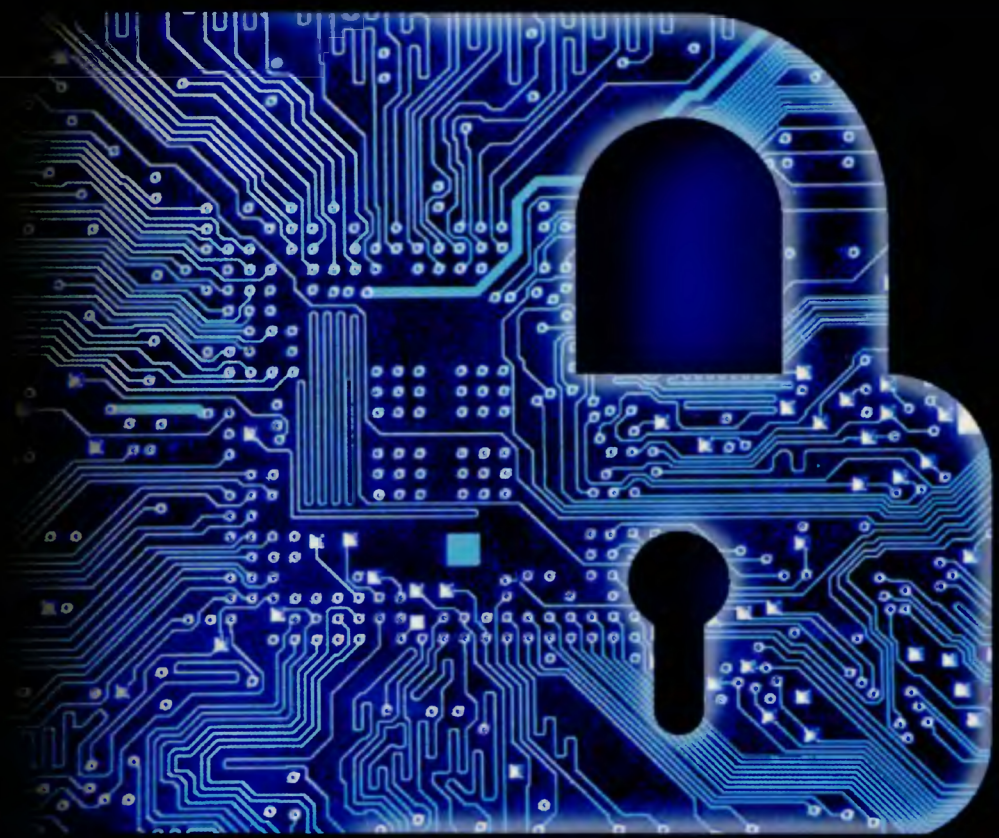
Камский В. А.

Защита личной информации в Интернете, смартфоне и компьютере



Как защититься от вирусов в Интернете, защита файлов в компьютере, защита электронной почты, анонимность в Интернете, защита личных данных в смартфоне, Tor и VPN

НиТ издательство

Камский В. А.

Защита личной информации

в Интернете, смартфоне и компьютере

Наука и Техника

Санкт-Петербург
2017

УДК 004.056

ISBN 978-5-94387-731-5

Камский В. А.

ЗАЩИТА ЛИЧНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТЕ, СМАРТФОНЕ И КОМПЬЮТЕРЕ. — СПб.: Наука и Техника, 2017. — 272 с., ил.

Серия «Просто о сложном»

По статистике большинство пользователей персональных компьютеров и Интернета сами позволяют похищать/использовать свои личные данные злоумышленникам или просто подкованным в техническом плане третьим лицам. И ущерб от таких противоправных действий колеблется от незначительного до катастрофического. Никто не поможет лучше всего защитить ваши данные чем ... вы Сами!

И эта книга вам в этом поможет. Простым и понятным языком здесь рассказано как эффективно защитить свою электронную почту, какими способами лучше воспользоваться для этой цели, а также приведены примеры взлома электронной почты. Вы узнаете как стать анонимным в Интернете, чтобы вас не беспокоили назойливые правила форумов, как защититься от вирусов в Интернете, что такое проект Tor и VPN-анонимайзер.

Пользователям Android-устройств (сотовых телефонов, смартфоны, планшеты) будет полезно прочитать, как защитить свои личные данные на своем портативном устройстве, что такое криптоконтейнер и как пользоваться защитой от прослушки.

Для пользователей персональных компьютеров будет важно узнать, что такое шифрование вашего жесткого диска, какими программами лучше для этого пользоваться, как защитить свои данные средствами вашей операционной системы, как защитить свою домашнюю сеть от нежданных гостей или назойливых соседей и многое другое.

Книга будет полезна всем, кто хочет быть спокойным за свои данные всегда и везде!

Контактные телефоны издательства:
(812) 412 70 25, (812) 412 70 26, (044) 516 38 66

Официальный сайт: www.nit.com.ru

© Камский В.А., ПРОКДИ, 2017
© Наука и техника (оригинал-макет), 2017

Содержание

ВВЕДЕНИЕ 11

Аудитория 11

Как читать эту книгу? 12

ЧАСТЬ 1. ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ 14

ГЛАВА 1. СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ 15

1.1. МЕТОДЫ КРИПТОГРАФИИ. СИММЕТРИЧНАЯ И АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ 15

1.2. АЛГОРИТМЫ ШИФРОВАНИЯ 16

1.3. СРЕДСТВА ЗАЩИТЫ ЭЛЕКТРОННОЙ ПОЧТЫ 19

1.3.1. PGP 19

1.3.2. Стандарт S/MIME 21

1.3.3. Безопасные почтовые сервисы. HushMail 22

1.3.4. Плагины браузера 25

Плагин браузера PGP Mail 25

Плагин браузера SecureGmail 26

Плагин браузера Encrypted Communication 27

1.3.5. Плагины почтовых клиентов 28

Плагин почтового клиента Enigmail 28

Плагин почтового клиента CyberSafe Mail 28

1.4. СРАВНЕНИЕ СРЕДСТВ ЗАЩИТЫ. ВЫБОР ИДЕАЛЬНОГО СРЕДСТВА .. 28

1.4.1. Проблема выбора 28

1.4.2. Выводы 34

ГЛАВА 2. КАК ВЗЛОМАТЬ ЭЛЕКТРОННУЮ ПОЧТУ 35

2.1. ТРОЯНСКИЙ КОНЬ 36

2.2. ВЗЛОМ ПО НОМЕРУ ТЕЛЕФОНА 41

2.3. ФИЗИЧЕСКИЙ ДОСТУП К КОМПЬЮТЕРУ 43

2.4. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ИЛИ ПРОСТО ОБМАН 46

2.5. МОДНОЕ СЛОВО «ФИШИНГ» 47

2.6. ВОССТАНАВЛИВАЕМ ПАРОЛЬ 50

2.7. КРАЖА COOKIES 51

2.8. XSS-УЯЗВИМОСТИ 52

2.9. МЕТОД ГРУБОЙ СИЛЫ 53

ГЛАВА 3. ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ 55

3.1. НЕМНОГО ТЕОРИИ. S/MIME, PKI И PGP 56

3.2. КАК БУДЕМ ЗАЩИЩАТЬ ПОЧТУ 58

3.3. ИСПОЛЬЗОВАНИЕ OPENSSL 59

3.4. ИСПОЛЬЗОВАНИЕ CYBERSAFE TOP SECRET 60

3.5. НАСТРОЙКА MICROSOFT OUTLOOK 64

3.6. НАСТРОЙКА ШИФРОВАНИЯ В ДРУГИХ ПОЧТОВЫХ КЛИЕНТАХ 70

ГЛАВА 4. ЭЛЕКТРОННАЯ ПОДПИСЬ 73

4.1. ЧТО ТАКОЕ ЭЛЕКТРОННАЯ ПОДПИСЬ? 74

4.2. СЛУЧАИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ В НЕБОЛЬШОЙ КОМПАНИИ 74

