывались и сохранялись электронные послания частных лиц, не значащихся в ордере на прослушивание. Во внутренних докладных записках ФБР значилось, что система Carnivore имела тенденцию к «некорректному сбору информации», и отмечалось, что «такой несанкционированный перехват не только нарушает права граждан на неприкосновенность частной жизни, но и способен серьезно помешать проведению расследований», и, в конце концов, признавалась незаконность подобного способа сбора информации.

В рамках борьбы с терроризмом ФБР продолжило использование системы Carnivore, причем, возможно, даже в более широких масштабах. И хотя, будем надеяться, что ошибки, связанные со сбором лишней информации, были исправлены, потенциальная угроза злоупотреблений по-прежнему существует. Все стандартные контрмеры, используемые для предотвращения других форм шпионажа, могут с успехом применяться для ограничения эффективности системы Carnivore. К подобным контрмерам относится использование шифрования, служб анонимной пересылки почты и использование анонимных прокси-серверов.

Для той категории наших читателей, которые работают в правоохранительных органах, заметим, что приводимые здесь контрмеры не относятся к категории ноу-хау, поэтому мы ни в коем случае не учим «плохих парней», как избежать правосудия, – все это известно и без нас. На самом деле преступники и террористы постоянно расширяют применение новых технологий, которые призваны помешать вашим попыткам установления законности. Даже если применение некоторых средств обеспечения неприкосновенности частной информации будет запрещено

законодательно, это не остановит людей, и без того нарушающих закон. Об этой «особенности» шпионажа лучше знать заранее, чтобы быть готовыми к изменению техники проведения расследований в случае столкновения с технически грамотными подозреваемыми.



Более подробную информацию о системе Carnivore можно найти на сайте американской правозащитной организации Electronic Privacy Information Center по адресу [www.epic.org/privacy/carnivore/](http://www.epic.org/privacy/carnivore/).

## Magic Lantern

ФБР, прияя к выводу о том, что будущее принадлежит цифровым средствам связи, попыталось идти нога в ногу с развивающимися технологиями. К концу 2001 года всплыла информация еще об одном наблюдательном проекте ФБР под названием Magic Lantern. Согласно информации, которую предоставило Федеральное бюро, Magic Lantern представлял собой «рабочий проект» (прототип), который мог бы получить дальнейшее развитие. Из кратких описаний проекта следовало, что он представляет собой троянское приложение, предназначенное для установки на компьютер подозреваемого с целью мониторинга клавиатуры и сбора доказательств. Разница между этим keylogger-приложением и программой, использовавшейся в деле Скарфо, заключалась в том, что агенту не нужен был физический доступ к целевому компьютеру; этот троянский конь мог устанавливаться дистанционно, через запуск вложений электронной почты либо путем использования других уязвимых мест системы защиты ОС Windows.

### Тактика: авторы Magic Lantern – сексуальные агрессоры?

Патрика Нотона можно назвать интернет-вундеркиндом. В 1998 году он начал работать в компании Sun Microsystems в команде разработчиков на Java. Во время всеобщей одержимости Интернетом он также работал в должности президента и главного технического специалиста компании Starwave, занимающейся разработкой веб-сайтов. Затем он перешел на службу в компанию Infoseek, которая позднее была приобретена компанией Disney. В свои 34 года во время «золотой лихорадки», охватившей Интернет и все, что с ним связано, он был «птицей высокого полета», занимая должность исполнительного вице-президента проекта Go Network компании Disney.

Мир вокруг Нотона начал рушиться в сентябре 1999 года, когда агенты ФБР задержали его по обвинению в нарушении нескольких федеральных законов, касающихся сексуальных домогательств к несовершеннолетним. До этого в течение нескольких месяцев Нотон общался в чате с человеком, выдающим себя за 13-летнюю девочку, которой Нотон назначил встречу в Санта-Моника Пир. Но вместо того, чтобы провести этот день в снятой неподалеку комнате отеля, он оказался за решеткой в результате проведенной ФБР операции. В ходе расследования на компьютере Нотона также были обнаружены фотографии с детской порнографией.

Патрик Нотон признал себя виновным и был приговорен к 5 годам испытательного срока и 9 месяцам домашнего ареста. Кроме того, его обязали при переезде на новое место жительства либо смене работы указывать факт своего привлечения по статье о сексуальных домогательствах к несовершеннолетним. На этом историю можно было бы закончить, если бы ни документы, обнародованные лос-анджелесским федеральным судом в августе 2000 года.

В рамках сделки между Нотоном и правительством он разработал для ФБР пять программных продуктов. Всего в обмен на избавление от тюремного заключения Нотон проработал на ФБР более 1000 часов.

Хотя детали работы, которую выполнял Нотон для ФБР, не подлежали разглашению, однако запрос, поданный журналом San Jose Mercury News, позволил пролить некоторый свет на разработанные Нотоном приложения. Выяснилось, что им были написаны: утилита для сравнения изображений, программа для отслеживания сервера, использовавшегося для отправки того или иного электронного письма либо размещения веб-страницы, программа для записи в журнал сессий чатов и еще один программный пакет, предназначенный для обнаружения закодированных стеганографических посланий.

Все эти инструменты предназначались для расследования преступлений, связанных с распространением детской порнографии и действиями сексуальных агрессоров, однако наиболее интересной оказалась его пятая программа. Нотон создал для ФБР «скелет» приложения, предназначенного для получения удаленного доступа к компьютерам с целью поиска на них информации.

Имеет ли это дело какое-то отношение к проекту Magic Laptop – неизвестно. Представитель Министерства обороны заявил в интервью репортерам Mercury News: «Детали этого дела засекречены. И, кроме того, разглашение подробностей использования таких приложений может снизить эффективность их применения в будущем».

О проекте Magic Lantern ходит великое множество слухов. К примеру, считается, что первым разработчиком проекта являлась компания Codex Data Systems, а сам программный продукт основан на утилите их собственной разработки Data Interception by Remote Transmission (D.I.R.T). Франк Джонс, глава компании Codex, пытался продать программу D.I.R.T различным полицейским управлениям. К сожалению, многие федеральные управление (как и иностранные правительства) совершенно упустили из виду тот факт, что Джонс в свое время был уволен из полиции Нью-Йорка и признан виновным в совершении уголовных преступлений, а в настоящее время он находится на испытательном сроке в связи с незаконным владением устройствами наблюдения. До этого он довольно долго занимался продажей товаров в сфере обеспечения безопасности компьютерных систем, которые многие эксперты считали абсолютно бесполезными. (Джонс, называвший себя «королем шпионов» (SpyKing), избежал заключения в тюрьме, заявив, что незаконные действия были вызваны его психическим состоянием. Судя по всему, вскоре после вынесения приговора он продолжил заниматься противозаконной деятельностью. Офицеру полиции, осуществлявшему надзор за условно осужденным Джонсом, был вынесен суровый выговор за то, что он упустил из виду многочисленные нарушения Джонсом правил условного осуждения.) По этой причине весьма сомнительно, чтобы ФБР использовало в своих целях программу D.I.R.T., хотя, как известно, с преступниками, осужденными за высокотехнологичные преступления, в Бюро происходят странные вещи.

Как и в случае с проектом Carnivore, обнародование сведений о проекте Magic Lantern возбудило общественные дебаты. Представители популярных компаний по производству антивирусного программного обеспечения, таких как Symantec (Norton Antivirus) и McAfee, заявили вначале, что их программы, дабы не мешать проведению расследований, не станут обнаруживать программный код системы Magic Lantern (затем эти решения были ими отменены), тогда как другие производители антивирусного и антитроянского ПО однозначно возразили, что не собираются скрывать от своих пользователей наличие шпионского ПО на их компьютерах. (На самом деле система Magic Lantern использовалась настолько редко, что производителям антивирусного ПО вряд ли удалось бы заполучить работающий программный код системы для добавления в базу данных известных троянских коней.)

После появления первых сведений о проекте Magic Lantern никакой новой информации по данной системе либо другим наблюдательным проектам ФБР не появлялось. Хотя к системе Magic Lantern и некоторым другим проектам ФБР в сфере компьютерного наблюдения имеет доступ ряд лиц, не связанных с правительством, вам для защиты от таких программ достаточно будет применить контрмеры по обнаружению и обезвреживанию наблюдательного ПО, описанные в главе 9 (ну и, конечно, не помешают коммерческие продукты для сканирования систем на предмет наличия враждебного ПО).



На веб-сайте Джона Янга также размещена информация по проектам D.I.R.T. и Magic Lantern (включая действующую копию системы D.I.R.T., которая, судя по всему, основана на известной программе Back Orifice). Посетите веб-страницы по адресу <http://cryptome.org/dirt-guide.htm>, [cryptome.org/dirty-lantern.htm](http://cryptome.org/dirty-lantern.htm) и [cryptome.org/dirty-secrets2.htm](http://cryptome.org/dirty-secrets2.htm).

## Модификация приложений и компонентов операционной системы

Еще один, более сложный способ получения доступа к конфиденциальной информации заключается в подмене приложений либо компонентов операционной системы (например, библиотек) их модифицированными версиями, которые либо допускают утечку информации, либо делают информацию уязвимой для атак. Модифицированные исполняемые файлы могут применяться в следующих целях:

- для ослабления шифровального ПО (использование слабых мест в алгоритме либо добавление дополнительных ключей, делающих шифрование нестойким);
- для разрешения несанкционированных сетевых действий (к примеру, модифицированная версия брандмауэра, тайно разрешающая определенные соединения);
- для тайного сбора информации (например, мониторинг клавиатуры).

Модифицированные исполняемые файлы и библиотеки нередко имеют троянскими конями или программами «с запасным входом», однако важно отметить различия между такими модифицированными файлами и троянскими приложениями, которые обсуждались в главе 9. Простейшие троянские приложения подменяют функции операционной системы «на лету», перехватывая вызов Windows API. Это подразумевает выполнение дополнительного кода до или после обращения к Windows API. Реализовать подобные «ловушки» несложно, однако для их работы необходимо вначале запустить враждебное приложение.

Более сложный подход подразумевает модификацию копии исполняемого файла с последующей заменой оригинальной версии на эту копию на целевом компьютере. Замена может осуществляться либо при наличии физического доступа к этому компьютеру, либо путем использования известных уязвимых мест в системе защиты сети.

Существует два способа модификации компонентов приложения или операционной системы:

- **Перекомпиляция исходных кодов.** В этом случае изменения вносятся в исходный код, после чего перекомпилируется исполняемый файл или библиотека (даже если в вашем распоряжении отсутствует исходный код, вы все равно можете создать модифицированную версию).
- **Модификация самого исполняемого файла.** Для этого используется редактор шестнадцатеричных кодов, при помощи которого изменяются ассемблерные инструкции внутри исполняемого файла. Вначале такой файл дизассемблируется, чтобы выяснить, какие инструкции необходимо модифицировать.

Некоторые пользователи полагают, что применение программного обеспечения, распространение исходных кодов которого запрещено, как, например, операционной системы Windows, представляет меньшую опасность в этом плане, чем применение операционной системы Linux, к примеру, которая распространяется свободно по принципу открытого кода. Основным аргументом в данном споре выступает тот факт, что, располагая исходными кодами программы, внести изменения в код намного проще, после чего вам останется только перекомпилировать программу и подменить файл на компьютере ничего не подозревающей жертвы.

Конечно, наличие исходных кодов облегчает процесс внесения изменений в файлы приложений и операционной системы в целях шпионажа, однако его отсутствие не в состоянии остановить опытного противника. Все, что необходимо в этом случае, – знание ассемблера, наличие программы дизассемблирования и транслятора; и вы можете разобрать программу на кусочки, модифицировать то, что вам нужно, заново перекомпилировать и подменить оригиналный файл на компьютере жертвы. (Помимо программ дизассемблирования, выводящих программный код на ассемблере, существуют также декомпиляторы, позволяющие восстанавливать из исполняемого двоичного файла программный код на языках высокого уровня, таких как С.)

У вас могло создаться впечатление, что подобная работа требует глубоких технических знаний, хотя на самом деле это не совсем так. Обратное проектирование (*reverse-engineering*) программного кода появилось еще на заре компьютерной эпохи, когда программисты взламывали схемы защиты программного обеспечения в играх и других приложениях. Сеть Интернет предоставляет в ваше распоряжение массу утилит для обратного проектирования двоичного исполняемого кода, а также широкую инфраструктуру для всех заинтересованных в дизассемблировании и повторной сборке приложений. И хотя вы, возможно, слышали о многих выдающихся программах, преуспевших в сфере обратного проектирования, однако в данном контексте качество «выдающийся» не так критично для эффективности процесса.

(Если нам все еще не удалось убедить вас в слабой устойчивости Windows перед подобными видами атак, посетите сайт [www.rootkit.com](http://www.rootkit.com), где вы сможете узнать о некоторых практических примерах и увидеть образцы программного кода. Вы, должно быть, очень удивитесь.)

## Тактика: патриотический долг?

Время от времени появляются слухи о том, что высокотехнологичные компании вступают в сотрудничество с правительственные организациями, чтобы облегчить им решение задач шпионажа за клиентами подобных компаний. В конце концов, все это выглядит достаточно патриотично (особенно после событий 11 сентября).

Разведывательные управления имеют немалый опыт в плане нарушения законов с целью шпионажа за американскими гражданами, причем иногда в добровольном сотрудничестве с американскими корпорациями.

В 1945 году организация-предшественник Управления национальной безопасности заключила партнерские договоры с RCA, ITT и Western Union по поводу передачи копий всех телеграфных сообщений, приходящих из-за границы и отправляемых за пределы Соединенных Штатов. В рамках операции «Трилистник» (Shamrock) ежемесячно на анализ в разведывательные управление передавалось до 150 000 сообщений. Такой незаконный шпионаж продолжался вплоть до 1975 года, когда об этой операции стало известно из слушаний в Конгрессе.