4.2.1. Внутренний документооборот 74

4.2.2. Обмен документами с филиалами и партнерами 75

4.2.3. Некоторые проблемы внедрения электронной подписи 76

4.3. РАБОТА С ЭЛЕКТРОННОЙ ПОДПИСЬЮ ПОСРЕДСТВОМ ПОЧТОВОГО КЛИЕНТА 77

4.4. РАБОТА С ЦИФРОВОЙ ПОДПИСЬЮ В LINUX 79

ЧАСТЬ 2. ЗАЩИТА ПЕРЕДАВАЕМЫХ ДАННЫХ И АНОНИМНОСТЬ В ИНТЕРНЕТЕ 85

ГЛАВА 5. КАК СТАТЬ АНОНИМНЫМ В ИНТЕРНЕТЕ 85

5.1. ПОСТАНОВКА ЦЕЛЕЙ 86

5.2. ВЫБОР СПОСОБА ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ 87

5.2.1. Разовое сокрытие IP-адреса и анонимайзеры 87

5.2.2. Постоянное сокрытие IP-адреса и анонимные прокси 88

5.2.3. Изменение региона, сокрытие IP и шифрование данных ... 90

5.3. ПОДВОДИМ ИТОГИ 92

5.4. ЧТО ЕЩЕ НУЖНО ЗНАТЬ ОБ АНОНИМНОСТИ 92

ГЛАВА 6. ПРОЕКТ TOR 94

6.1. ПРИНЦИП РАБОТЫ TOR 95

6.2. ЧТО ЛУЧШЕ – TOR ИЛИ VPN? 97

6.3. КОМБИНИРУЕМ VPN И TOR 98

6.4. ЧТО ДЕЛАТЬ С DNS-ТРАФИКОМ? 98

6.5. ИСПОЛЬЗОВАНИЕ TOR 99

ГЛАВА 7. ПРОСТОЙ VPN-АНОНИМАЙЗЕР: PIA (PRIVATE INTERNET ACCESS) 105

7.1. КАК РАБОТАЕТ PIA 106

7.2. КАК УСТАНОВИТЬ PIA 106

7.3. ИСПОЛЬЗОВАНИЕ PIA 109

ГЛАВА 8. ЗАЩИТА ОТ ВИРУСОВ В ИНТЕРНЕТЕ 111

8.1. КАК БУДЕТ ПРОИЗВОДИТЬСЯ ТЕСТИРОВАНИЕ 113

8.2. KASPERSKY INTERNET SECURITY 114

8.3. DR.WEB SECURITY SPACE 126

8.4. ESET SMART SECURITY 135

ЧАСТЬ 3. ЗАЩИЩАЕМ ФАЙЛЫ НА WINDOWS-КОМПЬЮТЕРЕ 138

ГЛАВА 9. ВЫБОР СРЕДСТВА ЗАЩИТЫ ДАННЫХ 139

9.1. ШИФРОВАНИЕ ДИСКА 139

9.2. КРИПТОКОНТЕЙНЕРЫ, ИЛИ ВИРТУАЛЬНЫЕ ДИСКИ 143

9.3. ПРОЗРАЧНОЕ ШИФРОВАНИЕ 144

ГЛАВА 10. ШИФРОВАНИЕ СРЕДСТВАМИ ОПЕРАЦИОННОЙ СИСТЕМЫ 146

10.1. ПРОЗРАЧНОЕ ШИФРОВАНИЕ ПОСРЕДСТВОМ EFS 147

10.1.1. Преимущества и недостатки EFS 147

10.1.2. Активация EFS-шифрования 149

10.1.3. Использование программы Advanced EFS Data Recovery для расшифровки зашифрованных EFS файлов 153

10.2. СРЕДСТВО ШИФРОВАНИЯ ДИСКА BITLOCKER 159

10.2.1. Что такое BitLocker 159

10.2.2. Шифрование диска 161

10.2.3. Работа с зашифрованным диском 165

10.2.4. Забыт пароль. Что делать? 166

10.3. ФАЙЛОВАЯ СИСТЕМА ECRYPTFS В LINUX 167

10.4. МОЖНО ЛИ ДОВЕРЯТЬ СТАНДАРТНОМУ ШИФРОВАНИЮ? 168

ГЛАВА 11. ШИФРОВАНИЕ ЖЕСТКОГО ДИСКА СТОРОННИМИ ПРОГРАММАМИ. TRUECRYPT И ЕЕ ПРОИЗВОДНЫЕ 169

11.1. ВЫБОР СТОРОННЕЙ ПРОГРАММЫ ДЛЯ ШИФРОВАНИЯ 170

11.2. ПРОГРАММА TRUECRYPT 171

11.2.1. История TrueCrypt и что случилось с проектом 171
11.2.2. Возможности программы 173
11.2.3. Использование программы 175
Установка программы 175
Создание виртуального диска (контейнера) 177
Шифрование всего раздела 185

11.3. ПРОГРАММА VERACRYPT 189

11.4. ПРОГРАММА CIPHERSHED 190

11.5. ПРОГРАММА CYBERSAFE И R-STUDIO 191

ГЛАВА 12. ПРОЗРАЧНОЕ ШИФРОВАНИЕ ПО ЛОКАЛЬНОЙ СЕТИ 195

12.1. СЛОЖНОСТИ С СЕТЕВЫМ ШИФРОВАНИЕМ В ЛОКАЛЬНОЙ СЕТИ .. 196

12.2. КАК УСТРОЕНО ПРОЗРАЧНОЕ ШИФРОВАНИЕ В CYBERSAFE 197

12.3. НАСТРОЙКА ПРОЗРАЧНОГО ШИФРОВАНИЯ 198

ГЛАВА 13. НЕКОТОРЫЕ ПОЛЕЗНЫЕ ПРОГРАММЫ 202

13.1. ПРОГРАММА FOLDER LOCK 203

13.1.1. Возможности программы 203
13.1.2. Использование программы 203

13.2. ERASER: УДАЛЕНИЕ ИНФОРМАЦИИ БЕЗ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ 209

ЧАСТЬ 4. ЗАЩИТА ДАННЫХ НА МОБИЛЬНОМ УСТРОЙСТВЕ ANDROID 211

ГЛАВА 14. ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ. MAILDROID 211

14.1. НЕОБХОДИМЫЕ ПРИЛОЖЕНИЯ 212

14.2. НАСТРОЙКА CRYPTO PLUGIN 212

14.3. НАСТРОЙКА MAILDROID 215

14.4. ПОСЛЕ УСТАНОВКИ MAILDROID 217

ГЛАВА 15. ЗАЩИТА ВАЖНЫХ ДОКУМЕНТОВ С ПОМОЩЬЮ КРИПТОКОНТЕЙНЕРА 221

15.1. ЗАЧЕМ НУЖНО ЗАЩИЩАТЬ ДАННЫЕ НА ANDROID-УСТРОЙСТВЕ .. 222

15.1.1. Способы защиты данных.....222

15.1.2. От кого защищаем данные? 222

15.1.3. Блокировка запуска приложения и запрет просмотра галереи 224

15.2. ШИФРОВАНИЕ ВСЕГО УСТРОЙСТВА..... 225

15.3. ВЫБОР ANDROID-ПРИЛОЖЕНИЯ ДЛЯ РАБОТЫ С КРИПТОКОНТЕЙНЕРАМИ 226

15.4. ПРИЛОЖЕНИЕ CYBERSAFE MOBILE 228

15.5. ПРИЛОЖЕНИЕ EDS LITE..... 232

ГЛАВА 16. ЗАЩИТА ФОТО И ВИДЕО "НА ЛЕТУ" 236

16.1. ПРИЛОЖЕНИЯ ДЛЯ ЗАЩИТЫ ФОТО И ВИДЕО 237

16.2. ПРИЛОЖЕНИЕ HIDE PICTURES & VIDEOS..... 237

16.3. CYBERSAFE MOBILE..... 243

ГЛАВА 17. ШИФРОВАНИЕ ОБЛАЧНОГО ДИСКА GOOGLE DRIVE..... 247

17.1. ШИФРОВАНИЕ И СИНХРОНИЗАЦИЯ ПАПКИ ОБЛАЧНОГО ДИСКА .. 248

17.2. ПРОСТОЕ ШИФРОВАНИЕ ОБЛАЧНОЙ ПАПКИ..... 252

17.3. ПЕРЕДАЧА ЗАШИФРОВАННЫХ ФАЙЛОВ ДРУГИМ ПОЛЬЗОВАТЕЛЯМ С ПОМОЩЬЮ GOOGLE DRIVE 254

ГЛАВА 18. ЗАЩИТА ПЕРЕДАВАЕМЫХ ПО СЕТИ ДАННЫХ ОТ ПРОСЛУШИВАНИЯ 255

18.1. КАК ЗАЩИЩАТЬ ПЕРЕДАВАЕМЫЕ ПО СЕТИ ДАННЫЕ В ANDROID? 256

18.2. ВЫБОР VPN-СЕРВИСА 257

18.3. НАСТРОЙКА VPN-КЛИЕНТА 258

18.4. TOR В ANDROID 259

ГЛАВА 19. ОБЗОР ANDROID-ПРИЛОЖЕНИЙ ДЛЯ ШИФРОВАНИЯ ДАННЫХ 262

19.1. МНОГООБРАЗИЕ ВЫБОРА 263

19.2. ПРИЛОЖЕНИЯ ДЛЯ ШИФРОВАНИЯ ОБЛАКА 263

19.3. КРАТКОЕ ОПИСАНИЕ ПРИЛОЖЕНИЙ ШИФРОВАНИЯ..... 264

19.4. СРАВНЕНИЕ ПРИЛОЖЕНИЙ ДЛЯ ШИФРОВАНИЯ..... 266

ЗАКЛЮЧЕНИЕ 269





Введение



Введение

В современном мире утечка конфиденциальной информации может повлечь серьезные последствия, но при этом многие пользователи используют для хранения файлов и совместной работы над ними средства, которые не всегда защищены достаточно надежно.