Имеют ли место подобные действия сегодня? Достоверно об этом известно только правительству Соединенных Штатов, мы просто поведаем вам о последних весьма любопытных фактах.

В 1997 году в одной из шведских газет промелькнуло упоминание о том, что использующееся в системе Lotus Notes шифрование легко может быть взломано американским правительством. Напомним, что на тот момент на все программные продукты, продаваемые за границу, налагались суровые экспортные ограничения. Тогда как 64-битовое шифрование, реализованное в программе Lotus Notes, могло использоваться на территории Соединенных Штатов, очевидно, что в экспортной версии программы, которая также поддерживала 64-битовое шифрование, содержался некий подвох. Цитируем Элена Руддена, вице-президента компании Lotus: «Различия между версией Lotus Notes, продаваемой на территории Соединенных Штатов, и ее экспортным вариантом заключаются в уровне шифрования. 64-битовые ключи шифрования доступны в обеих версиях, однако 24 бита ключа из экспортной версии находятся на хранении у правительства США. Таким образом обстоят дела сегодня». Шведов не слишком обрадовала эта новость. Правительственное учреждение США, на хранении у которого находились эти ключи, названо не было.

В сентябре 1999 года один из исследователей в области безопасности обнаружил, что в криптографическом API от Microsoft имеется недокументированный ключ под названием NSAKEY. В адрес компании Microsoft посыпались обвинения в том, что она разместила в своих операционных системах запасные входы для Управления национальной безопасности и других правительственные управлений. Компания по производству программных продуктов отвергла все обвинения, заявив, что ключ был назван так потому, что Управление национальной безопасности (NSA) контролировало экспорт технологий шифрования, и этот ключ здесь присутствует исключительно для согласования с экспортными законами США. По утверждениям Microsoft, ключ NSAKEY является просто резервной копией одного из ключей, используемого компанией исключительно с целью обновления компонентов криптографической системы. Компания просит прощения за название для ключа, выбранное не лучшим образом, и подчеркивает, что все обвинения в ее адрес выглядят довольно иронично, поскольку Microsoft в свое время выступала категорически против предлагаемой правительством политики условного депонирования ключей. (Согласно информации, предоставленной журналистом Уэйном Мэдсеном, в 2001 году на Межведомственном техническом форуме, проходившем в Национальном институте стандартов и технологий (NIST), начальник отдела Microsoft по безопасности мобильных кодов сообщил о том, что компания содержит полноценный офис в штаб-квартире Управления национальной безопасности, где работает персонал, имеющий доступ к секретной информации.)

Любопытно отметить, что еще в 1995 году в июньском выпуске журнала *Computer Fraud & Security Bulletin* Мэдсен, бывший сотрудник Управления национальной безопасности, написал, что компании Microsoft и Lotus только что завершили подписание соглашений с Управлением национальной безопасности, которые затрагивают вопросы защиты информации в их продуктах.

Основная методика защиты от подобного рода атак заключается в использовании алгоритма MD5 для хеширования значений только что установленных из надежных источников программных продуктов и библиотек. Впоследствии вам придется регулярно проверять хешированные значения и сравнивать их с текущими. Если значение изменилось без видимых причин, значит, этот файл был модифицирован в целях шпионажа.

Кроме того, необходимо зашифровать список хешированных значений и хранить его в безопасном месте. Если шпион осуществит подмену системного файла его модифициированной версией, он в первую очередь займется поиском на жестком диске файлов с хешированными значениями, чтобы изменить старое хешированное значение на новое, соответствующее

модифицированному файлу. Таким образом, пользователь во время очередной проверки хешированных значений не сможет определить, что модификации подверглись оба файла.



В течение пяти лет некий европеец, известный под псевдонимом Fravia, занимался поддержкой веб-сайта, на котором размещена масса информации по теме обратного проектирования. Сайт содержит обучающие материалы и эссе, написанные опытными «аналитиками» по дизассемблированию и последующей рекомпиляции приложений. С 2000 года Fjalar Ravia тратит свою энергию на овладение нюансами поиска информации в сети Интернет. Его сайт [www.fravia.com](http://www.fravia.com) стоит посетить любому шпиону, которого не удовлетворяют возможности поисковых серверов. Зеркала сайта можно встретить буквально повсюду, одно из них находится по адресу <http://tsehp.cjb.net/>. (Помните, что американский Закон о соблюдении авторских прав на цифровую интеллектуальную собственность запрещает обратное проектирование.)

## Разведывательные вирусы и «черви»

В связи с повсеместным распространением Интернета, в распоряжении шпионов появились такие средства, которые отсутствовали еще лет пять–десять назад. Широкие возможности в плане получения доступа к конфиденциальной информации предоставляют так называемые программы-вирусы и черви.

Существуют некоторые различия между разведывательными вирусами и «червями», с одной стороны, и обычными вирусами – с другой. С последними вы сталкиваетесь либо, по крайней мере, слышите о них буквально каждый день:

- **Разведывательные вирусы и «черви» предназначены для тайного сбора информации.** Единственной целью такого программного кода является незаметная кража информации; разработчик не желает, чтобы его творение стало достоянием общественности. В отличие от большинства обычных вирусов и «червей», программный код целевых вирусов намного сложнее и лучше «вылизан». Для проникновения в систему в них могут использоваться различные уязвимые места в отличие от единственного способа, применяемого в большинстве обычных вирусов. Разведывательный вирус может попытаться завершить работу любого защитного программного обеспечения, способного помешать выполнению его миссии.

- Целью атаки разведывательных вирусов и «червей» обычно служат отдельные лица либо организации. В отличие от традиционного вредительского программного кода, который обычно просто использует подвернувшиеся благоприятные возможности, разведывательные программы действуют более избирательно, и в этом смысле их можно сравнить с управляемыми ракетами. Перед началом атаки программный код может проверять ключи реестра на предмет соответствия данного компьютера профилю целевого объекта. Целевые атаки также означают меньший риск обнаружения разведывательного вируса или «червя», поскольку появление такого вируса на ограниченном числе компьютеров пройдет незамеченным для производителей антивирусного ПО. (Концепция целевых атак может применяться не только в целях шпионажа, но и в рамках информационной войны. В качестве примера можно привести программный код, выполняющий проверку локализации версии Windows и атакующий только арабские версии.)

Хотя пока мы не можем достоверно заявлять о существовании подобных разведывательных программ, разработанных правительством либо организациями, вовлеченными в шпионские операции высокого уровня, потенциально это возможно. На практике уже имели место интернет-атаки различной сложности. Очевидно, что все шпионские атаки похожи по своей природе, просто менее масштабные и более целенаправленные операции не так заметны, не имеют общественного резонанса и не попадают на первые полосы газет.

## Вирусы и «черви»

Вирусом называется приложение, предназначенное для выполнения специфических действий и распространяющееся путем инфицирования других программ или файлов. «Червь» по своим действиям напоминает вирус, но при этом он не занимается заражением других файлов. Проблема состоит в том, что даже производители антивирусного ПО не всегда в состоянии провести четкую грань между этими двумя типами вредоносного кода. В нашем обсуждении мы не станем четко разграничивать их, считая, что оба типа программ занимаются самовоспроизведением и предназначены для выполнения враждебных действий, о которых ничего не известно пользователю компьютера.

Цель разведывательных червей или вирусов – распространиться, собрать информацию с зараженных компьютеров и отправить отчет назад своему создателю (по электронной почте, FTP, через группы новостей USENET, по факсу, подключением к сетевому принтеру либо любым другим способом электронной передачи данных). Приложение может атаковать все компьютеры подряд либо выбирать определенные цели. Например, если вы занимаетесь промышленным шпионажем против корпорации IBM, вы можете задействовать вирус, который крадет документы, предварительно

проверяя, на какую компанию зарегистрирована копия пакета Microsoft Office. Если в качестве имени организации значится IBM или нечто похожее, вирус скопирует этот документ и отошлет его удаленному получателю. Если же офисные приложения зарегистрированы на другую компанию, вирус удалит себя и следы своего присутствия (и, возможно даже, не станет распространяться далее).

По сети Интернет реально вот уже несколько лет разгуливает ряд разведывательных вирусов и «червей», о которых мы расскажем вам в следующих разделах.

## CALIGULA

В 1997 году я написал статью о возможностях практических атак против программы PGP (посетите мою веб-страничку по адресу [www.privacy.com.au/pgpatk.html](http://www.privacy.com.au/pgpatk.html)). Один из предложенных мною вариантов носил название «Вирусы с включенной опцией шпионажа» и предназначался для сбора и кражи информации. Я допустил возможность существования вируса, активизирующегося только на тех компьютерах, где установлена программа PGP. Разве я мог предположить, что спустя несколько лет моя идея будет превращена в живой вирус, а моя фамилия – значиться в списке благодарностей.

В феврале 1999 года средства массовой информации сообщили о появлении нового вируса Caligula, написанного неким Opic из ныне распавшейся группы создателей вирусов под названием CodeBreakers. Caligula стал одним из первых разведывательных вирусов, заслуживших мировую известность, и его целью являлись пользователи пакета PGP. Макро-вирус Word осуществлял поиск программы PGP на жестком диске компьютера. В случае обнаружения утилиты вирус подключался к удаленному FTP-серверу и загружал набор секретных ключей пользователя. По-видимому, к зашифрованным при помощи PGP данным применялась словарная атака на случай использования ненадежного пароля. При взломе пароля зашифрованная почта пользователя могла быть скомпрометирована.

В интервью массмедиа Opic заявил, что разработанный им вирус являлся проверочным, предназначенным исключительно для демонстрации уязвимых мест PGP. Неизвестно, сколько наборов ключей PGP было скопировано и сколько атак увенчались успехом. (Архивная версия веб-страницы Opic, содержащая информацию об этом вирусе, размещена по адресу <http://web.archive.org/web/19990221015817/http://members.tripod.com/opiccb/index.htm.>)

## MARKER

Через несколько месяцев после появления вируса Caligula стало известно о существовании еще одного вируса от группы CodeBreakers. Он получил название Marker (из-за строки в начале кода «this is a marker»). Вирус запрашивал имя владельца зарегистрированной копии Microsoft Word и

записывал дату инфицирования цели. Первого числа каждого месяца вирус пытался подключиться к FTP-серверу группы CodeBreakers для отправки собранной информации. Опять-таки, данный вирус был отнесен к разряду проверочных, поскольку он только определял процент зараженных компьютеров и общее количество распространившихся копий. Автором вируса Marker оказался 17-летний хакер под псевдонимом Spooky, прекративший заниматься написанием вирусов, когда стало известно о заражении компьютеров организации Blue Cross\*. «Должны же существовать какие-то рамки, а я считаю, что своих я уже достиг», – объяснил он на своем веб-сайте напоследок.

### Тактика: вирус Далай-лама

В сентябре 2002 года менеджер тибетского компьютерного центра в Дхармсала, Индия, обвинил китайское правительство в разработке и распространении вируса, предназначенного для кражи информации. Получателями вируса стали группы активистов по всему миру, тогда как в качестве отправителя значился именно этот компьютерный центр. По заявлению менеджера центра, вирус был разработан таким образом, чтобы отправлять собранные данные на шесть электронных почтовых ящиков в Китае, включая несколько университетов и государственных институтов. По-видимому, злоумышленники отсылали инфицированные электронные письма в двух различных случаях.

Китайское правительство отвергло все обвинения, заявив, что оно всегда выступало против хакеров. Копии вируса так и не появились в сети Интернет, так что дать независимую оценку того, являлся ли этот вирус шпионским, не представляется возможным. Исходя из его описания, можно сделать вывод, что он принадлежал к вирусам типа SirCam, и его целью являлись не только организации, поддерживающие Далай-ламу. Тем не менее, принимая во внимание антипатию китайского правительства по отношению к движению Свободный Тибет и заинтересованность в технологиях проведения информационных войн, можно сделать вывод, что вероятность того, что эта атака являлась целенаправленной, достаточно велика.

### SIRCAM

В июле 2001 года по Интернету быстрыми темпами распространился червь под названием SirCam. Заражение происходило в тот момент, когда ничего не подозревающий пользователь открывал вложение в электронном письме следующего содержания: «Привет! Как дела? Я посылаю тебе этот файл, потому что мне нужен совет. Заранее благодарю. Пока!» (Ра-

\* Национальная сеть компаний страховой медицины в США. – Прим. перев.

зумеется, письмо было написано на английском, а в качестве отправителя якобы выступал кто-то из друзей или знакомых получателя, поскольку адрес выбирался из инфицированной адресной книги. Но, если честно, сколько ваших знакомых, друзей или деловых партнеров могут отправить письмо подобного содержания? Так что перед вами яркий пример использования приемов социотехники.)

После открытия вложения «червь» копировал случайным образом выбранный документ (в формате .DOC, .XLS или .ZIP) с инфицированного компьютера и отправлял письмо с вложением зараженного файла людям из вашей адресной книги.

Несколько месяцев вирус SirCam терроризировал пользователей Интернета, перегружая трафик посланиями электронной почты, содержащими инфицированные личные и деловые документы, которые отсылались посторонним лицам. Среди жертв вируса оказался Центр защиты национальной инфраструктуры ФБР, ряд личных документов из которого был разослан людям за пределами Бюро. ФБР поспешило заявить, что никакой утечки секретной либо конфиденциальной информации не произошло.

## BADTRANS.B

В ноябре 2001 еще один разведывательный «червь» начал терроризировать пользователей Интернета. «Червь» под названием Badtrans.B (разновидность вируса Badtrans, появившегося в апреле того же года) после открытия вложений электронной почты начинал выполнение серьезных шпионских операций. После запуска «чертви», он распространялся дальше по электронной почте, используя электронные адреса из адресной книги Outlook. Червь устанавливал программу мониторинга клавиатуры, предназначенную для записи паролей к ящикам электронной почты, FTP-серверам, службам Telnet и к бюджетам пользователей веб. Помимо паролей, keylogger мог записывать любую другую информацию, набираемую пользователем.

Собранныю информацию вирус Badtrans отсылал на один из двадцати ящиков электронной почты, открытых на бесплатных почтовых серверах. Один из таких адресов выглядел как s\*#!\_me\_p\$#\*%@ijustgotfired.com. Сообщения с зараженных компьютеров начали поступать на этот адрес где-то после обеда 24 ноября. Вскоре максимальный объем ящика был превышен, что повлекло за собой отключение данного бюджета. На следующий день, пытаясь определить причину, по которой сервер работает слишком медленно, системный администратор обнаружил, что на этот электронный почтовый ящик приходит около сотни сообщений в минуту. Дальнейшее расследование показало, что вирус Badtrans вызвал отправку конфиденциальной информации с более чем 100 000 компьютеров только за первый день своего существования.

Провайдер услуг Интернета MonkeyBrains.net, владелец домена ijustgotfired.com, вскоре определил, что происходит, и начал собирать все входящие сообщения электронной почты. Руди Ракер-младший, глава компании, организовал базу данных всех присланных вирусом документов. До-

ступ к этой базе можно было получить непосредственно со специально созданной веб-страницы. Новость о происходящем распространилась чрезвычайно быстро, и Ракеру пришлось отключить некоторые функции просмотра данных.

Вскоре и ФБР узнало о сайте Ракера, запросив копию нескольких гигабайт конфиденциальных данных, присланных провайдеру MonkeyBrains, включая около 1 500 000 сведений о бюджетах и паролях пользователей, около 6 000 000 запротоколированных сеансов работы в сети и более 300 000 адресов электронных почтовых ящиков, инфицированных этим вирусом. Однако Ракер отказал ФБР в предоставлении подобного рода информации без наличия соответствующего ордера, сославшись на то, что речь идет о соблюдении права на неприкосновенность частной жизни сотен тысяч людей, и без того пострадавших от вируса.

Червь Badtrans. В стал классическим примером быстроты распространения подобных вирусов и их возможностей в плане сбора информации. Подвергшаяся обработке версия базы данных Ракера, где вы сможете найти немало любопытной информации, по-прежнему доступна онлайн по адресу: <http://badtrans.monkeybrains.net/>.

## БУДУЩЕЕ ВИРУСОВ

Очевидно, что с обнаружением новых уязвимых мест в системе защиты операционной системы Windows создатели вирусов и червей постараются извлечь из них максимум «пользы». Кроме того, ряд новых, быстро развивающихся технологий может представить в ближайшем будущем немало дополнительных возможностей в плане организации разведывательных атак, направленных на сбор информации.

- **Мобильные устройства.** Пока что такие мобильные устройства, как, например, сотовые телефоны, не являются целью авторов вирусов, однако это всего лишь вопрос времени. Поскольку в них все чаще интегрируются функции КПК, перспективы разработки шпионских вирусов, предназначенных для кражи информации из адресных книг, организеров и других приложений, становятся все более реальными.
- **«IP everywhere».** Пока что видимые лишь сквозь призму хрустального шара будущего перспективы различного рода продуктов с интегрированными IP-функциями в домашних или корпоративных решениях представляют огромный потенциал в плане шпионажа. Речь идет не только о краже информации с тех или иных устройств, но также и об уязвимых местах в защите сетей в целом. Учитывая, что обычно новые технологии обладают ощутимыми прорехами в плане обеспечения безопасности, можно предположить, что с повсеместным распространением компьютерных устройств «IP everywhere» вам придется вести себя очень осторожно.

## Контрмеры

Хотя антивирусные утилиты, программы, предназначенные для обнаружения троянских коней, и брандмауэры предоставляют первичную защиту от разведывательных вирусов и червей, серьезный противник, без сомнения, воспользуется модифицированными пользовательскими фрагментами кода, дабы избежать обнаружения со стороны коммерческих программ, предназначенных для защиты информации.

Вы можете уменьшить шансы превратиться в жертву, если будете придерживаться строгой политики безопасности (в особенности при работе с электронной почтой), а также использовать программы мониторинга сетевых подключений, системного реестра и файловой записи. (Соответствующие политики и утилиты обсуждались в разделах «Контрмеры» глав 8 и 9.)

Еще один способ минимизировать риски – избегать хранения конфиденциальной информации на компьютерах, которые являются потенциально уязвимыми к сетевым атакам. Для этого в военных и разведывательных управлениях используется концепция цветовой идентификации «красный/черный» (red/black). Красные компьютеры и сети считаются безопасными (они могут соответствовать стандартам TEMPEST, использовать зашифрованные виртуальные частные сети и т. п.). Черные компьютеры считаются небезопасными, то есть хранимой на них информации может угрожать опасность. Системы красных и черных компьютеров четко разделены между собой во избежание утечки секретной информации с красных систем на небезопасные черные системы.

Вам необязательно работать в штаб-квартире Управления национальной безопасности, чтобы принять должные меры для защиты собственного компьютера. Простейшая система, построенная в соответствии с концепцией «красный/черный», включает в себя «черный» компьютер, подключенный к некоторой сети, и «красный» компьютер, не подключенный ни к одной сети. Любые зашифрованные сообщения, принятые на небезопасный «черный» компьютер переносятся на «красный» компьютер вручную (на дискете, флэш-карте либо переносном USB-винчестере).

«Красный» компьютер используется для шифрования и дешифрования сообщений электронной почты и для работы с конфиденциальной информацией (только файлы данных, желательно в форматах, не поддерживающих присутствие макровирусов, должны переноситься с «черного» на «красный» компьютер). Использование промежуточного «черного» компьютера сводит на нет любые возможные сетевые угрозы компрометации конфиденциальной информации на безопасном компьютере. Разумеется, на обоих компьютерах должно быть установлено антивирусное ПО, программы для обнаружения троянских коней, брандмауэры и другие утилиты, предназначенные для обеспечения безопасности. (Конечно, использовать два компьютера не всегда удобно, однако такой подход позволяет предотвратить большинство удаленных атак в среде с высоким уровнем опасности.)

# Камеры наблюдения

Если вы обладаете физическим доступом к целевому объекту, одним из способов сбора конфиденциальной информации, включая пароли, является использование камер наблюдения. ФБР использовало скрытые видеокамеры во многих своих расследованиях, чтобы выяснить, чем шпион занимается за своим компьютером. Достаточно выбрать незаметное место (например, в подвесном потолке), направить камеру так, чтобы в ее объектив попадал компьютерный монитор и клавиатура, и подождать, пока камера не запишет что-нибудь интересное.

Скорее всего, вы будете использовать некоторое цифровое устройство, в котором все реализовано на одном кристалле, поэтому давайте вкратце обсудим существующие технологии. Цифровые и видеокамеры используют сенсоры, преобразующие свет в электрический заряд. Существует два типа сенсоров: приборы с зарядовой связью (ПЗС) и комплементарные металлооксидные полупроводники (КМОП).

## Контрмеры: техническое наблюдение

Технические контрмеры, направленные на предотвращение визуального наблюдения за вами, сводятся к обнаружению и отключению устройств наблюдения. Ранее речь шла преимущественно об аудиопрослушивании, однако сейчас не меньшую актуальность приобрело видеонаблюдение. (Учтите, что акустические «жучки» могут использоваться и для наблюдения за компьютерной техникой. К примеру, в ходе операции ENGULF, проводившейся еще в 50...60-х годах XX века, британцы расшифровывали закодированные французско-египетские переговоры по шуму, производимому шифровальной машиной. Атаки подобного рода могут быть организованы против матричных принтеров и клавиатур.)

Хорошим веб-ресурсом, который поможет вам в изучении устройств и технологий защиты от аудиовизуального наблюдения, является сайт компании Granite Island Group, размещенный по адресу [www.tscm.com](http://www.tscm.com). Поддерживаемый Джеймсом Эткинсоном, уважаемым профессионалом в данной области, этот сайт содержит массу детальной информации по аудиовизуальному наблюдению и защитным контрмерам.

- ПЗС-сенсор представляет собой набор крошечных диодов, осуществляющих преобразование фотонов (свет) в электроны (электрический заряд). На одном кристалле может быть размещено несколько сотен тысяч диодов.
- КМОП-сенсор работает почти так же, как его собрат с зарядовой связью, однако он в десять раз менее чувствителен и не позволяет

получать изображения с высоким разрешением. Основное его преимущество – малая стоимость и намного меньшая потребляемая мощность.

В отличие от «жучков», приспособленных для аудионаблюдений, которые передают сигнал в радиочастотном диапазоне и легко могут быть обнаружены при помощи анализатора спектра либо специального прибора для обнаружения «жучков», скрытые проводные камеры (иногда называемые системами кабельного мониторинга) не излучают радиосигнал, который можно было бы выявить при помощи обычных детекторов. Один из способов обнаружения скрытых камер наблюдения (не считая переворачивания всего вверх дном и разламывания стен) – использование ручного сканера теплового излучения. И камера, и ее источник питания обязательно будут видны на сканере, даже если они спрятаны в стене или за каким-то объектом. (Конечно, этот метод может и не сработать, в случае если вы стали объектом шпионажа со стороны разведки или правительства, которые могут позволить себе применение спецоборудования для аудиовизуального наблюдения, не обнаруживаемого стандартными средствами.)

## Веб-камеры

Хотя веб-камеры (небольшие камеры, предназначенные для передачи видео через Интернет) нельзя отнести к прогрессивным шпионским технологиям, они определенно могут использоваться в целях шпионажа и контршипионажа. В главе 9, если вы помните, мы говорили о троянских приложениях, способных перехватывать поступающий с видеокамеры сигнал и выполнять его удаленную ретрансляцию. В главе 11 вы убедились в том, что шпион с соответствующим оборудованием легко может осуществлять перехват сигнала от беспроводных видеокамер. Поэтому, применяя веб-камеру либо камеры подобного типа, не забывайте о том, что она может быть использована против вас.

Помимо удаленного перехвата видеосигнала от видеокамеры ничего не подозревающего пользователя, вы можете использовать веб-камеры для ведения локального наблюдения. Существует масса специальных приложений, которые позволяют превратить вашу веб-камеру в полноценную систему наблюдения, способную контролировать ваш дом или офис. В этих приложениях используется алгоритмы обнаружения движения, активизирующие видеокамеру, когда кто-то начинает перемещаться в ее зоне обзора (причем камера может находиться как внутри, так и снаружи помещения, за окном). Можно настроить программное обеспечение таким образом, чтобы в случае обнаружения камерой движения вам поступало уведомление по электронной почте либо в режиме реального времени вы бы принимали через Интернет изображение с камеры на удаленный компьютер.

## Шпионский инструментарий: камеры наблюдения в общественных местах

Видеокамеры наблюдения все чаще появляются на уличных столбах и снаружи зданий по всей территории Соединенных Штатов. С их помощью правоохранительные органы имеют возможность быстро реагировать на совершаемые преступления еще до того, как о них будет сообщено сознательными гражданами. Кроме того, видеозаписи могут служить в качестве доказательств при расследовании уголовных преступлений.

Камеры наблюдения могут и не подвергаться активному мониторингу (как, например, банкомат на территории банка, где видеосигнал записывается на кассету), либо, наоборот, изображение постоянно выводится на дисплей, за которым кто-то постоянно наблюдает. Возможно также удаленное управление камерой, так что работник охраны может изменить угол обзора камеры, увеличить или сфокусировать картинку на определенном человеке или ситуации.

Видеокамеры наблюдения стали неотъемлемой частью городского пейзажа в Англии (ведущей страны, если говорить о развитии видеонаблюдения в общественных местах). По оценкам некоторых бесприбыльных организаций, на сегодняшний день в Британии установлено от 1,5 до 2 миллионов видеокамер наблюдения. Лондонская наблюдательная группа Privacy International назвала сумму в 9 миллиардов долларов, которые были потрачены правительством на организацию и проведение наблюдательных операций за последние 15 лет.

Чтобы вы сами смогли оценить масштабы видеонаблюдения в США, сообщим вам, что в рамках проекта New York City Surveillance Camera было зарегистрировано местоположение более 2300 камер наблюдения, установленных в общественных местах только в самом Нью-Йорке и предназначенных для записи перемещений пешеходов и автомобилистов. (В это число входят только камеры, расположенные снаружи, а ведь сколько их установлено внутри зданий!) Карты и более подробную информацию о размещении видеокамер наблюдения в Нью-Йорке вы можете получить на официальном сайте проекта [www.mediaeater.com/cameras](http://www.mediaeater.com/cameras).

Хотя защитники наблюдательных проектов утверждают, что это помогает снизить преступность и облегчить расследование уже совершенных преступлений, поборники прав на неприкосновенность частной жизни не столь уверены в этом и считают установку камер очередным шагом, направленным на вмешательство в частную жизнь граждан. Более подробно тема установки видеокамер наблюдения в общественных местах в связи с соблюдением прав граждан на неприкосновенность частной жизни обсуждается на сайте [www.epic.org/privacy/surveillance/](http://www.epic.org/privacy/surveillance/).

Перечислим некоторые наиболее популярные программные утилиты для работы с веб-камерами:

- Digi-watcher, программный пакет за \$39, обладающий расширенными функциями журнала. Этот пакет можно найти на сайте [www.digi-watcher.com](http://www.digi-watcher.com).
- InetShepard, программа, которая записывает аудио- и видеосигнал и может управляться по телефонной линии. Версия для одной камеры стоит \$35, и ее можно заказать на сайте <http://inetshepherd.com>.



Информация о других продуктах, предназначенных для работы с веб-камерами, доступна на веб-сайте [www.webattack.com/shareware/webpublish/swwebcam.shtml](http://www.webattack.com/shareware/webpublish/swwebcam.shtml).