Цель данной книги – показать различные способы получения доступа к конфиденциальным данным, а также способы их защиты – по принципу «действие-противодействие». Вы узнаете, как злоумышленник может получить доступ к вашим данным, следовательно, вы узнаете, как можно защититься.

Раньше обработка информации была сложнее – гораздо больше ручной работы, горы бумаги. Все неэффективно и сложно. С другой стороны, так данные были более защищены, чем сейчас. Представьте: чтобы похитить конфиденциальную информацию, например, государственную или коммерческую тайну, нужно было проникнуть внутрь часто охраняемого объекта, или же «перехватить» эту информацию по пути следования на другой объект. Все это сложно.

Сегодня обработка данных производится на компьютере. Постепенно, благодаря развитию электронно-цифровой подписи, происходит отказ от бумаги. Но при этом гораздо проще отправить жертве троян, и все ее данные будут как на ладони.

Но неужели нет эффективных средств защиты данных? Есть, и они будут рассмотрены в этой книге.

Аудитория

Книга рассчитана на начинающих пользователей и пользователей средней квалификации, желающих защитить свои данные. В книге не будет двух вещей: самых основ (поэтому она не подойдет для самых начинающих пользователей, ну не хочется мне объяснять, что такое файл, раздел и т.д.) и скучной теории – вместо нее будет занимательная практика. Конечно, кое-какие теоретические сведения, например, введение в асимметричную криптографию, все же будут приведены – без этого никак. Но в целом буду стараться писать так, чтобы материал книги был понятен даже самым начинающим пользователям – без лишних технических подробностей.

В основном материал книги будет ориентирован на пользователей операционных систем Windows и Android (думаю, большая часть пользователей в мире использует именно эту связку), однако будет кое-что интересное и для пользователей Linux. Тем более, что программы шифрования данных зачастую доступны не только для Windows, но и для Linux.

Большая часть рассматриваемых в книге программ бесплатна. Приводятся и некоторые платные программы – чтобы вы могли сравнить и выбрать лучшую для своих нужд. Но знайте, что всегда есть бесплатный аналог, функционал которого ничуть не хуже, чем у коммерческого «сородича». Преимущество бесплатных программ еще в том, что они зачастую являются программами с открытым исходным кодом (Open Source), а это значит, что в них точно нет «закладок», «дыр», «черных ходов» и прочих штучек, позволяющих спецслужбам получить доступ к вашим данным. Все элементарно просто: когда код доступен всем, рано или поздно кто-то найдет в нем изъян.

Как читать эту книгу?

Книга – не учебник. Ее не нужно читать от корки до корки. Если вам интересно в данный момент, как защитить данные на своем мобильном телефоне, вы можете начать читать сразу с третьей части, с любой ее главы. Если вам что-то будет непонятно, и «пробел в знаниях» был заполнен в предыдущих главах, вы обязательно найдете перекрестные ссылки.

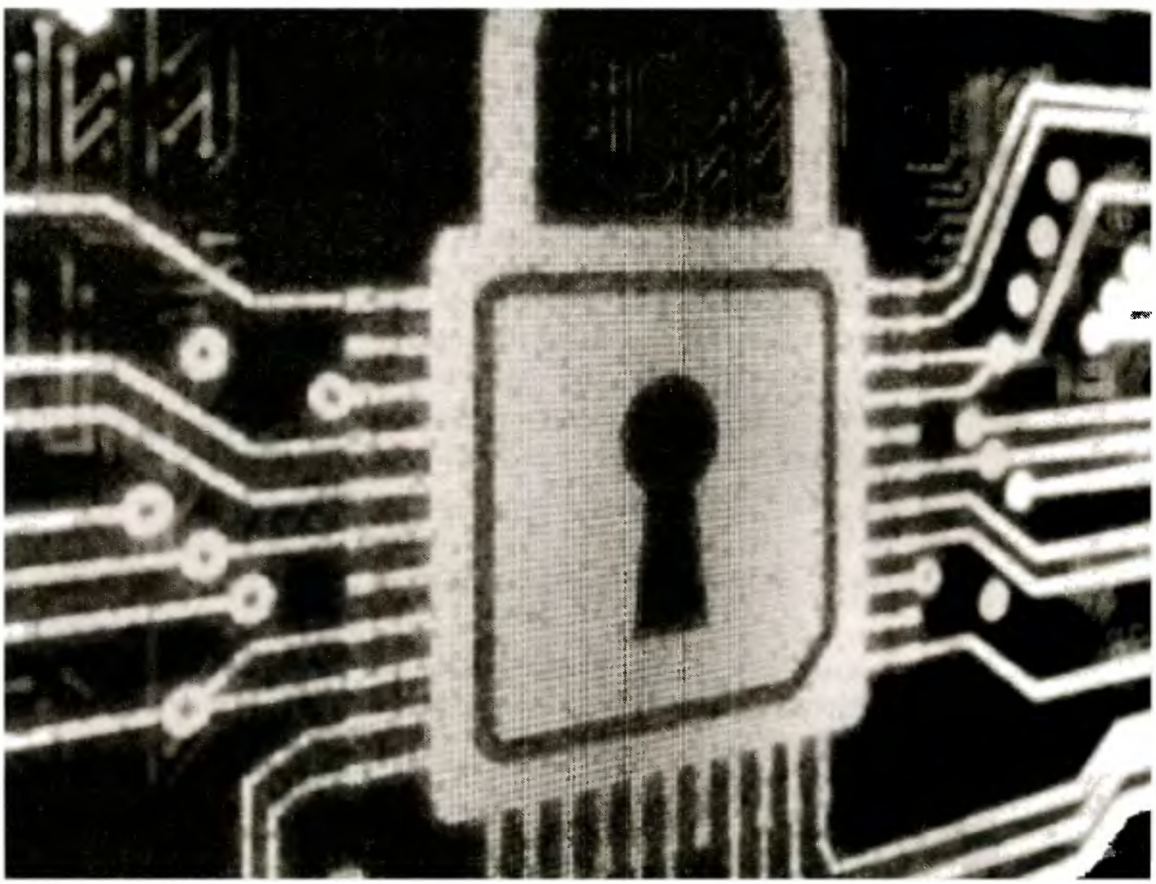
Во время чтения книги обращайте внимание на примечания, которые для большего удобства были разделены на следующие группы:

- **Примечание**. Обычные примечания, несущие дополнительную информацию.
- **Важно**. Какие-то важные сведения, с которыми обязательно нужно ознакомиться.
- **Внимание.** Если вы не прочитаете такое примечание, велика вероятность потерять данные или сделать что-то непоправимое. Попробуем прямо сейчас.

> **Внимание!** В данной книге будет рассматриваться шифрование ваших данных. Учиться лучше на данных, которые вы не боитесь потерять. Если таких данных у вас нет и все данные важные, перед шифрованием или еще каким-либо видоизменением данных обязательно делайте резервную копию! Пока вы учитесь, велика вероятность что-

то сделать неправильно. Все рассматриваемые в книге программы стабильны и не экспериментальны, однако есть большая вероятность допустить ошибку по незнанию. Поэтому лучше сделать резервную копию – ее всегда можно удалить, если данные были зашифрованы (и расшифрованы, что не менее важно) успешно.

Часть 1. Защита электронной почты



Часть 1. Защита электронной почты

Впервые электронная почта появилась в 1965 году и до сих пор остается одним из основных методов обмена информации. Поэтому данную книгу целесообразно начать именно с защиты электронной почты.

Глава 1. Средства и методы защиты электронной почты

1.1. Методы криптографии. Симметричная и асимметричная криптография

В современном мире существуют две основные криптосистемы – *симметричные* и *асимметричные*, или криптосистемы с открытым ключом. В первых для шифрования и дешифрования информации используется один и тот же ключ. Другими словами: чтобы получатель смог расшифровать зашифрованный текст, он должен знать ключ, которым его зашифровали. Такая система шифрования может использоваться при полном доверии между всеми ее участниками. К тому же при росте количества участников придется увеличивать и количество ключей. Например, вы переписываетесь с Марком, Владимиром и Ольгой. Можно, конечно, шифровать все сообщения одним паролем, который будут знать все три адресата. Но это не есть правильно. Правильнее создать отдельные ключи (пароли) для каждого из адресатов. Когда их трое, особых проблем это не составит. Но когда вам нужно обмениваться электронной почтой с сотнями адресатов, как запомнить все ключи? Следовательно, такая система шифрования удобна при обмене электронной почтой с небольшой группой адресатов.