Конечно, качество передаваемой веб-камерой картинки не дотягивает до телевизионного, но для выполнения некоторых шпионских операций его бывает вполне достаточно. Тем не менее, если вы нуждаетесь в скрытой камере, способной выдавать высококачественное изображение, вам необходимо обратиться к категории камер, специально разработанных для наблюдения.

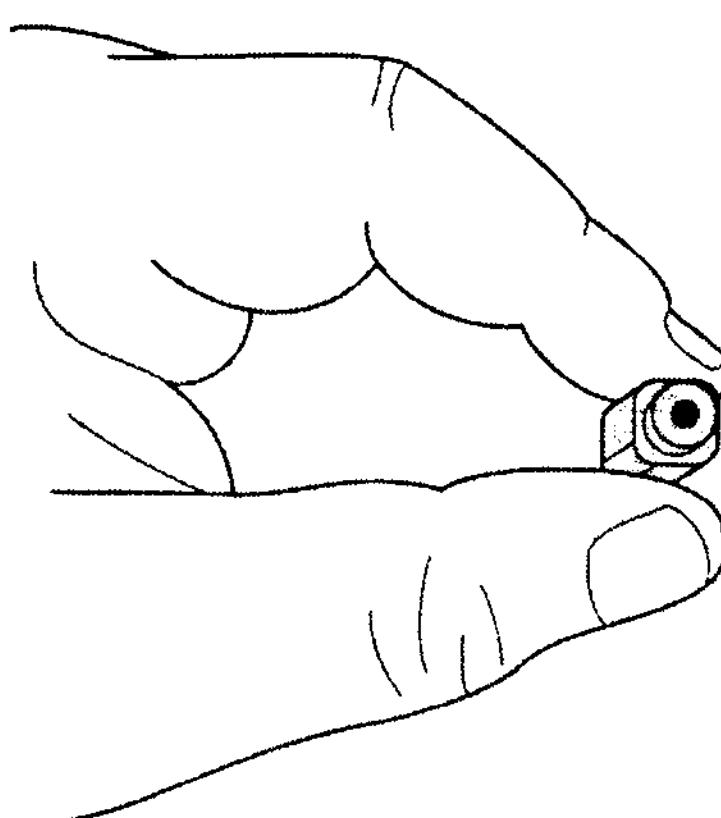
## Промышленные камеры наблюдения

Хотя для наблюдения можно использовать и веб-камеры, лучше всего прибегнуть к камерам промышленного производства, специально предназначенным для шпионских целей. Обычно подобные камеры имеют даже меньший размер, чем стандартная веб-камера (рис. 13.2), обладают большей разрешающей способностью и расширенными функциями, как, например, съемка в темноте. Такие миниатюрные камеры могут быть спрятаны в подвесном потолке, часах, терmostатах, радиопередатчиках, водораспыляющих головках системы противопожарной защиты и вообще практически везде, где вы только можете себе представить.

Большинство таких камер разработаны для использования с внешними источниками питания и вывода видеосигнала на кассетный видеомагнитофон. Возможны варианты с беспроводными камерами, что избавляет вас от необходимости подключать их непосредственно к магнитофону.



У правоохранительных органов и охранных компаний в плане видеонаблюдения пользуется популярностью компания SuperCircuits. Она занимается производством камер, магнитофонов, то есть практически всего, что может понадобиться для проведения видеонаблюдения. Онлайновый каталог продукции этой фирмы доступен на сайте [www.supercircuits.com](http://www.supercircuits.com).



**Рис. 13.2.** Миниатюрная черно-белая видеокамера SuperCircuits.

Эту камеру размером 1×1,5 см, передающую видеосигнал в формате NTSC, можно разместить практически где угодно. А благодаря стоимости всего \$99 ее может позволить себе даже шпион с весьма ограниченным бюджетом

Хотя, в соответствии с рядом федеральных законов, на продажу и использование устройств аудионаблюдения наложено множество ограничений, в плане продажи и производства устройств видеонаблюдения количество ограничений намного меньше. Сложные камеры и устройства записи видеосигнала доступны практически всем, причем по довольно разумным ценам. (Не забывайте при этом, что существуют законы на невмешательство в частную жизнь, запрещающие видеосъемку в определенных ситуациях.)

## Заключение

Отбросив форсмажорные ситуации (например, пожар, в котором бы сгорели все микросхемы на Земле), можно ожидать, что компьютерный шпионаж будет существовать всегда. По мере того как наша зависимость от компьютеров возрастает и они продолжают все глубже проникать в нашу повседневную жизнь, возможности шпионов и наблюдателей в плане шпионажа также увеличиваются.

Конечно, это не означает, что вам придется надевать на голову металлический колпак для защиты от всепроникающего влияния радиоволн, шифровать все ваши телефонные разговоры и закупать на интернет-аукционе eBay оборудование, соответствующее стандартам TEMPEST. В большинстве случаев, если, конечно, вы не являетесь жертвой шпионажа со стороны крупных разведывательных управлений и других организаций со

значительным бюджетом, вам не стоит беспокоиться о перечисленных в данной главе приемах высшего компьютерного шпионажа.

Разумеется, хорошо финансируемые организации (размер бюджета Управления национальной безопасности засекречен, однако по приблизительным оценкам он составляет более 13 000 000 000 долларов в год) имеют в своем распоряжении ресурсы, которые позволяют им на 5...20 лет опережать общедоступные технологии безопасности, и устройства, о существовании которых мы даже не знаем. Но использование всего этого дорогостоящего оборудования для постоянного шпионажа за гражданами США экономически не обосновано. (Возьмем, к примеру, ECHELON. Ведь, в конце концов, перехваченные данные требуют ручного анализа со стороны специалиста для головоломного восстановления происходящих событий.)

Кроме того, учтите, что даже компании со значительным бюджетом, имеющие права на использование наблюдательного и разведывательного аппаратного и программного обеспечения, не так всемогущи, как это иногда изображают в средствах массовой информации и шоу-бизнесе. Вспомним хотя бы неспособность правительства предугадать террористическую атаку 11 сентября, тот факт, что правоохранительным органам так и не удалось найти злоумышленников, рассылавших в конвертах споры сибирской язвы, и весьма скромные успехи США в войне с международным терроризмом, несмотря на огромное количество затраченных денежных и людских ресурсов.

Размышляя о том, возможно ли совершение против вас серьезных операций компьютерного шпионажа, применяйте оправданные средства безопасности (помните о различии между возможной и вероятной угрозой), но при этом никогда не недооценивайте вашего противника.

## Приложение

# Наша веб-страница

Официальная веб-страница, на которой размещены ссылки на различные информационные ресурсы и утилиты, которые обсуждаются в этой книге, находится по адресу [www.wiley.com/combooks/mcnamara](http://www.wiley.com/combooks/mcnamara). В этом приложении мы вкратце расскажем вам о содержимом веб-сайта. В частности, в приложении будут освещены следующие вопросы:

- системные требования,
- ссылки на веб-сайты,
- разрешение вопросов.

## Системные требования

Поскольку данная книга в первую очередь посвящена компьютерному шпионажу на системах под управлением Microsoft Windows, большинство из приводимых ссылок указывает на программы, предназначенные для работы (именно так!) под ОС Windows. (Вы также встретите пару ссылок на хорошие утилиты под Linux для инакомыслящих и просто любознательных, которым до этого еще не приходилось работать с другими операционными системами.)

Поскольку за последние годы компания Microsoft выпустила несколько различных версий операционной системы Windows, некоторые из перечисленных на страницах книги и на нашем веб-сайте утилит предназначены для работы исключительно под определенной версией операционной системы: Windows 3.x, 9.x/Me, NT или же 2000/XP. Версия Windows, под которой должна работать та или иная программа, четко оговаривается в соответствующем ссылке месте книги. Советуем вам вначале прочесть теоретические сведения о заинтересовавшей вас утилите, чтобы потом, к примеру, не пришлось тратить время на поиск и загрузку утилиты для взлома паролей в .PWL-файле, тогда как, оказывается, вам необходимо взломать SAM-файл на компьютере под управлением Windows XP.

Говоря об аппаратных требованиях, необходимых для вашей работы, следует заметить, что они зависят исключительно от типа используемой вами операционной системы.

Минимальные требования (при удовлетворении которых, правда, система будет работать чрезвычайно медленно) следующие:

- компьютер Intel Pentium 120 МГц или более мощный;
- 32 Мб оперативной памяти;
- модем со скоростью 28,8 Кбит/с либо широкополосное подключение;
- доступ к Интернету.

Общее правило: чем больше у вас оперативной памяти и чем быстрее процессор (до определенного предела), тем легче вам будет работать.

## Ссылки на нашем веб-сайте

Наш веб-сайт разбит на разделы, соответствующие главам книги. Под каждым заголовком вы увидите все приводимые в данной главе ссылки с краткими описаниями ресурса.

Поскольку в данной книге и так размещено огромное количество ссылок, вместо того чтобы добавлять еще нескольких десятков страниц с дополнительными ссылками, мы советуем вам действовать следующим образом: прочесть главу, затем посетить наш официальный веб-сайт, либо набрать приведенную в тексте гиперссылку непосредственно в адресной строке браузера и просмотреть интересующие вас ресурсы. Структура веб-сайта и краткие описания призваны ускорить процесс поиска нужной вам информации.

Учтите, что веб-сайты появляются и исчезают, как шпионы в夜里, поэтому, если вы натолкнетесь на неработающую ссылку, сформируйте строку запроса и задайте ее на вашем любимом поисковом сервере. Кроме того, в сети Интернет найдется масса мест, где продублирована интересующая вас информация, в том числе «зеркала» сайтов и т. п., мы же со своей стороны постарались привести на нашем сайте достаточно информации для того, чтобы вы смогли грамотно составить запрос по нужной теме.

## Разрешение вопросов

Я сомневаюсь, что у вас могут возникнуть какие-либо проблемы с нашим веб-сайтом, поскольку он написан с использованием стандартного языка HTML и не требует для своей работы Flash или других подключаемых модулей. Internet Explorer, Opera или Mozilla – во всех этих браузерах наша веб-страничка выглядит вполне пристойно.

Тем не менее, если у вас, не дай бог, возникнут проблемы с нашим сайтом, пожалуйста, позвоните в отдел по работе с клиентами издательства Wiley по телефону 1-800-762-2974 (в США) или 317-572-3994 (за пределами США). Вы также можете обратиться в службу поддержки издательства Wiley по электронной почте: [techsupdum@wiley.com](mailto:techsupdum@wiley.com). Учтите, что компания Wiley Publishing предоставляет техническую поддержку только по общим вопросам; за технической поддержкой программных продуктов вам необходимо обращаться к разработчикам либо дистрибуторам данного продукта. (Если по какой-либо причине на сайте не работают те или иные ссылки – перечитайте еще раз раздел «Ссылки на нашем веб-сайте» данного приложения, перед тем как звонить нам.)

# Предметный указатель

## A

Abi-Coder утилита  
шифрования файлов, 200  
AccessData  
набор инструментов  
для взлома паролей, 233  
набор инструментов  
для судебной  
экспертизы, 188–189  
распределенные сетевые  
атаки, 233  
ACT (Ассоциация  
конкурирующих  
технологий), 35  
ADS (альтернативный поток  
данных), 172–174  
Advanced NT Security  
Explorer, 143, 145  
AIBO собачка-робот, 399  
AirDefense утилита, 425  
Air-Jack утилита, 411  
AirMagnet утилита, 423  
AiroPeek NX сетевой  
монитор, 419  
Alert Standard Format (ASF)  
технология, 126  
Alibris компания  
по онлайновой продаже  
книг, 82–83  
Altivore утилита, 355  
AMA (American Management  
Association), 28  
Amazon, 82–83  
Amecisco  
Invisible KeyLogger Stealth  
(IKS), 287  
аппаратный  
KeyLogger, 289–290

## American Management

Association (AMA), 28

American Megatrends, Inc.  
(AMI), 124

Apple iPod, 265

ARP (протокол  
разрешения адресов)  
фальсификация, 354  
ASF (Alert Standard Format)  
технология, 126

## B

Back Orifice троянский конь, 326

Badtrans.B червь, 496

Baseline Security Advisor  
утилита, 150

BestCrypt утилита, 200–201

BIOS (базовая система  
ввода/вывода)

CMOS, 126–129

версии, 124–125, 140

взломщики паролей, 142–143

жесткий диск, 126

настройки

безопасности, 149–150

ноутбуки, 129–130

опция обнаружения вскрытия

компьютера, 127

пароли, 122–130, 150

последовательность

загрузки, 123

производитель, 122

ссылки, 122

уязвимые места, 122–130

BlackBerry, 451–452, 454

BlackIce PC Protection, 369

Blowfish Advanced CS утилита  
шифрования, 199

BND (Bundesnachrichtendienst), 40

BO (Back Orifice) троянский конь, 326  
 BOClean утилита, 335  
 BugTraq список адресов электронной почты, 136  
 Bundesnachrichtendienst (BND), 40  
 Business Engine (компания по производству ПО), 27  
 BWMACHAK утилита, 394

**C**

Cain & Abel утилита, 367  
 CALEA (Закон о сотрудничестве компаний, предоставляющих услуги связи, с правоохранительными органами), 64  
 Cali картель, 42  
 Caligula вирус, 494  
 Carnivore/DCS-1000 программа, 354, 482–485  
 cDc (Cult of the Dead Cow) группа хакеров, 327  
 CD-R/CD-RW, 258–260  
 CERT (группа компьютерной «скорой помощи»), 136  
 CF (Compact Flash), 262–263  
 Chevron, 30  
 Chntpw (Change NT password) утилита, 148  
 CIA Commander утилита, 145–146  
 ClearLogs утилита, 147  
 Cmospwd utility, 127, 140  
 CodeBreakers группа хакеров, 494–495  
 CompactFlash (CF), 262–263  
 Compaq iPAQ, 402–403  
 CompuSafe прибор, 307  
 Content Scrambling System (CSS), 215–216  
 Convera RetrievalWare, 355  
 CoolMiner, 482

Corporate Systems Portable Pro привод, 267  
 Creative Labs Cardcam digital camera, 271  
 Nomad Jukebox Zen, 265  
 Cryptcat программа, 270–271  
 cryptome.org веб-сайт, 43  
 CSDiamond RegistryProt, 334  
 CSS (Content Scrambling System), 215–216  
 Cult of the Dead Cow (cDc) хакерская группа, 327  
 CyberScrub программа, 210  
 Cypherpunk Type I, программа анонимной пересылки корреспонденции, 383

**D**

data dumper (dd) утилита, 188  
 Data Encryption Standard (DES), 194, 226  
 Data Interception by Remote Transmission (D.I.R.T.), утилита, 487  
 DCFL (компьютерная судебная лаборатория Министерства обороны), 186  
 DCS-1000/Carnivore программа, 354, 482–485  
 DeCSS утилита, 216  
 Déjà Vu система аутентификации, 250  
 Deloitte & Touche (аудиторская фирма), 34  
 DES (Data Encryption Standard), 194, 226  
 DESCHALL проект, 227  
 Dialpwd утилита, 239  
 DIBS USA, 164  
 Digi-watcher (ПО для работы с веб-камерами), 502  
 D.I.R.T. (Data Interception by Remote Transmission), 487

DISA (Агентство по оборонным информационным системам), 398  
Dow Chemical компания, 30  
DragNet утилита, 355  
DragonWare Suite программный пакет, 482  
DriveCrypt утилита, 202  
DriveSavers восстановление данных, 185  
Dshield утилита, 374  
Dsniff утилита, 366  
DTMF-декодер (двутональный многочастотный набор), 442  
DVD-диски, 261–262

**E**

EasyRecovery Professional утилита, 193  
eBlaster программа мониторинга клавиатуры, 46  
ECHELON система сбора информации, 24, 473–478, 480–481  
ECPA (Закон о защите электронных систем связи) 64–67, 74  
EES (Evil Eye Software), 328  
EFS (шифрованная файловая система), 146, 154, 201  
ElcomSoft, 233–234  
EnCase утилита, 188–189  
ERD Commander, 145  
Ethereal утилита, 365–366  
Ettercap утилита, 366–367  
Evil Eye Software (EES), 329

**F**

Fake AP утилита, 425  
FakeGINA, 144

File Monitor утилита, 297–298  
FIREWAR утилита, 371  
FlashGo! Card устройство для чтения и записи флэш-карт, 263  
Forensic Toolkit (FTK), 189

**G**

General Motors, 26  
GFI LANguard System Integrity Monitor утилита, 334  
Ghost программа, 187  
GINA (графическая система идентификации и авторизации), 145  
Glide утилита, 236–237  
GnuPG (Gnu Privacy Guard), 198  
God программа мониторинга клавиатуры, 300  
GPS устройства, 409–410, 458–459

**H**

Hardware KeyLogger, 290  
Hawaiian Airlines, 69  
HIJACK, 473  
Hotmail почтовый сервер, 381  
HTML-приложения (HTA), 382  
Hunter утилита, 335  
HushMail, 381

**I**

IACIS (международная ассоциация специалистов по расследованию компьютерных преступлений), 159  
IDS (системы обнаружения вторжений), 367–370, 424–425  
IEEE 1394, стандарт, 260–261

IETF (проблемная группа проектирования Интернет), 117  
 IGI (международный отдел расследований), 35  
 IIP утилита, 379  
 IKS (Invisible KeyLogger Stealth), 287  
 ILook утилита, 190  
 Imation FlashGo!, устройство для чтения и записи флэш-карт, 263  
 InetShepard наблюдательное ПО для работы с веб-камерами, 502  
 Intelligent Computer Solutions Image Masster Solo-2, 267  
 Interface Security компания, 288  
 Interloc, Inc. компания, 83  
 Internet Assigned Numbers Authority (центральный координатор по присвоению уникальных параметров протоколов Интернет), 350  
 Internet Explorer, 337, 360  
 Investigator средство мониторинга клавиатуры, 288  
 Invisible KeyLogger Stealth (IKS), 287  
 Inzider утилита, 375  
 iOpus Password Recovery XP, утилита, 238  
 «IP everywhere», 497  
 iPAQ (Compaq), 402–403  
 iPod (Apple), 265

**J**  
 Jasc Quick View Plus, 192  
 John the Ripper утилита, 148

**K**

KeyDisk утилита, 129  
 KeyGhost утилита, 289  
 KeyKatcher утилита, 288, 290  
 keylogger  
     eBlaster, 46  
     God, 300  
     Hardware KeyLogger, 289–290  
     Investigator, 288  
     Invisible KeyLogger Stealth (IKS), 287  
     KeyGhost, 288–290  
     KeyKatcher, 290  
     keylogger на заказ, 291  
     Linux, 306  
     Magic Lantern проект, 292  
     Spector Professional Edition, 286–287  
     WinWhatWhere Investigator программа, 288–289  
     аппаратные keylogger, 282–286, 288–290  
     библиотеки периода выполнения на VB, 298–299  
     веб-камеры, 279  
     возможности, 278–279  
     встроенные в клавиатуру, 303–304  
     кампании по дезинформации, 294  
     контрмеры, 291–298  
     мониторинг операций записи в файлы, 296–298  
     нарушения Закона о прослушивании линий связи, 86  
     обзор, 286–291  
     обнаружение, 277, 293–299, 303–308  
     определение, 273  
     пароли, 304, 306  
     персональные брандмауэры, 299  
     поиск строки, 299

- программные keylogger,  
275–279, 281, 287–288
- программы мониторинга  
реестра, 299–300
- программы перехвата  
сетевых пакетов, 303
- программы проверки  
целостности файлов,  
299–300
- система мониторинга  
клавиатуры (KLS),  
281
- скрытие, 277
- сообщения об ошибках, 306
- стоимость, 286–288,  
290–291
- удаление, 306–307
- Kismet утилита, 417–418
- Kiwi Syslog Daemon  
программа, 372
- KLS (система мониторинга  
клавиатуры), 281
- Kroll, Inc. компания, 185
- L**
- L.A.S. Systems компания, 459
- LANfiltrator троянский  
конь, 327–328
- LC утилита, 141–143
- Legion утилита, 364–365
- Logicube SF-5000 устройство  
дублирования информации  
на жестких дисках, 266
- Logon.scr файл, 148
- LOphtCrack утилита, 141–143
- Lotus Notes программа, 490
- M**
- MAC-адреса,  
фальсификация, 394–395
- Magic Lantern  
проект, 292, 485–488
- MapPoint программа, 421–422
- Marker вирус, 494–495
- MemoryStick, 263
- Microdrives, 269
- Microsoft  
Baseline Security Advisor, 150
- Hotfix Checker утилита, 150
- Hotmail бесплатная почтовая  
служба, 381
- MapPoint программа, 421–422
- информационные бюллетени  
по безопасности, 136, 149
- обвинения в наличии  
«запасных лазеек» для  
входа в систему, 491
- схемы шифрования, 236
- уязвимые места ПО, 337
- Minox сверхминиатюрная  
цифровая камера, 271
- Mischel Internet Security, 335
- Mixmaster Type II программа  
анонимной пересылки  
корреспонденции, 383
- MP3-плееры, 265, 458
- MSinfo32 утилита, 296
- MyNetWatchman утилита, 374
- N**
- NAT (NetBIOS Auditing Tool), 364
- Nessus утилита, 364
- NetBIOS Auditing Tool (NAT), 364
- NetBIOS утилиты атаки, 364
- NetBIOS, 351–353, 380
- NetBus троянский конь, 321, 326
- NetCat утилита, 270–271
- Net-Devil троянский конь, 328
- NetIntercept утилита, 355
- netstat команда, 375
- NetStumbler утилита, 400,  
415–418
- Network Associates компания,  
292, 355, 419
- New Technologies Inc. компания  
(NTI), 159
- Niku Corporation (компания по  
производству ПО), 27

NIPC (Правительственный Центр защиты национальной инфраструктуры), 136

NISPOM (Национальная программа промышленной безопасности. Справочное руководство), 117

Nmap утилита, 362–363

Nomad Jukebox Zen, 264

NONSTOP стандарт, 473

Nortek Computers, Ltd., 131

Norton Ghost, 187

Norton Utilities, 193

NSSpyglass утилита, 424–425

NTBugTraq список рассылки, 135

NTFSDOS утилита, 147

NTI (New Technologies Inc.), 159

NWCC (Национальный центр административных преступлений), 159

## O

Optix троянский конь, 328

Oracle, 35

ORiNOCO Gold сетевая карта, 405–406

## P

Packeteer, 482

Packetstorm Security веб-сайт, 235

Passware Kit, 234–235

Password Crackers, Inc., 131

Password Recovery набор утилит, 233

PasswordSpy, 238

PC Magazine журнал, 287

pcAnywhere технология, 330

PDA Defense утилита, 456

PestPatrol программа для обнаружения keylogger, 302

PGPfone утилита, 442

PGP (Pretty Good Privacy) утилита, 66, 197, 377

Phoenix Technologies пароли к BIOS, 125

PhoneBook Viewer v1.01 с, 239

PI (Private Idaho) утилита, 383

Pockey DataStor, 268

Pretty Good Privacy (PGP) утилита, 66, 197, 377

Private Idaho (PI) утилита, 383

Process Explorer утилита, 295–296

Ptech, Inc. компания, 317

Pwdump утилита, 144–145

PWL утилиты для взлома, 237

PWLHack утилита, 237

PWLTool утилита, 237

PWLView утилита, 237

## Q

Quick View Plus утилита, 192

## R

RAHAB проект, 40

Ramsey Electronics, 439

Ratware программа обхода защиты хранителя экрана в Win9x, 141

Raytheon SilentRunner, 354

RCFL (региональная компьютерная судебная лаборатория), 157

RegEdit утилита, 177–178

RegistryProt утилита, 334

RetrievalWare утилита, 355

Revelation утилита, 237–238

RIM BlackBerry пейджер, 451, 454

## S

Safe Technology Co. Ltd., 307

SafeBack программа для дублирования информации, 187

SAM (администратор учетных данных в системе защиты), 136–139  
SamSpade утилита, 362–363  
Sandstorm Enterprises  
    NetIntercept, 355  
SCP (Secure Copy), 379  
Srsavpw утилита, 141  
Secure Copy (SCP), 379  
Secure Digital карты памяти, 263  
Secure Shell (SSH), 380  
Securepoint Intrusion Detection программа, 369  
Sentry 2020 утилита, 456  
SER (Stealth Email Redirected), 359  
SilentRunner утилита, 354  
SiPix StyleCam Snap цифровая камера, 271  
SirCam червь, 495–496  
SmartMedia карты памяти, 263  
Sniffer Wireless утилита, 419  
Snitch утилита, 237–238  
Snort программа обнаружения вторжений, 369  
Sony AIBO собачка-робот, 399  
SpamMimic веб-сайт, 203  
Speak Freely утилита, 441  
Spector Professional Edition  
    программа мониторинга клавиатуры, 287  
Spybot Search & Destroy  
    программа для обнаружения keylogger, 302–303  
SpyCop программа для обнаружения keylogger, 278, 301  
SpyShield утилита, 379  
SSH (Secure Shell), 379  
Starium, Inc. (торговец безопасными телефонами), 441  
Stealth Email Redirector (SER), 359

Steganos  
    Security Suite, 200  
Stegdetect утилита, 205  
S-Tools утилиты, 205  
STU-III<sup>s</sup> (безопасные телефоны), 439–441  
StumbVerter утилита, 422  
Stunnel утилита, 375  
Sub7 троянский конь, 327  
SuperCircuits миниатюрная видеокамера, 502–503  
SuperScan утилита, 363  
SurfSecret Privacy Protector, 210  
Symantec  
    Norton Utilities, 193  
    pcAnywhere, 330–331  
Synergy International Systems, 316–317  
Sysinternals  
    FileMon, 297–299  
    Process Explorer, 295–296  
    TCPView, 375  
    TDImon, 375

**Т**  
Tauscan утилита, 335–336  
TCP/IP характерные особенности заголовков, 351  
TCPView утилита, 375  
TDImon utility, 375  
TDS (Trojan Defense Suite), 335  
TealLock утилита, 456  
TEMPEST, 463–465, 467–472  
TEMPEST оптические стандарты, 472–473  
The Wall Street Journal 146  
TightVNC, 331  
TiVo цифровой видеомагнитофон, 460  
Treason 101 веб-сайт, 105  
Trillian утилита, 378  
TriWest Healthcare Alliance Corp., 256  
Trojan Defense Suite (TDS), 335

**U**

USA Today газета, 204  
 USB (универсальная последовательная шина), 260–261  
 USB Flash Drive, 263

**V**

Voice over Internet Protocol (VoIP), 441  
 Volkswagen, 26  
 VoIP протокол, 441  
 VPN Labs веб-сайт, 375  
 VPN (виртуальные частные сети), 373–375, 428

**W**

Wakefield Integrated Technologies, 437  
 WallWatcher утилита, 372  
 Wang Research Laboratories, 467  
 war chalking, 403  
 war driving (поиск беспроводных сетей), 398–400, 412–416  
 wbStego4 утилита, 206  
 Whack-A-Mole игра, 321  
 Who's Watching Me программа для обнаружения keylogger, 302  
 Window Washer утилита, 210  
 WinHex утилита, 191–192  
 WinPcap утилита, 366  
 WinWhatWhere Investigator программа мониторинга клавиатуры, 288–289  
 WinZapper утилита, 147  
 WS\_FTP утилита, 237

**X**

X-10 беспроводная камера, 399  
 Xerox камера в копировальной машине, 434  
 наблюдение за сотрудниками, 30