Криптосистема с открытым ключом гораздо совершеннее. В такой системе используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация (в нашем случае текст сообщения) шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения. *В этом случае вы можете раздать всем желающим ваш открытый ключ, например, опубликовать его на своем сайте, чтобы каждый мог написать вам зашифрованное сообщение, расшифровать которое вы сможете только с помощью закрытого ключа, который вы должны хранить в тайне.*

> **Внимание!** Запомните, что публичный ключ используется для шифрования информации, адресованной вам, а для ее расшифровки используется приватный ключ. Если приватный ключ утерян, расшифровать информацию будет невозможно, поэтому регулярно нужно делать резервное копирование ваших ключей.

Существует и еще один метод защиты электронной почты – электронная подпись. Правда, она позволяет только проверить авторство и подлинность сообщения, но не зашифровать сам текст, поэтому в данном обзоре средства для работы с ЭЦП рассматриваться не будут. Если вам интересно, то об электронной подписи мы поговорим в главе 4.

1.2. Алгоритмы шифрования

Существуют различные алгоритмы шифрования, но в этой главе мы поговорим об основных алгоритмах, которые применялись и применяются именно при шифровании электронной почты.

Одним из первых алгоритмов шифрования, получивших распространение в современном мире, является DES (Data Encryption Standard). Он разработан в 1977 году, но, тем не менее, дожил до наших дней и все еще используется в некоторых криптосистемах. Алгоритм DES представляет собой блочный алгоритм шифрования с симметричным ключом. Размер ключа равен 64 битам, но только 56 из них используются для шифрования, а остальные 8 – для контроля четности.

В качестве усовершенствованной версии DES в 1978 году был разработан алгоритм 3DES (Triple-DES). Размер ключа у 3DES составляет 168 бит.

Алгоритм 3DES в три раза медленнее, чем DES, но гораздо надежнее, поскольку время, необходимое для криптоанализа 3DES, гораздо больше, чем время, необходимое для взлома DES. В 1998 году алгоритм DES был взломан всего за три дня. Учитывая возможности современных компьютеров, сегодня на взлом DES понадобится гораздо меньше времени.

Оба алгоритма давно устарели. Хотя 3DES и надежнее, чем обычный DES, для большей надежности рекомендуется использовать другие алгоритмы. Но все же 3DES на сегодняшний день считается самой простой заменой DES.

Следующий алгоритм – это RC5 (Ron's Code 5 или Rivest's Cipher 5). Представляет собой блочный шифр, разработанный в 1994 году Роном Ривестом из компании RSA Security Inc. с переменным количеством раундов, длиной блока и длиной ключа. Максимальный размер ключа – 2048 бит, размер ключа по умолчанию – 128 бит.

Алгоритм RC5 является более быстрым и более надежным алгоритмом, особенно при длине ключа более 512 бит, поскольку в настоящее время ключи с длиной 512 бит и меньше считаются как недостаточно устойчивые.

Алгоритм RSA назван по первым буквам фамилий своих создателей Rivest, Shmir, Adleman. Один из первых алгоритмов шифрования с открытым ключом. Алгоритм используется до сих пор. Небезызвестная программа PGP использует именно RSA.

Позволю себе сделать небольшой экскурс в принцип работы RSA. Сначала выбираются большие простые числа – M и N. Затем вычисляется их произведение Q = M x N. После этого выбирается такое число D, которое должно быть взаимно простым с результатом умножения (M-1)x(N-1). Другими словами, оно не должно иметь с результатом умножения общих делителей, отличных от единицы. После этого вычисляется число A из выражения (AxD)mod[(M-1)x(N-1)] = 1.

Публичным ключом считается пара чисел (A,Q), а *приватным (закрытым) ключом* является пара чисел (D,Q). Открытым ключом можно закодировать передаваемый текст, а для его раскодирования нужен закрытый ключ.

Для кодирования числа S используется формула C = M^A mod Q. Для раскодирования используется обратная операция S = C^D mod Q.

Чтобы взломать RSA (другими словами, чтобы взломать PGP и другие программы, которые используют RSA), нужно разложить число Q (его можно получить из открытого ключа, который будет опубликован пользователем в Интернете) на простые множители. Вот только незадача: над этим бились известные математики многие годы и ничего, увы, у них не получилось. В

математике нет теорем, которые могут предсказать, будет ли определенное число простым. Есть теоремы, которые могут определить, является ли число составным, но если число не является составным, это не означает, что оно является простым. Такое число якобы является простым, но чтобы убедиться в этом, нужно применять более сильные теоремы, реализации которых на машине сводятся к банальному перебору, на что уходит много времени.

Если взять число, например, из четырехсот десятичных знаков, то для его разложения на простые множители понадобится столько времени, что расшифрованная информация уже давно потеряет актуальность.

Конечно, есть некоторые алгоритмы, позволяющие более эффективно разложить число на простые множители, но они эффективны только в частных случаях, когда сомножители лежать близко к корню.

Казалось бы, взломать RSA невозможно. Но возможности компьютеров постоянно растут, и то, что казалось невозможным в 1977 году, становится реальностью в наше время. Будет ли взломан ваш ключ, зависит от его длины. Тут простое правило: чем больше, тем лучше. Еще относительно недавно ключи с длиной 512 бит считались довольно надежными, и даже некоторые авторитетные издания писали[1], что длины ключа в 256 бит хватит навсегда (и было это совсем недавно – всего четыре года назад, а именно в 2012 году). Однако авторы той статьи, очевидно, не знали, что группе инженеров из Японии, Швейцарии, Нидерландов и США удалось успешно вычислить данные, зашифрованные при помощи криптографического ключа стандарта RSA длиной 768 бит. То есть ключ длиной в 768 бит был успешно взломан[2] еще в 2010 году. А чуть позже был взломан и ключ длиной в 1024 бита. В связи с этим Microsoft побыстрее увеличила длину ключа до 2048 бит в Windows Server[3].

Другими словами, при использовании RSA минимальная длина ключа должна быть 2048 бит, а еще лучше – 4096 бит, если есть желание получить запас надежности на ближайшие 5-10 лет.

Нужно рассмотреть еще один алгоритм, достаточно популярный в наше время, – AES (Advanced Encryption Standard). Это симметричный алгоритм с размером ключа 128, 192 и 256 бит. Принят в качестве стандарта шифрования правительством США. Все бы хорошо, но асимметричные алгоритмы с большой длиной ключа будут все-таки надежнее. Однако могут встречаться и комбинированные варианты шифрования: сначала сообщение кодируется с помощью некоторого ключа симметричного алгоритма, например, 3DES или AES, а потом ключ шифруется алгоритмом RSA и передается вместе с

1 https://xakep.ru/2012/12/28/59888/
2 http://www.cybersecurity.ru/crypto/85133.html
3 https://support.microsoft.com/en-us/kb/2627272

закодированным сообщением. Это позволяет достичь высокой скорости обработки информации и обеспечивает дополнительную защиту.

Алгоритм AES в чистом виде используется для шифрования данных на жестком диске, то есть когда данные не должны выходить за пределы информационной системы. Когда же данные выходят за пределы информационной системы и адресуются определенному лицу, лучше использовать асимметричное шифрование.

1.3. Средства защиты электронной почты

В этом разделе будут рассмотрены различные средства защиты электронной почты и приведены преимущества и недостатки каждого из них.

1.3.1. PGP

Начнем с классики жанра. Думаю, все знакомы с PGP – даже если кто ее не использовал, тот знает о ее существовании. Если кто-то знаком с PGP, тогда рекомендую отличную статью «Введение в шифрование с открытым ключом и PGP»[4]. В ней как описаны основы криптографии с открытым ключом, так и рассказано, что такое PGP.

Лучше остановимся на преимуществах и недостатках PGP, а если быть предельно точным, программы PGP Desktop от Symantec. Если отбросить все остальные возможности программы PGP Desktop, а остановиться только на защите электронной почты, то преимуществ (на фоне других решений) будет не так уж и много – наличие сервера ключей keyserver.pgp.com, который пользователи могут использовать для обмена ключами. Больше нет необходимости публиковать свои открытые ключи на сайте или передавать их лично каждому адресату.