**Y**

YahooMail почтовая служба, 381

**Z**

ZIP-диски, 262

**A**

автоматическое определение координат транспортного средства (AVL), 458  
 автоответчики, 449–450  
 Агентство по оборонным информационным системам (DISA), 398  
 администратор учетных данных в системе защиты (SAM), 136–139  
 Аль-Каида, 39, 81, 146, 204, 317  
 альтернативный поток данных (ADS), 172–174  
 Американская ассоциация библиотек, 75  
 Американское общество промышленной безопасности, 25, 39  
 анализ трафика, 344  
 анализаторы протоколов см. программы перехвата сетевых пакетов  
 Антивирус Касперского (KAV), 334  
 антивирусное ПО, 334  
 аппаратные брандмауэры, 371

- аппаратные средства  
мониторинга клавиатуры,  
282–286, 288–291
- Апелляционный суд по делам  
иностранный разведки, 62
- Арингтон, Уинстон, *Как  
услышать это*, 439
- архиваторы, 254
- Ассоциация конкурирующих  
технологий (ACT), 35
- атака «в лоб» при подборе  
паролей, 225–229
- атака при помощи  
словаря, 224–225
- Атаки хакеров раскрыты*,  
Джон Чирилло, 348
- атаки эскалации  
привилегий, 140–142
- Б**
- базовая система  
ввода/вывода, см. BIOS
- баннеры, 350
- безопасность  
базовых станций (точек  
доступа) 428–429
- беспроводных сетей,  
397, 423–429
- веб-браузеров, 372
- безопасные протоколы, 379
- безопасные телефоны,  
439–441
- Бернхэм, Дэвид  
*Над законом*, 96
- беспроводные сети  
GPS-устройства, 409
- ORiNOCO Gold сетевая  
карта, 405
- SSID (идентификаторы),  
390–392, 427
- war driving,  
397–401, 412–416
- WEP (эквивалент  
безопасности проводных  
сетей), 391–393, 427
- антенны, 405–409, 423
- атаки «отказа  
в обслуживании», 396
- базовая станция (точка  
доступа), 390, 410–411
- безопасность, 397, 422–429
- виртуальные частные сети  
(VPN), 428–429
- история, 388
- карманные ПК, 402
- наблюдение, 400–403, 411–416
- настройки  
по умолчанию, 396–397
- ноутбуки, 402
- операционная система  
Windows XP, 422
- поиск беспроводных  
сетей, 398–401, 410–417
- популярность беспроводных  
сетей, 387
- радиоволны, 395–396
- сетевые карты, 401, 403, 405
- символы для обозначения  
статуса сети, 404
- системы обнаружения  
вторжений (IDS), 424–425
- список MAC-адресов,  
392–394, 427
- удаленный доступ, 397
- уязвимые места, 389–397
- фальшивые сети-  
приманки, 424
- Биометрический консорциум, 249
- биометрия, 245–250
- брандмауэры  
аппаратные, 371
- безопасность, 372
- обработка данных  
журналов, 372
- персональные, 299–300,  
333, 371–373
- программные, 372–373

проверка состояний пакетов, 370 производители, 373 тестирование, 371 уязвимые места, 377 файлы журнала, 372 фильтрация на уровне пакетов, 370 приложений, 370 шлюз, 372 браузеры CyberScrub, 210 Window Washer, 210 автозаполнение, 179 вредительские веб-сайты, 360 Журнал, 179 избранное, 178 кэш, 178 прокси- и веб-серверы, 383–385 файлы cookies, 180 файлы index.dat, 180 Браун, Стивен Пауэл (шпион), 46 быстрый набор номера (телефоны), 443

**В**

ван Эк, Вим (инженер), 466 веб-браузеры CyberScrub, 210 Index.dat файлы, 180 Window Washer утилита, 210 вредительские веб-сайты, 359–360 Журнал, 179 избранное, 178 кэш, 178 прокси-серверы в веб, 383–385 файлы cookies, 180 функция автозаполнения, 179

веб-камеры keylogger, 279 наблюдение, 501–502 троянские приложения, 312 веб-сайты Crucial Security, 174 cryptome.org, 43 Nortek Computers, Ltd., 131 Packetstorm Security, 235 Password Crackers, Inc., 131 SpamMimic, 203 «Treason 101», 105 TrojanForge, 329 VPN Labs, 375 Национального института безопасности, 72 Национального собрания законодательных органов штатов, 72 наша веб-страница, 505–506 Общества профессионалов конкурентной разведки, 26 *Взгляд изнутри: дневник ЦРУ, Филипп Эйджи*, 273 ЦРУ – секреты одного из наиболее могущественных разведывательных управлений в мире, Рональд Кесслер, 38 взлом и проникновение, 106–108 взлом криптосистем, 239–240 взломщики, 40–41 видеокамеры, 499–503 Видстром, Арни (программист), 144 виртуальные частные сети (VPN), 373–375, 428 вирусы Caligula, 494 Marker, 494–495 контрмеры, 499 определение, 493 вирусы разведывательные, 492–497

восстановление  
данных с жесткого  
диска, 185  
пароля, 126  
удаленных файлов, 170–171  
враждебные  
веб-сайты, 359–360  
вредительские  
приложения, 359  
время создания  
модификации,  
обращения, 167  
вычисления в виртуальных  
сетях (VNC), 331

## Г

Ганхас, Кристина (участница  
политической  
кампании), 357–358  
голосовые сканеры, 249  
гражданский суд, 81–83  
графическая идентификация и  
авторизация (GINA),  
145–146  
группа компьютерной «скорой  
помощи» (CERT), 136  
Грэмс, Роб (политик), 357–358

## Д

данных копирование  
CD-R/CD-RW-  
диски, 258  
DVD, 261–262  
Microdrives, 269  
архиваторы, 254  
дискеты, 257  
диски ZIP, 262  
доступные ресурсы, 254  
жесткие диски, 264–269  
жесткие диски USB, 268  
системы архивирования на  
магнитной ленте, 269  
передача информации по  
сети, 270–271  
пропускная способность,  
255, 258, 260

советы, 253–255  
цифровые камеры, 271  
энергонезависимая память,  
262–264  
деньги, идеология, шантаж и  
честолюбие (принцип  
MICE), 104  
Детч, Джон (бывший глава  
ЦРУ), 345  
диски, 184–186, 207, 258–262  
дисковый редактор, 190–192  
Диспетчер задач, 295  
доносчики, 41–44  
дублирование информации,  
163–164, 265–267

## Ж

жесткие диски  
дублирование информации,  
163–164, 187–188,  
265–267  
жесткие диски USB, 267–268  
неиспользуемое дисковое  
пространство, 174–175  
пароли, 129  
программы  
безвозвратного удаления  
файлов, 206–209  
«жучки»  
для клавиатуры, 304  
для телефонов, 439  
журналы сервера, 355–356

## З

загранкомандировки, советы  
по защите информации,  
115–116  
Закон о защите электронных  
систем связи (ECPA),  
64–67, 82  
Закон о компьютерном  
мошенничестве и  
злоупотреблениях,  
67–68, 74, 76

- Закон о прослушивании линий связи, 58–61, 74, 86
- Закон о сотрудничестве компаний, предоставляющих услуги связи, с правоохранительными органами (CALEA), 63
- Закон о хранимой информации, 65–67, 73–74
- Закон об иностранной разведке (FISA), 61–62, 74–78
- Закон об экономическом шпионаже (EEA), 71
- законы  
воплощение законов в жизнь, 79–81
- О защите электронных систем связи, 64–67, 83
- О компьютерном мошенничестве и злоупотреблениях, 67–68, 76–78
- О прослушивании линий связи, 58–61, 74–86
- О сотрудничестве компаний, предоставляющих услуги связи, с правоохранительными органами, 64
- О хранимой информации, 65, 67, 74
- Об иностранной разведке, 61–63, 74–78
- Об экономическом шпионаже, 71
- законы штатов, 71–72, 78–79
- Национальный закон о трудовых взаимоотношениях, 84
- ограничения, 87
- Патриотический Акт США, 31, 72–76, 78–79, 97
- законы штатов, 71–72, 78–79
- Замки, сейфы и безопасность, Марк Тобиас, 107
- запасные пароли к BIOS, 123–125
- засекреченные стандарты HIJACK, 473
- NONSTOP, 473
- TEMPEST, 463–465, 467–469, 471–473
- И**
- игровые приставки, 458
- идентификатор абонента, 442
- Изучение места электронного преступления: руководство для прибывших первыми*, Министерство юстиции, 158
- инженерный анализ исходного кода, 230, 489
- К**
- камеры наблюдения, 499–502
- карманные ПК, 455–457
- коммерческие услуги по восстановлению информации, 185
- коммутируемая сеть, 239
- компьютерная судебная лаборатория Министерства обороны (DCFL), 186
- компьютерная экспертиза, 32
- компьютерные полицейские дублирование информации, 163–164
- задачи, 155, 158
- изъятие компьютеров и периферии, 160–163
- навыки, 156
- обучение, 158
- определение, 155
- полицейские расследования, 30–33

- сертификация, 159  
спрос на компьютерных  
полицейских, 160  
судебная экспертиза,  
164–166  
характеристики  
доказательств, 191  
цепочка владельцев, 162  
компьютерные судебные  
эксперты  
задачи, 155–156  
навыки, 156  
определение, 155  
проблемы, 158–160  
спрос, 158  
конкурентная разведка, 27  
Коноп, Роберт (пилот Hawaii  
Airlines), 69  
консультанты, 33, 36  
контрмеры  
DCS-1000/Carnivore  
программа, 483–485  
ECHELON система сбора  
информации, 475,  
477–479  
вирусы, 497  
мониторинг побочного  
излучения, 470  
наблюдение, 367–370  
определение, 49  
сетевые атаки, 367–385  
слабые места в защите с  
помощью паролей, 153  
средства мониторинга  
клавиатуры (keylogger),  
293–299  
тайные проникновения,  
110–118  
троянские кони, 331–337  
уязвимые места BIOS,  
149–150  
уязвимые места защиты  
Windows, 149–154  
черви, 495–497
- копирование данных  
CD-R/CD-RW-диски, 258  
DVD, 261–262  
Microdrive, 269  
архиваторы, 254  
дискеты, 257–258  
дискеты ZIP, 262  
доступные ресурсы, 254  
жесткие диски USB, 267–268  
жесткие диски, 264–269  
передача информации  
по сети, 270–271  
пропускная способность,  
255, 258, 260  
системы архивирования  
на магнитной ленте, 269  
советы, 253–255  
цифровые камеры, 271  
энергонезависимая память,  
262–264
- Копп, Джеймс (активист  
движения против  
абортов), 183–184  
Корзина, 170–171, 173  
корпоративные шпионы, 25–28  
КПК, 455–457  
кражи ноутбуков, 130  
криминальные шпионы, 40–41  
криptoанализ, 228–229  
криптография  
история, 194–196  
определение, 194  
ресурсы, 194
- Купер, полковник Джефф  
(разработчик системы  
цветовых кодов), 48
- Кесслер, Рональд, ЦРУ –  
секреты одного из  
наиболее могущественных  
управлений в мире, 38
- Л**
- Лопес, Хосе Игнасио  
(экономический шпион), 26

**M**

Мэйрес, Дэн (компьютерный судебный эксперт), 187  
 машины для уничтожения бумаг, 434–437  
 Международная ассоциация специалистов по расследованию компьютерных преступлений (IACIS), 159  
 Международный отдел расследований (IGI), 35  
 микроприводы, 269  
 минимизация, 62, 77  
 Министерство юстиции  
   *Расследование электронных преступлений: руководство для начинающих*, 158  
 модифицированные исполняемые файлы, 488–489, 492  
 мониторинг побочного излучения, 465–470  
 Монтес, Анна Белен (сотрудница оборонной разведывательной службы), 208  
 мультимедийные карты памяти (MMC), 263  
 Мюллер, Роберт (глава ФБР), 80

**N**

наблюдательные программы  
   Ethereal, 365–366  
   Kismet, 417–418  
   Legion, 363  
   Nessus, 364

NetBIOS Auditing Tool (NAT), 364–365  
 NetStumbler, 415–417  
 Nmap, 362–363  
 SamSpade, 361–362  
 SuperScan, 363  
 наблюдение  
   ECHELON система сбора информации, 24, 473–478, 481  
 GPS-устройства, 458  
 MP3-плееры, 458  
 NetBIOS, 351–353, 380  
 TiVo, 460  
 автоответчики, 449–450  
 анализ трафика, 344  
 беспроводные сети, 400–405, 411–417  
 беспроводные телефоны, 444  
 враждебные веб-сайты, 360  
 враждебные приложения, 359–360  
 игровые приставки, 458  
 исходные точки, 341–342  
 компьютеры,  
   предназначенные для общественного пользования, 360, 380  
 контрмеры, 367–385  
 КПК, 455–457  
 локализация цели, 348–349  
 мобильные телефоны, 443–449  
 общий доступ к файлам в Windows, 351–353, 380–382  
 определение версии операционной системы, 350–351  
 отраженный свет (от компьютерных мониторов), 472