Особенность программы – это ее метод защиты электронной почты, а именно перехват на уровне драйвера трафика почтового клиента. Программа обнаруживает трафик почтового клиента и шифрует отправляемые сообщения и автоматически расшифровывает входящие сообщения. Казалось бы, такой метод защиты очень удобен. Ведь не нужно отдельно настраивать почтовый клиент, да и метод перехвата работает с любым почтовым клиентом. Вам не нужно знать особенности настройки каждого клиента, если вам захочется, например, перейти с Outlook на The Bat!

4 https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

Настраивать сами клиенты при этом не нужно, но нужно настроить программу PGP Desktop для каждого почтового ящика, который вы используете, – нужно задать e-mail, адреса SMTP/POP/IMAP-серверов (рис. 1.1) и т.д. Понятное дело, также нужно настроить и ключи шифрования. Все это не очень просто для начинающего пользователя. Настройка программы будет описана в главе 3, пока лишь вам нужно знать, что это не самый простой способ защиты электронной почты, да и не самый надежный, как будет показано далее.

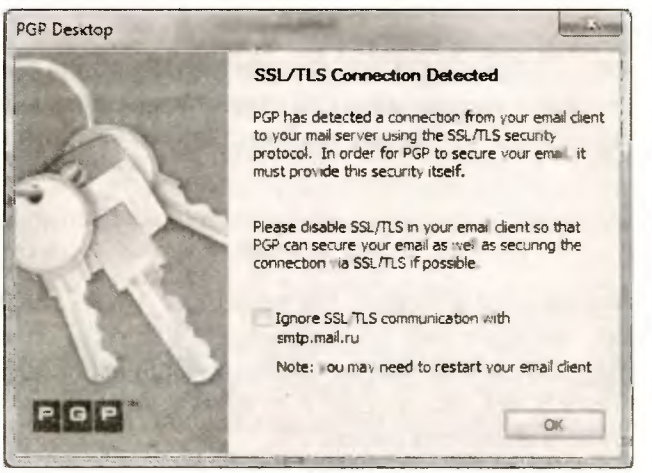


Рис. 1.1. Настройка программы PGP Desktop

Но ведь отсюда вытекает и главный недостаток программы – уже расшифрованные письма остаются незащищенными на клиенте. То есть, запустив почтовый клиент, который ничем не защищен, можно прочитать переписку. Если злоумышленник перехватит трафик, то прочитать ваши сообщения он не сможет, а вот если он завладеет вашим жестким диском, то все будет открыто, как на ладони. Понятно, что программа поддерживает также и создание виртуальных контейнеров, и шифрование физических дисков. Можно хранить базу сообщений почтового клиента в виртуальном контейнере или на зашифрованном диске, тогда у злоумышленника ничего не получится. Но речь сейчас сугубо о защите электронной почты без всяких вспомогательных средств.

Есть и еще один, не менее существенный недостаток. Если приложение PGP Desktop не было запущено, а потовый клиент уже получил сообщения, то они останутся нерасшифрованными. И повторно их расшифровать... непонятно как... Конечно, в Symantec не могли этого не предусмотреть и разработали специальный плагин для почтового клиента Outlook, который

называется Outlook Addin. Вот только есть два момента: о «глюках» данного плагина не говорил разве что ленивый[5], и что делать тем пользователям, у которых вместо Outlook, скажем, Thunderbird?

1.3.2. Стандарт S/MIME

Стандарт S/MIME (Secure/Multipurpose Internet Mail Extensions) – это стандарт для шифрования и подписи в электронной почте с помощью открытого ключа. Принцип защиты электронной почты следующий. Пользователь генерирует ключевую пару (открытый/закрытый ключ), настраивает свой почтовый клиент и предоставляет открытый ключ всем желающим. Они шифруют его открытым ключом письма, которые можно расшифровать только закрытым ключом. Другими словами, посредством S/MIME можно реализовать классическую схему асимметричного шифрования со всеми ее преимуществами и недостатками.

К преимуществам данного метода можно отнести следующие:

- S/MIME поддерживает большинство почтовых клиентов, в том числе и мобильные клиенты (например, MailDroid).
- Сообщения в почтовом клиенте зашифрованы, пока вы их не расшифруете. Для расшифровки нужно ввести пароль, который указывается при создании ключевой пары.
- Нет проблем с расшифровкой сообщений, как при использовании PGP Desktop. Поскольку расшифровка происходит средствами почтового клиента, а не сторонней программы, то расшифровать письмо можно в любой удобный момент.

Конечно, есть и недостатки:

- Главная проблема S/MIME – какой программой сгенерировать сертификат?
- Каждому адресату нужно предоставить свой открытый ключ. Конечно, это можно немного сгладить при использовании сервера ключей, об этом мы поговорим чуть позже.
- Сложность настройки. S/MIME требует отдельной настройки для каждого почтового клиента. Например, если у вас в офисе используется Outlook, дома The Bat!, а на мобильном телефоне – MailDroid, то вы должны знать, как настроить все эти клиенты. А это требует квалификации пользователя выше среднего.

5 http://www.symantec.com/connect/forums/pgp-outlook-plugin-issue

- Сложности при смене ключа, особенно если пользователи плохо понимают, что они делают.

Впрочем, не все недостатки являются такими уж и недостатками. Если использовать специальные программы для создания и управления сертификатами пользователя, то первые два недостатка неактуальны – вы сможете создать и опубликовать свой ключ на сервере ключей. Также программа позволяет выполнять поиск ключей, опубликованных другими пользователями. О создании ключей (сертификатов) мы поговорим в главе 3, а пока знайте, что создать ключ, опубликовать его публичную часть на сервере – не проблема.

По сути, единственный ощутимый недостаток S/MIME – это необходимость настройки каждого почтового клиента вручную. На предприятии можно настроить адресную книгу Outlook, и все будет гораздо проще (при условии, что используется Outlook). Если же вы – конечный пользователь и используете шифрование для личных целей, вам придется настраивать сертификаты в каждом почтовом клиенте, который вы используете. О настройке почтовых клиентов мы поговорим в главе 3, в ней же будет показано, как упростить данную процедуру.

1.3.3. Безопасные почтовые сервисы. HushMail

Ранее считалось, что достаточно «завести» почтовый ящик на защищенном почтовом сервисе вроде GMail.com, и таких мер безопасности будет вполне достаточно для сохранности электронной почты. Однако в 2013 году компания Google заявила, что больше не гарантирует безопасность данных[6]. Такое заявление повергло многих пользователей этого сервиса в шок и заставило искать либо средства шифрования, либо сразу защищенные сервисы. Преимущество последних очевидно – ничего не нужно настраивать. Просто заводите себе «безопасный» почтовый ящик и используете его как обычно.

Один из таких сервисов – HushMail. На их сайте все очень красиво расписано, в чем вы можете убедиться в этом самостоятельно:

```
https://www.hushmail.com/about/technology/security/
```

Даже приведена матрица угроз, позволяющая определить, от каких угроз может защитить HushMail, а от каких – нет. На сайте сказано, что сервис поможет от перехвата вашего интернет-соединения, от утечки данных, от

6 http://mashable.com/2013/08/14/google-email-privacy-out-of-context/#CGvuqjGWmkqt

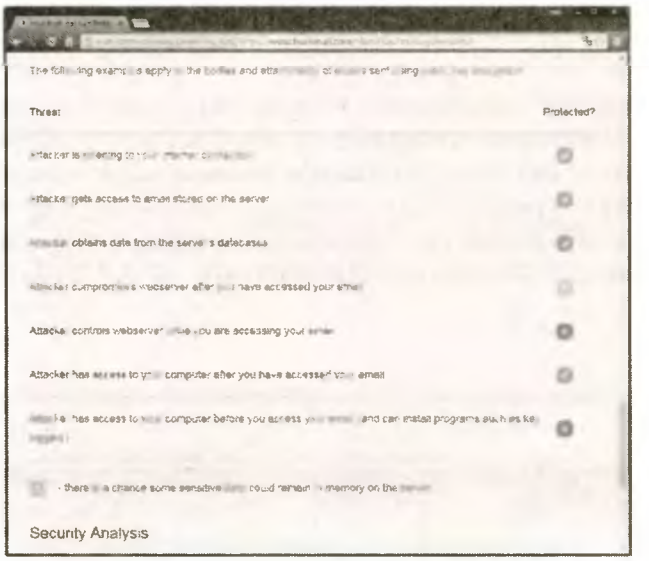


Рис. 1.2. Матрица угроз HushMail

неавторизированного анализа контента, а также от правительственных программ наблюдения.

Особенно хочется остановиться на последней возможности. Однако всем известно, что ранее компания HushMail передала полиции[7] расшифрованные сообщения некоторых своих пользователей – при судебном разбирательстве дела о контрабанде наркотиков. Суть даже не в факте передачи данных (понятное дело, никому не хочется укрывать преступников), а в факте расшифровки данных.

Когда-то HushMail был знаменит тем, что он был единственным криптографическим сервисом, где все криптографические операции выполнялись на клиентской стороне в специальном Java-апплете. В этом же апплете генерировались ключевые пары, а на сервере хранились лишь зашифрованные пользователями сообщения, что исключало доступ к закрытым ключам пользователя. Данный апплет даже проверялся на наличие закладок. Их не обнаружили. Но факт передачи расшифрованных сообщений был, и с этим не поспоришь.

Далее HushMail превратился в обычную почтовую службу с поддержкой SSL, хотя и с поддержкой OpenPGP, однако все криптографические операции при этом выполняются на сервере. Именно поэтому мы не рекомендуем

7 http://www.pcauthority.com.au/News/97414,hushmail-turns-out-to-be-anything-but.aspx

использовать подобные сервисы – никогда не знаешь, что происходит «на той стороне».

К слову, у HushMail два варианта интерфейса – новый и «оригинальный» (исходный). Последний изображен на рис. 1.3. Именно в этой версии интерфейса есть пункт меню Hushtools, вызывающий одноименное окно, предоставляющее средство управления ключами. В «новой» версии интерфейса вообще непонятно, как управлять ключами и шифрованием. В ней HushMail похож на обычную почтовую службу вроде Gmail.com.



Рис. 1.3. Исходный интерфейс HushMail

Еще у HushMail есть один существенный недостаток. Если вы пользуетесь бесплатным аккаунтом и не заходили в него последние три недели (например, просто уехали в отпуск, где нет доступа к Интернету), то его заблокируют, а для разблокировки предложат осуществить апгрейд до премиум-аккаунта за почти 50 долларов (рис. 1.4). Как по мне, это очень дорого, особенно учитывая посредственность такой защиты и наличие бесплатных решений (которые также будут рассмотрены в этой книге).

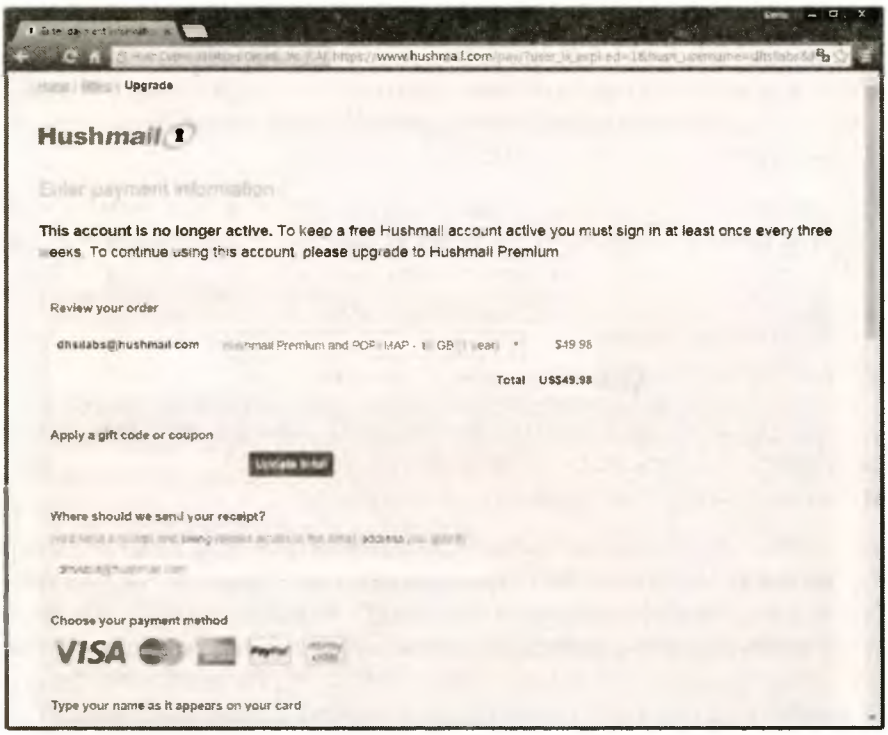


Рис. 1.4. Мой аккаунт заблокировали

1.3.4. Плагины браузера

Плагин браузера PGP Mail

Позволяет использовать асимметричное шифрование (то есть шифрование с открытым/закрытым ключами) на стороне клиента. О возможностях данного плагина можно прочитать на официальном сайте[8]. Нужно упомянуть лишь четыре его особенности:

- Поддерживаемые браузеры: Firefox, Chrome, Opera, Safari
- Рекомендуется использовать Firefox, поскольку функции шифрования в Firefox работают быстрее, чем в Chrome или Opera
- Рекомендуется использовать TOR[9]
- Шифрование осуществляется на стороне клиента

8 https://pgpmail.cc/
9 https://www.torproject.org/

То, что шифрование производится на стороне клиента, – это единственное преимущество данного плагина. А вот рекомендация использования TOR может усложнить знакомство с этим плагином для неопытных пользователей. А ведь для таких пользователей данный плагин и создается, поскольку все более опытные используют PGP или S/MIME.

Да и зависимость от браузера – тоже не есть хорошо. А что, если пользователь использует IE? А ведь этот браузер, несмотря на популярность Chrome и Firefox, довольно популярен только потому, что он «придворный» браузер Microsoft.

Плагин браузера SecureGmail

В отличие от PGP Mail, плагин SecureGmail[10] предлагает симметричное шифрование, то есть каждое секретное сообщение шифруется паролем, который должен знать и отправитель, и получатель.

Такая система шифрования может использоваться при полном доверии между всеми ее участниками. К тому же при росте количества участников придется увеличивать и количество ключей. Можно, конечно, шифровать все сообщения одним паролем, который будут знать все ваши адресаты. Но это не есть правильно. Правильнее создать отдельные ключи (пароли) для каждого из адресатов. Когда их трое, особых проблем это не составит. Но когда вам нужно обмениваться электронной почтой с сотнями адресатов, как запомнить все ключи? Следовательно, такая система шифрования удобна при обмене электронной почтой с небольшой группой адресатов.

10 https://www.streak.com/securegmail

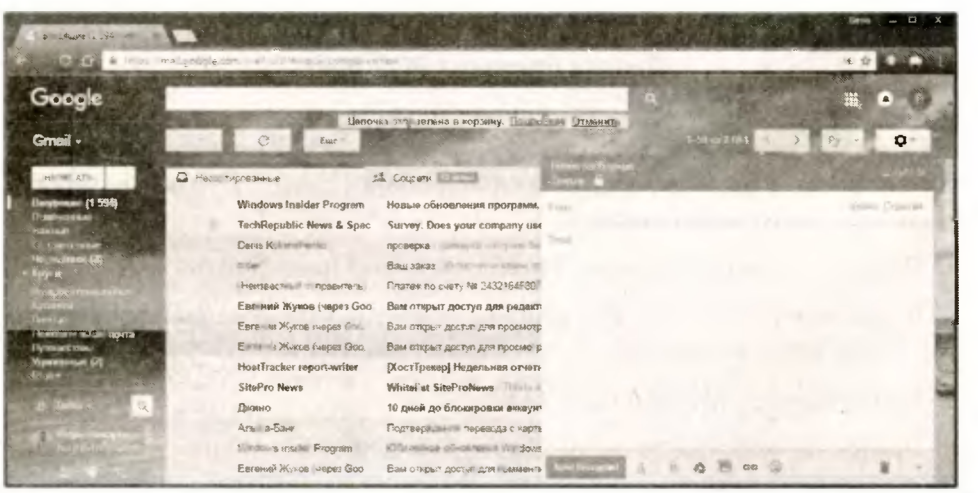


Рис. 1.5. Плагин SecureGmail

Плагин SecureGmail работает в паре с браузером Chrome, остальные браузеры он не поддерживает.

Плагин браузера Encrypted Communication

Плагин Encrypted Communication[11] по своему функционалу похож на SecureGmail, однако работает только в браузере Firefox, остальные браузеры не поддерживаются.

О недостатках симметричной системы шифрования мы уже говорили, поэтому не будем повторяться. Если вы переписываетесь секретной информацией с одним-двумя пользователями, такие плагины еще оправдывают свое существование. В противном случае лучше использовать асимметричную систему.