- пароли по умолчанию, 358
- партнерство правительства США с технологичными компаниями, 490
- пейджеры, 451–454
- печатные машинки, 273–274
- программы перехвата сетевых пакетов, 353–355
- светодиодные индикаторы статуса, 472
- серверные журналы, 355–356
- системы голосовой почты, 449–451
- сканирование портов, 349
- сканирование при помощи команды ping, 348
- сканирование уязвимых мест, 351
- сотовые телефоны, 443–449
- средства мониторинга клавиатуры, 273
- телефоны, 438–442
- файлы журнала, 355–356
- факсы, 431–433
- широкополосные подключения, риски, 344–347
- электромагнитный шпионаж, 463–470
- наблюдение «из-за плеча», 361
- наблюдение за сетевыми подключениями, 376
- наблюдение за сотрудниками
- Закон о защите информационных систем связи, 83
- использование согласия, 85
- Национальный закон о трудовых взаимоотношениях, 84
- неявное согласие, 84
- подписи в сообщениях, 85
- союзы рабочих, 84
- статистика, 28
- типичные программы мониторинга, 29
- набор инструментов для проведения судебных экспертиз (FTK), 189
- Над законом, Девид Бернхэм, 96
- надежные пароли, 154, 241
- настройки безопасности BIOS, 149–150
- операционной системы Windows, 149–154
- Национальная служба контрразведки, 115
- Национальное собрание законодательных органов штата, 72
- Национальная программа промышленной безопасности. Справочное руководство (NISPOM), 117
- Национальный закон о трудовых взаимоотношениях, 84
- Национальный институт безопасности, 72
- Национальный консорциум юридической информации и статистики, 287
- Национальный центр административных преступлений (NWCC), 159
- Национальный центр образовательной статистики, 117
- «невидимки», 36–40
- Независимый институт, 35
- неиспользуемое дисковое пространство, 174–175

нестойкое шифрование, 215–216  
ненадежные пароли, 216–221  
Николсон, Гарольд (агент ЦРУ), 91  
Нотон, Патрик (сексуальный агрессор), 485–486  
ноутбуки  
  кража, 130  
  пароли к BIOS, 129–130  
  поиск сетей, 398–400  
뉴-йоркский проект по наблюдению, 501

**О**

обеспечение физической безопасности, 111–114  
обнаружение  
  средств мониторинга  
    клавиатуры, 277, 293, 295–306, 308  
  тロянских приложений, 331–335  
оборудование  
  OnlyMe утилита, 457  
  Ontrack Data International, 185  
  OnTrack EasyRecovery Professional, 191  
  машины для уничтожения бумаг, 434–438  
Сводный закон о контроле преступности и уличной безопасности, 58–61  
факсы, 431–433  
  шифрование «на лету», 200  
общественного пользования компьютеры, 360, 379–380  
Общество профессионалов конкурентной разведки, веб-сайт, 26  
общий доступ к файлам в Windows, 351–352, 380–381

операционная система  
  версии, 124–125, 140  
  модификация компонентов операционной системы, 488–489, 492  
пароли, 121, 123–125, 128–129, 131–134, 137–139  
операционная система Windows Logon.scr файл, 148  
автоматическое обновление, 150  
администратор учетных данных в системе защиты (SAM), 136–140  
атака эскалации  
  привилегии, 140–142  
беспроводные сети, 387–430  
графическая идентификация и авторизация (GINA), 145  
Корзина, 173  
настройки  
  безопасности, 149–153  
остатки кластеров, 174  
пароли, 121, 123–125, 128–129, 131–134, 137–139, 153  
реестр, 176–177  
страничный файл, 175  
уязвимые места, 120, 132–142  
файл подкачки, 175  
шифрованная файловая система (EFS), 139, 146, 154, 201  
операция CHAOS, 38  
Организация по расследованию высокотехнологичных преступлений (HTCIA), 159  
Организация электронных границ, 73  
организованная преступность, 41  
остатки кластеров, 174  
отгадывание паролей, 125, 133–134, 222

отраженный свет  
(от компьютерных мониторов), 472

## П

пароли

keylogger, 273, 304–305  
«лобовая» атака, 225–229  
BIOS, 122–130, 150  
LAN Manager  
хешированные пароли, 153  
администратора, 123  
альтернативные решения, 245–250  
восстановление, 126  
выбор пароля, 153, 217–219  
диалоговое окно входа в систему, 132  
длина пароля, 153  
жесткий диск, 129  
изменение, 244  
использование разных паролей для разных областей, 243  
коммутируемые сети, 239  
ненадежные пароли, 216–220  
операционной системы Windows, 131–136, 138–140, 153  
отгадывание, 125, 133–134, 220, 222  
пароли по умолчанию, 359  
подбор с помощью словаря, 224–225  
подглядывание, 237, 361  
пользователя, 123  
сгенерированный случайно, 242  
социотехника, 243  
устойчивые пароли, 241–242  
учетные записи службы мгновенных сообщений, 183

хранение списка паролей, 244–245  
«хранители экрана», 132–133  
электронная почта, 181–183  
пароли Award BIOS, 124  
пароли к «хранителям экрана», 132–133  
пароли по умолчанию, 358–359  
пароль администратора, 121  
Патриотический Акт США (USAPA)  
аналитика, 73  
беспокойство по поводу Акта, 97  
влияние на законы штатов, 78–79  
Закон о компьютерном мошенничестве и злоупотреблениях, 74, 76  
Закон о прослушивании линий связи, 73–75  
Закон о хранимой информации, 73  
Закон об иностранной разведке, 74–75, 77  
положения, 78  
последствия, 32, 72–76, 78–79  
пейджеры, 451–454  
перебор паролей, 225–227  
переплетчики (троянские кони), 319–320  
персональные брандмауэры keylogger, 299  
преимущества использования, 372–373  
троянские кони, 325–330  
уязвимые места, 300  
пломбы, 305  
ПО для обнаружения троянских коней, 335–337  
 побочное излучение, 463–471  
поддержка читателей издательства Wiley, 506  
подслушивание мобильных переговоров, 443–451  
поиск беспроводных сетей, 397–403, 407, 411–417  
политика безопасности, 114–118

- политика паролей, 241  
пользовательский пароль, 121  
последний набранный номер (телефоны), 443  
последовательность загрузки компьютера, 122  
потребительская электроника, 455–460  
почтовые серверы, 382–385  
правительственные разведывательные учреждения, 36–40  
**Правительственный Центр защиты национальной инфраструктуры (NIPC)**, 136  
преследование, 459  
приемы социотехники, 105–106, 243  
приложения для управления паролями, 244–245  
проблемная группа проектирования Internet, 117  
программа тайных проникновений (ФБР), 94–95  
программные брандмауэры, 372–373  
программы анонимной пересылки корреспонденции, 382–383  
программы архивации, 255  
программы безвозвратного удаления файлов, 206–209  
программы для взлома паролей Advanced NT Security Explorer, 143  
BIOS, 149–150  
Chntp (Change NT password), 148  
CIA Commander, 145–146  
ClearLogs, 147  
Dialpwd, 239  
ElcomSoft, 233–234  
ERD Commander, 145  
FakeGINA, 144  
Glide, 236–237  
iOpus Password Recovery XP, 238  
John the Ripper, 148  
LOphCrack, 141–143  
NTFSDOS, 147  
Passware Kit, 234–235  
Password Recovery Toolkit набор утилит, 233  
PasswordSpy, 238  
PhoneBook Viewer v1.01c, 239  
Pwdump, 144–145  
PWLHack, 237  
PWLTool, 237  
PWLView, 237  
Ratware программа для обхода защиты «хранителя экрана» в Win9x, 141  
Revelation, 237–238  
Scrsavpw, 141  
Snitch, 237–238  
WinZapper, 147  
WS\_FTP, 237  
пароли к приложениям, 231–232  
распределенные сетевые атаки (DNA), 233  
ресурсы, 234–235  
программы мониторинга клавиатуры, 275–282, 287–288  
программы мониторинга реестра keylogger, 299–300  
троянские приложения, 333–334  
программы обнаружения keylogger PestPatrol, 302  
Spybot Search & Destroy, 302–303  
SpyCop, 279, 302  
Who's Watching Me, 302  
использование ПО, 300–301

программы очистки журнала, 147  
программы перехвата пакетов для беспроводных сетей, 418–421  
программы перехвата сетевых пакетов, 303, 353  
AiroPeek NX, 419  
Altvore, 355  
Cain & Abel, 367  
DragNet, 355  
Dsniff, 366  
Ethereal, 365–366  
Ettercap, 366–367  
keylogger, 303  
NetIntercept, 355  
RetrievalWare, 355  
SilentRunner, 354  
Sniffer Wireless, 419  
запуск внутри вашей собственной сети, 377  
наблюдение, 353  
опасности, 420  
программы перехвата для беспроводных сетей, 417–421  
тロянские кони, 329–330, 333  
программы проверки целостности файлов 333–334  
keylogger, 299–300  
тロянские кони, 333–334  
программы регистрации сетевых адресов, 60, 75  
программы сертификации, 159  
программы сканирования портов, 377  
прокси-серверы и веб, 383–385  
прослушивание беспроводных телефонов, 444–446  
прослушивание линий связи внутрисемейные случаи, 85–87

Закон о сотрудничестве компаний, предоставляющих услуги связи, с правоохранительными органами, 64  
статистика, 66–67  
телефоны, 439  
шифрование, 67  
прослушивание телефонов, 438–442

## Р

работа с замками, 102  
разведывательные управления, 36–40  
раздельные пароли, 243  
распознавание символов, 250  
распределенные сетевые атаки (DNA), 233  
региональная компьютерная судебная лаборатория (RCFL), 157  
регистраторы сетевых адресов, 60, 75  
редактор шестнадцатеричных кодов, 170–171, 190–192  
реестр, 176–177  
Руководство по безопасности Управления национальной безопасности, 117  
Рэйган, Брайен Патрик (шпион), 479–480

## С

сбрасыватели (тロянские приложения), 321  
Сверинген, Вес, Секреты ФБР: разоблачение агента, 95  
светодиодные индикаторы состояния, 472  
Секреты ФБР: разоблачение агента, Вес Сверинген, 95

- сетевые атаки  
NetBIOS, 351–353, 380  
активная атака, 340  
анализ трафика, 344  
враждебные веб-сайты, 360  
враждебные  
приложения, 359  
журналы сервера, 355  
компрометация  
информации, 343–346  
компьютеры общественного  
пользования, 360–361,  
380  
контрмеры, 367–385  
локализация цели, 348–349  
начальные точки, 341–343  
определение версии  
операционной  
системы, 350–351  
пароли по умолчанию,  
358–359  
пассивная атака, 340  
поиск уязвимых мест, 351  
программы перехвата  
сетевых пакетов,  
353–355  
сканирование портов,  
349–350  
сканирование при помощи  
программы ping, 349  
случайные атаки, 341  
тайные проникновения, 91–93  
файлы журнала, 356–358  
файлы Windows с общим  
доступом, 351–353,  
380–382  
целевые атаки, 340–341  
широкополосные  
подключения, риски,  
344–346
- сетевые мониторы  
AiroPeek NX, 419  
Altivore, 355  
Cain & Abel, 367  
DragNet, 355
- Dsniff, 366  
Ethereal, 363–365  
Ettercap, 366–367  
keylogger, 303  
NetIntercept, 355  
RetrievalWare, 355  
SilentRunner, 354  
Sniffer Wireless, 419  
запуск внутри вашей  
собственной сети, 376  
наблюдение, 353–355  
опасности, 420  
программы перехвата  
для беспроводных  
сетей, 418–420  
троянские кони, 332–333  
сетевые подключения, 376  
символы для обозначения  
состояния беспроводных  
сетей, 404  
система глобального  
позиционирования  
(GPS), 409–410, 458–459  
системные требования  
для работы утилит, 505  
системный блок,  
опломбирование, 305  
системы архивирования  
на магнитной ленте, 269  
системы голосовой  
почты, 449–451  
системы мониторинга  
клавиатуры (KLS), 280–281  
системы обнаружения  
вторжений  
(IDS), 368–369, 424–425  
сканеры отпечатков  
пальцев, 247–248  
сканеры сетчатки глаза, 248–249  
сканирование портов, 349  
сканирование при помощи  
программы ping, 349  
Скарфо, Никодермо-младший  
(гангстер), 280–281  
скрытые файлы, 168

- службы обмена мгновенными сообщениями, 183–184, 378–379
- службы сканирования портов, 371
- случайным образом сгенерированные пароли, 242
- смарт-карты, 249–250
- смена паролей, 244
- социотехника, 105–106, 243
- Союз американских гражданских свобод, 73
- специально разработанное keylogger, 291
- Справочник по безопасности сайтов (RFC2196), IETF*
- проблемная группа проектирования Интернет, 117
- средства восстановления данных, 192–193
- средства дублирования информации, 187–189
- средства мониторинга клавиатуры
- eBlaster, 47
  - God, 300
  - Hardware
    - KeyLogger, 290–291
    - Investigator, 288
    - Invisible KeyLogger
      - Stealth (IKS), 287
    - KeyGhost, 288–290
    - KeyKatcher, 290
    - keylogger на заказ, 291
    - Linux, 306
    - Magic Lantern проект, 292
    - Spector Professional Edition, 286–287
    - WinWhatWhere Investigator программа, 288
- аппаратные keylogger, 282–286, 288–291
- библиотеки периода выполнения на VB, 298–299
- веб-камеры, 279
- возможности, 278–279
- встроенные в клавиатуру, 303–304
- кампании
- по дезинформации, 294–295
- контрмеры, 293–299
- мониторинг операций
- записи в файлы, 296–299
- нарушения Закона о прослушивании линий связи, 86
- обзор, 286
- обнаружение, 277, 293–299, 303–308
- определение, 273
- пароли, 304, 306
- персональные брандмауэры, 299
- поиск строки, 299
- программные keylogger, 275–282, 286–288
- программы мониторинга реестра, 299–300
- программы перехвата сетевых пакетов, 303
- программы проверки целостности файлов, 299–300
- распространение, 274
- система мониторинга клавиатуры (KLS), 281
- скрытие, 277
- сообщения об ошибках, 306
- стоимость, 286
- удаление, 306–307
- средства наблюдения ECHELON, 24, 473–478, 481
- веб-камеры, 500, 502
- устройства для регистрации сетевых адресов, 60, 75

статистика  
кражи ноутбуков, 130  
наблюдения  
за сотрудниками,  
28–30  
операций  
по прослушиванию  
линий связи, 66–67  
стеганография, 202–206  
«стойкое» шифрование,  
240–241  
страничный файл, 175  
суд по делам иностранной  
разведки, 62  
судебная экспертиза  
(компьютерной техники)  
дискеты, 185–186  
доказательства  
в веб-браузерах,  
178–180  
жесткие диски, 184–185  
мгновенные  
сообщения, 183–184  
память, 186  
первичные задачи, 163–164  
ПО для автоматического  
сбора и анализа  
доказательств,  
165, 186–187  
экспертиза вручную, 165  
системный реестр, 176–177  
файлы, 167–180  
электронная почта, 181–183  
Сучита, Николас  
(шпион-любитель), 45

**Т**

тайные проникновения  
«внутренняя команда», 95  
документирование  
обстановки, 108–109  
законность, 89, 95–96  
зачистка, 110  
команда наблюдения, 95  
команда надзора, 95

команда управления, 96  
компьютерный шпионаж, 91  
контрмеры, 110–118  
определение, 89  
отход с места операции,  
110–111  
планирование, 92–93, 97–101  
пробный рейд, 99–100  
проникновение  
в здание, 103–108  
сбор информации, 109–110  
сетевые атаки, 91–92  
случайные атаки, 93  
судебный ордер, 95  
транспортная команда, 95  
Уотергейтское дело, 92  
уязвимые места, 101  
физические атаки, 91  
шесть правил, 101–102  
*Как услышать это,*  
Аррингтон, Уинстон, 439  
террористическая атака  
11 сентября, 72  
тестирование  
брандмауэров, 371  
троянских приложений,  
325–326  
техническая поддержка  
веб-сайтов, 506  
технические консультанты, 33, 36  
технические контрмеры для  
защиты от наблюдения, 499  
технические контрмеры,  
направленные  
на предотвращение  
визуального наблюдения, 499  
Тобиас, Марк, Замки, сейфы  
и безопасность, 107  
торговая палата США, 25  
«троянские кони», 321–331  
троянские приложения  
Back Orifice, 327  
HTML-приложения, 323–324  
LANfiltrator, 327–328  
NetBus, 321, 326  
Net-Devil, 328

Optix, 328  
pcAnywhere, 330–331  
Sub7, 327  
VNC (вычисления в виртуальных сетях), 331  
антивирусное ПО, 335–336  
архиваторы, 320  
вандализм, 312  
веб-камеры, 312  
возможности, 311–313  
исходные коды, 312–313  
клиентская часть, 315  
контрмеры, 331–337  
культура разработчиков и пользователей, 329  
локальный доступ к системе, 313  
обнаружение, 319–321, 332–337  
определение, 309  
переплетчики, 321  
персональные брандмауэры, 333, 370, 372–373  
ПО для обнаружения, 335–337  
порты, 315, 330  
принципы работы, 310–311, 313–316  
программы мониторинга реестра, 333–334  
программы перехвата сетевых пакетов, 333  
программы проверки целостности файлов, 333–334  
распространение, 326–327  
редактор сервера, 315  
самовоспроизведение, 313  
«сбрасыватели», 320–321  
серверная часть, 314  
тестирование, 325–326  
удаление, 336  
удаленный доступ, 313–314  
установка, 321–325  
туннелирование, 374

## У

уголовный суд, 81–83  
удаление keylogger, 307  
троянских приложений, 336  
удаленный доступ беспроводные сети, 397  
троянские приложения, 313–314  
универсальная последовательная шина (USB), 260–261  
Уотергейтское дело, 92  
упаковщик UPX, 320  
Управление национальной безопасности, 38–39, 154  
усовершенствованный стандарт шифрования (AES), 233  
устройства для чтения флэш-памяти, 262–264  
утилиты Abi-Coder, 200  
Advanced NT Security Explorer, 143, 145  
AirDefense, 425  
Air-Jack, 411  
AirMagnet, 423  
AiroPeek NX, 418  
AirSnort, 421  
Altivore, 355  
Baseline Security Advisor, 150  
BestCrypt, 200–201  
BlackIce PC Protection, 369  
Blowfish Advanced CS, 199  
BOClean, 335  
BWMACHAK, 394  
Cain & Abel, 367  
Chntpw (Change NT password), 148  
CIA Commander, 145–146  
ClearLogs, 147  
Cmospwd, 127, 140  
Cryptcat, 270–271  
CyberScrub, 210  
dd (data dumper), 188

- Dialpwd, 239  
Distributed Network Attack (DNA), 233  
DragNet, 355  
DragonWare Suite, 482  
DriveCrypt, 202  
Dshield, 374  
Dsniff, 366  
EasyRecovery Professional, 193  
ElcomSoft, 233–234  
EnCase, 188–189  
ERD Commander, 145  
Ethereal, 365–366  
Ettercap, 366–367  
Fake AP, 425  
FakeGINA, 144  
File Monitor, 297–298  
File Viewer, 190  
FIREWAR, 371  
Forensic Toolkit (FTK), 189  
GFI LANguard программа мониторинга целостности системы, 334  
Glide, 236–237  
IIP, 379  
ILook, 190  
Inzider, 375  
iOpus Password Recovery XP, 238  
John the Ripper, 148  
KeyDisk, 129  
Kismet, 417–418  
Kiwi Syslog Daemon, 372  
Legion, 364–365  
LOphtCrack, 141–143  
MapPoint, 421–422  
MSinfo32, 296  
MyNetWatchman, 374  
Nessus, 364  
NetCat, 270–271  
NetIntercept, 355  
NetStumbler, 400, 416–417  
Nmap, 362–363  
Norton Ghost, 187  
Norton Utilities, 193  
NSSpyglass, 424–425  
NTFSDOS, 147  
OnlyMe, 456  
Passware Kit, 234–235  
Password Recovery набор утилит, 233  
PasswordSpy, 238  
PDA Defense, 456  
PestPatrol программа для обнаружения keylogger, 302  
PGPfone, 442  
PhoneBook Viewer v1.01 с, 239  
Pretty Good Privacy (PGP), 66, 197, 377  
Private Idaho (PI), 383  
Process Explorer, 295–296  
Pwdump, 144–145  
PWLHack, 237  
PWLTool, 237  
PWLVView, 237  
Quick View Plus, 192  
Ratware программа для обхода защиты с помощью хранителя экрана в Win9x, 141  
RegEdit, 177–178  
RegistryProt, 334  
RetrievalWare, 355  
Revelation, 237–238  
SafeBack, 187  
SamSpade, 362–363  
Scrsavpw, 141  
Securepoint Intrusion Detection, 369  
Sentry 2020, 456  
SilentRunner, 354  
Sniffer Wireless, 419  
Snitch, 237–238  
Snort, 369  
Speak Freely, 441  
SpyShield, 379

- Spbot Search & Destroy  
программа  
для обнаружения  
keylogger, 302–303
- SpyCop программа  
для обнаружения  
keylogger, 278, 301
- Stealth Email Redirector  
(SER), 359
- Steganos Security Suite, 200
- Stegdetect, 205
- S-Tools, 205
- StumbVerter, 422
- Stunnel, 375
- SuperScan, 363
- SurfSecret Privacy  
Protector, 210
- Tauscan, 335–336
- TCPView, 375
- TDlmon, 375
- TealLock, 456
- Trillian, 378
- Trojan Defense Suite  
(IDS), 335
- Trojan Hunter, 335
- WallWatcher, 372
- wbStego4, 206
- Who's Watching  
Me программа  
для обнаружения  
keylogger, 302
- Window Washer, 210
- WinHex, 191–192
- WinZapper, 147
- WS\_FTP, 237
- анонимной пересылки  
корреспонденции,  
382–383
- дисковый  
редактор, 190
- очистки журнала, 146–147
- редактор  
шестнадцатеричных  
кодов, 169, 190–192
- системные требования,  
505–506
- системы обнаружения  
вторжений (IDS), 368–369
- уязвимые места  
BIOS, 121–132  
Internet Explorer, 360  
беспроводных сетей, 390–397  
брандмауэров, 371–373  
наблюдение, 351  
операционной системы  
Windows, 120, 131–142
- определение, 49
- персональных  
брандмауэров, 300
- программного обеспечения  
Microsoft, 337
- сканеров отпечатков  
пальцев, 247–248
- тайные  
проникновения, 101–102
- электронной почты, 182–183
- Ф**
- файл подкачки, 175
- файлы  
альтернативный поток данных  
(ADS), 172–174  
буфер обмена, 178  
временные файлы, 169  
временные файлы, созданные  
программой Scan Disk,  
172  
время создания,  
модификации,  
обращения, 167  
изменение расширений,  
169–170  
кластеры, 174  
Корзина, 173  
неиспользуемое дисковое  
пространство, 174–175  
общий доступ к файлам  
из Windows,  
351–353, 380–382  
остатки кластеров, 173  
реестр, 176–177  
скрытые файлы, 168–169

- список последних файлов, 177  
страничный файл, 175  
удаленные файлы, 171–172  
файл подкачки, 175  
файлы INFO, 172  
файлы спулинга печати, 171–172  
шифрование, 198–200  
ярлыки, 167–168  
файлы журнала  
брандмауэра, 372  
сетевых атак, 355–356  
факсы, 431–433  
фальсификация  
MAC-адресов, 394  
протокола разрешения  
адресов (ARP), 354  
фальсификация  
протокола разрешения  
адресов (ARP), 354  
фальшивые сети  
утилита Fake AP, 425  
ФБР  
DCS-1000/Carnivore  
программа, 354, 482–485  
Magic Lantern проект, 292, 485–488  
отчеты о  
кибер-преступлениях, 80  
подразделение  
технических  
специалистов, 98  
программа тайных  
проникновений, 95  
расследования, 33, 80–81  
региональные  
компьютерные  
судебные лаборатории  
(RCFL), 157  
системы мониторинга  
клавиатуры  
(KLS), 281  
специальные оперативные  
группы (SOG), 96  
федеральное  
законодательство  
воплощение законов  
в жизнь, 79–81  
Закон о защите электронных  
систем связи, 64–67, 83  
Закон о компьютерном  
мошенничестве  
и злоупотреблениях,  
67–68, 70, 76  
Закон о прослушивании  
линий связи,  
58–61, 74, 86  
Закон о сотрудничестве  
компаний,  
предоставляющих услуги  
связи,  
с правоохранительными  
органами, 63–64  
Закон о хранимой  
информации, 66–67, 73  
Закон об иностранной  
разведке, 61–62, 64,  
74–75, 77  
Закон об экономическом  
шпионаже, 71  
Национальный закон  
о трудовых  
взаимоотношениях, 84  
Патриотический Акт  
США, 31, 72–76, 78, 97  
физические атаки (тайные  
проникновения), 91  
Филлер, Рассел (подрядчик  
NASA), 377
- X**
- Хансен, Роберт (шпион, бывший  
агент ФБР), 104, 259–260  
характеристики  
доказательств, 191

**Ц**

цветовые коды  
(осведомленности и подготовленности), 48

Центр демократии и технологий, 73

Центральное Разведывательное Управление (ЦРУ), 38–39

центральный координатор по присвоению уникальных параметров протоколов Интернет, 350

цепочка владельцев, 162

Цирези, Майк (политик), 357–358

цифровой видеомагнитофон TiVo, 460

цифровые камеры, 271, 457, 499–503

ЦРУ (Центральное Разведывательное Управление), 38

**Ч**

частные детективы, 33–36

черви

- Badtrans.B, 496
- SirCam, 495
- контрмеры, 498
- определение, 493
- разведывательные черви, 492–497

Чирилло, Джон, *Атаки хакеров раскрыты*, 348

**Ш**

шифрование

- Abi-Coder утилита для шифрования файлов, 200

Advanced Encryption Standard (AES), 233

Blowfish Advanced CS утилита для шифрования файлов, 199

Data Encryption Standard (DES), 194, 226

EFS (шифрованная файловая система), 154

GnuPG (Gnu Privacy Guard), 198

Pretty Good Privacy (PGP), 67, 197–198

КПК, 455–457

криptoанализ, 228–229

мгновенные сообщения, 378–379

мобильные телефоны, 446–447

ненадежное шифрование, 215–216

определение, 194

продукты Microsoft, 235–237

прослушивание линий связи, 66

советы по использованию, 195–196

сотовые телефоны, 446–447

стеганография, 202–206

стойкое шифрование, 240–241

файлы, 198–200

факсы, 431–433

шифрование «на лету», 200

шифрованная файловая система (EFS), 146, 154, 201

шпионаж за печатными машинками, 273–274

электронная почта, 197–198, 378

шпионы

- анализ рисков, 49–53
- взломщики, 40–41
- доносчики, 41–44
- друзья и семья, 44–47

защита от шпионов, 47–49  
 консультанты, 33, 36  
 криминальные  
   шпионы, 40–41  
 любители, 21  
 мотивация, 24–25  
 начальники, 28–30  
 полиция, 30–33  
 правительственные  
   разведывательные  
   управления, 38–40  
 профессионалы, 22  
 частные сыщики, 34–36  
 шпионы-«невидимки»,  
   36–37  
 экономические  
   шпионы, 25–28

**Э**

Эйджи, Филипп, *Взгляд  
 изнутри: дневник ЦРУ*, 273  
 экономическая разведка, 25  
 экономические шпионы, 25–28

экономический  
   шпионаж, 25–28, 38–40  
 электромагнитный  
   шпионаж, 463–470  
 электронная почта  
   Stealth Email Redirector  
     (SER), 359  
 клиенты, 181–183  
 копирование данных, 269  
 пароли, 182–183  
 почтовые веб-серверы, 381  
 программы анонимной  
   пересылки, 382–383  
 судебная экспертиза, 180–182  
 уязвимые места, 182  
 шифрование, 194–202,  
   377–378  
 эманация, 465–470  
 энергонезависимая  
   память, 262–264

**Я**

Янг, Джон (доносчик), 43  
 ярлыки, 355