11 https://addons.mozilla.org/en-US/firefox/addon/encrypted-communication/



Рис. 1.6. Плагин Encrypted Communication

Преимущество подобных плагинов – простота использования. Не нужно разбираться с асимметричным шифрованием (ведь концепция открытого/закрытого ключа может показаться сложной новичкам), не нужно морочить голову с ключами, их резервным копированием. Просто нужно помнить пароль и желательно сообщить его своим друзьям так, чтобы злоумышленник не мог перехватить его.

1.3.5. Плагины почтовых клиентов

Плагин почтового клиента Enigmail

Аналогично браузерам, для почтовых клиентов также существуют плагины шифрования. Один из них – Enigmail[12]. Он представляет собой OpenPGP-плагин для Thunderbird и Postbox.

Особых преимуществ у этого решения нет, поскольку все равно приходится устанавливать и настраивать дополнительное программное обеспечение – программу GnuPG. Когда все настроено, можно сказать, что плагин удобен в использовании.

Недостаток – все равно нужно вникать в асимметричную систему шифрования и разбираться, что есть открытый и закрытый ключ и для чего используется каждый из них. Впрочем, это недостаток всех способов, использующих асимметричную криптографию. Здесь или безопасность и знание, или же незнание и симметричная криптография.

Плагин почтового клиента CyberSafe Mail

Еще один плагин для почтового клиента[13]. Сразу к недостаткам этого плагина: он платный и поддерживает только Outlook, да и то не всех версий. Была бы поддержка The Bat! и Mozilla Thunderbird, тогда бы он полностью оправдывал свою стоимость. Конечно, если вы используете Outlook, вам все равно, поддерживает ли этот плагин другие почтовые клиенты или нет, главное, чтобы вас устраивал его функционал.

А вот преимуществ у этого плагина гораздо больше: в отличие от Enigmail, пользователю не нужно устанавливать дополнительное программное обеспечение. Также он использует асимметричную систему шифрования, создание сертификатов и управление ими происходит в самом плагине.

1.4. Сравнение средств защиты. Выбор идеального средства

1.4.1. Проблема выбора

Практичный человек решает проблему выбора отсутствием самого выбора. Гораздо проще было бы выбирать, если был бы только один почтовый клиент, например, Outlook, и один-два плагина шифрования для него, допустим, один платный с более удобным функционалом, а второй – бесплат-

12 http://www.enigmail.net/home/index.PGP

13 http://cybersafesoft.com/products/mail-encryption/

ный с ограниченным функционалом. Тогда бы проблема выбора отпала бы сама собой. Есть средства и необходимость – используй платную версию, необходимости нет (или нет денег) – бесплатную.

Но в реальном мире все гораздо сложнее. Существует множество различных средств защиты электронной почты, часть из которых была рассмотрена в этой главе. Теперь давайте попытаемся подытожить и сравнить рассмотренные ранее средства.

Вскоре мы рассмотрим матрицу угроз (табл. 1.2), но сначала предлагаем вам ознакомиться с общей таблицей преимуществ и недостатков каждого средства защиты электронной почты (таблица 1.1).

Таблица 1.1. Сравнительная таблица средств защиты почты

№	Средство	Преимущества	Недостатки
1	PGP Desktop	Наличие сервера ключей Простота настройки почтовых клиентов	Расшифрованные письма ничем не защищены на клиенте Если программа не запущена, а зашифрованное сообщение получено, непонятно, как его расшифровать Программа платная и стоит недешево
2	S/MIME	S/MIME поддерживают большинство почтовых клиентов, в том числе и мобильные Сообщения на клиенте хранятся в зашифрованном виде Расшифровка осуществляется средствами почтового клиента, а не стороннего ПО Можно бесплатно реализовать надежную защиту	Необходим сервер ключей для комфортной работы Сложность настройки Необходимо каждый почтовый клиент настраивать отдельно

3	Hushmail	Простота использования	Возможность расшифровки сообщений нечестной администрацией сервиса или по решению суда Шифрование производится на стороне сервера, а не клиента
4	PGP Mail	Шифрование/расшифровка на стороне клиента	Поддерживаются не все браузеры Для большей безопасности нужно использовать TOR, что может вызвать затруднения у неопытных пользователей
5	SecureGmail	Простота использования	Только для Chrome Ключ известен как отправителю, так и получателю сообщения
6	Encrypted Communication	Простота использования	Только для Firefox Ключ известен как отправителю, так и получателю сообщения
7	Плагин Enigmail	Удобен в использовании	Требует GnuPG Поддерживает только Thunderbird и Postbox
8	Плагин CyberSafe Mail	Удобен в использовании	Платный Поддерживает только Outlook

При построении таблицы 1.2 использовалась матрица угроз проекта HushMail, она была несколько дополнена, и теперь мы можем использовать ее для сравнения описанных в таблице средств защиты электронной почты. Значение «Да» означает, что вы защищены от угрозы. Значение «Да/Нет» означает, что есть какие-либо ограничения, о которых мы расскажем. Последнего плагина в таблицах 1.2 и 1.3 нет, но его результаты такие же, как у Enigmail, поскольку принцип их работы схож.

Таблица 1.2. Сравнение средств защиты электронной почты в разрезе матрицы угроз

Угроза	PGP Desktop	S/MIME	Hushmail	PGP Mail	Secure Gmail	Encrypted Communication	Enigmail
Злоумышленник прослушивает ваше интернет-соединение	Да	Да	Да	Да	Да	Да	Да
Злоумышленник получает доступ к e-mail, хранящемуся на сервере	Да	Да	Да	Да	Да	Да	Да
Злоумышленник компрометирует веб-сервер после того, как вы получили доступ к e-mail	Да	Да	Нет	Да	Да	Да	Да
Злоумышленник контролирует веб-сервер, пока вы смотрите e-mail	Да	Да	Нет	Да	Да	Да	Да
Злоумышленник получает доступ к вашему компьютеру после того, как вы просмотрели ваше e-mail	Нет	Да	Да	Да	Да	Да	Да
Злоумышленник получает доступ к компьютеру до того, как вы просмотрели e-mail, и может установить программы по типу keylogger	Нет	Да/ Нет	Нет	Нет	Нет	Нет	Нет
Злоумышленник получил доступ к вашему жесткому диску	Да/ нет	Да	Да	Да	Да	Да	Да

Рассмотрим данную таблицу на примере средств защиты PGP Desktop и Huhsmail (колонки 1 и 3).

Поскольку шифрование осуществляется на стороне клиента, то программа PGP Desktop защищает вашу переписку от прослушивания интернет-соединения. Что же касается HushMail, приходится полагаться только на SSL. Но такую защиту предлагает и gmail, и если вас в первую очередь интересует именно защита от «прослушки» интернет-соединения, то можно вообще не использовать какие-либо средства защиты. Однако на сайте HushMail указано, что сервис защищает от прослушки, поэтому в таблице указано «Да».

Что будет, если злоумышленник узнает ваш пароль от почтового ящика? Поскольку на сервере письма хранятся в зашифрованном виде, то ничего страшного не произойдет: максимум, что он сможет прочитать, – это спам (куда же без него) и прочую неважную корреспонденцию, которую вы никак не шифровали.

А что будет, если злоумышленник компрометирует или контролирует сам веб-сервер? PGP Desktop, как и любое средство, где шифрование происходит на стороне клиента, защитит вас от этой неприятности. Ведь данные с пользовательского компьютера уже пересылаются в зашифрованном виде. Чего не скажешь о HushMail. Да, от прослушки спасает протокол SSL, а «внутри него» данные передаются в открытом виде. Поэтому веб-сервер обладает полным доступом к данным. Это и есть ответ на вопрос, как администрация HushMail смогла предоставить доступ к переписке при судебном разбирательстве.

При использовании PGP Desktop после расшифровки сообщения хранятся в незашифрованном виде. Поэтому если кто-то получит доступ к вашему компьютеру после прочтения вашего письма или же завладеет вашим жестким диском, то PGP Desktop вам мало чем поможет. Конечно, если PGP Desktop не была запущена на момент поступления сообщения, следовательно, его не было кому расшифровать, тогда, может быть, информация все еще останется в тайне. Поэтому напротив PGP Desktop в таблице 2 стоит значение Да/Нет для последней угрозы. Что же касается HushMail, то вам не нужно беспокоиться об этих угрозах – ведь сообщения находятся на сервере в зашифрованном виде.

Зато оба средства защиты уязвимы при использовании клавиатурного шпиона (keylogger). Если злоумышленник перехватит ваши пароли (в частности, от сертификатов), то вам уже ничто не поможет. Разве что переход на токены вместо ввода паролей. Кстати, нужно сделать важное замечание относительно S/MIME, а именно почему при правильном использовании S/MIME может не помочь даже «кейлоггер». Если ключ добавлен в хранилище как неэкспортируемый, то у злоумышленника ничего не выйдет. Именно поэтому на данный момент S/MIME можно считать самым надежным способом защиты электронной почты.

Все остальные средства защиты используют шифрование на стороне клиента, поэтому им не страшен ни перехват, ни доступ к вашему почтовому ящику – сообщения будут зашифрованы. Единственно, что предоставляет угрозу для этих средств защиты, – это перехват ввода с клавиатуры. Злоумышленник может получить доступ не только к вашим паролям, но и к обычному тексту, который вы вводите в теле сообщения перед тем, как оно будет зашифровано.

Сводная таблица с общими характеристиками средств шифрования электронной почты приведена ниже.

Таблица 1.3. Сводная таблица по средствам шифрования почты

	PGP Desktop	S/MIME	Hushmail	PGP Mail	Secure Gmail	Encrypted Communication	Enigmail
Шифрование на стороне	клиента	клиента	сервера	клиента	клиента	клиента	клиента
Тип шифрования	асим.	асим.	асим.	асим.	сим.	сим.	асим.
Поддержка почтовых клиентов	все Windows-клиенты	все, поддерж. S/MIME	-	-	-	-	Thunderbird Postbox
Поддержка браузеров	-	-	Все поддерж. SSL	Firefox, Chrome, Opera, Safari	Chrome	Firefox	-
Требуется ли доп. ПО	нет	да	нет	нет	нет	нет	да
Открытый код	да (*)	-	Да	нет	да (**)	н/д	да (***)
Сложность настройки	средняя	средняя	слабая	слабая	слабая	слабая	средняя

1.4.2. Выводы

Самый простой способ защиты электронной почты – это использование симметричного шифрования. Для его реализации можно использовать плагины браузера SecureGmail и Encrypted Communication или вообще обойтись без них, а использовать программы, позволяющие создавать архивы, защищенные паролем (например, WinRAR, 7-Zip). Расчет прост: вы защищаете архивом файл, помещаете в него сообщение с возможными вложениями и отправляете другому человеку. Он, зная пароль, открывает архив. Самый простой в реализации, но не очень простой в использовании способ. Создавать архив для каждого нового сообщения вам быстро надоест. Плагины SecureGmail и Encrypted Communication делают симметричное шифрование более удобным, но безопаснее оно от этого не становится.

Более надежна система асимметричного шифрования. Она реализована множеством самых разных способов. Можно использовать стандарт S/MIME (что позволяет использовать асимметричную криптографию даже на мобильных устройствах), можно использовать PGP и производные продукты (OpenPGP, PGP Mail, GnuPG).

В идеале мы как раз и рекомендуем использовать стандарт S/MIME как наиболее надежный и универсальный.

Надежность его заключается в том, что в самом почтовом клиенте сообщения хранятся в зашифрованном виде и расшифровываются только по мере обращения к ним (то есть если кто-то завладеет вашим жестким диском, он не сможет расшифровать ваши сообщения). При расшифровке запрашивается пароль, который знаете только вы (в отличие от симметричного шифрования, где пароль знают как минимум двое).

Универсальность заключается в том, что один раз сгенерировавши свой сертификат, вы можете использовать его в любых почтовых клиентах (разумеется, с поддержкой S/MIME), а также в любых операционных системах, в которых работают эти почтовые клиенты. Например, вы можете сгенерировать сертификат Windows-программой, установить его в Outlook и мобильном почтовом клиенте MailDroid. Никаких ограничений на использование сертификатов нет. Главное при использовании S/MIME выбрать удобную программу для создания самих сертификатов. Желательно, чтобы она позволяла публиковать сертификаты на сервере ключей и управлять ними.

Глава 2.

Как взломать электронную почту



В этой главе будут рассмотрены реальные способы взлома электронной почты. Зная эти способы, вы будете знать, какие способы используют злоумышленники, и как от них защититься.

2.1. Троянский конь

Довольно распространенным способом получения доступа к чужому ящику является рассылка электронных писем со встроенными вирусами. Точнее, вирус встраивается не в само письмо, а письмо лишь содержит ссылку на вирус. Обычно содержание письма должно чем-то «зацепить» пользователя. Оно должно быть таким, на которое пользователь не сможет не отреагировать.

Дальше все просто: пользователь переходит по ссылке, и на его компьютер загружается вредоносный код.

Примеры троянов – DarkComet RAT, SpyEye, Carberp. О DarkComet RAT много что было написано в Сети, Carberp тоже известный троян. А SpyEye – это троян, разработанный Александром Паниным, который даже засветился в сводках ФБР[1].

По роду своей деятельности мне иногда приходится исследовать информационную безопасность того или иного предприятия. В последний раз я использовал модифицированную версию трояна ZeuS. На момент создания созданную модификацию не обнаруживал ни один антивирус (рис. 2.1), к тому же в нем была функция отключения процессов антивирусов, среди которых есть Dr.Web. Однако на компьютере жертвы был установлен Comodo – так даже лучше.

1 https://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty/spyeye-malware-mastermind-pleads-guilty

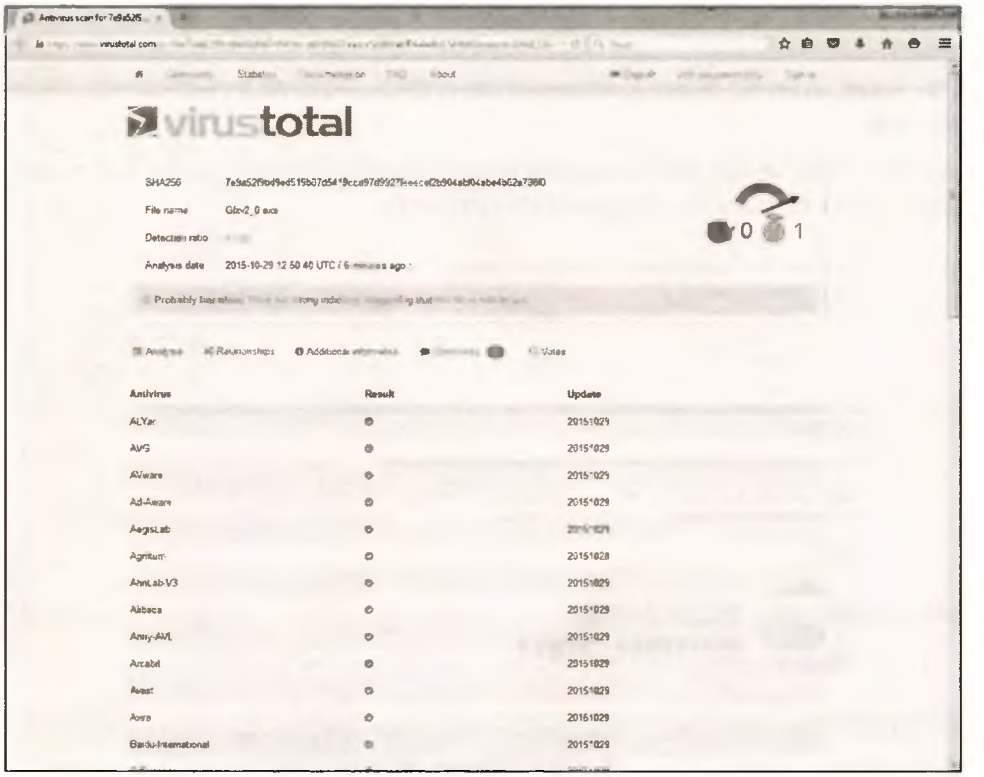


Рис. 2.1. Отчет VirusTotal

В качестве жертвы мы выбрали бухгалтера нашей компании Юлию. Ради чистоты эксперимента она ничего не подозревала о том, что мы собираемся сделать. Думаю, об этом не стоило даже и говорить.

Итак, у нас есть модифицированный ZeuS, но как заставить Юлию запустить его? Если просто отправить ей ссылку, понятное дело, она переходить по ней не будет. Обещать золотые горы в письме – тоже прошлый век, на такое пользователи уже не реагируют.

Когда троян создан, осталось самое малое – написать жертве письмо, в котором нужно мотивировать ее запустить троян. Здесь нужно проявить изобретательность. Конкретных рекомендаций дать не могу, все зависит от жертвы. Например, бухгалтеру можно отправить какое-то обновление бухгалтерской программы, если вы, конечно, знаете, какая программа используется и заказаны ли обновления к ней. Иначе (если обновления не заказаны) такое письмо (даже от имени якобы разработчиков программы) вызовет подозрения.

Чтобы поле From содержало внушительное название, а не xaker134566788@gmail.com, были подделаны заголовки письма. Это делается довольно просто, а как именно, будет показано в способе 5. Пока не будем на это отвлекаться.

В нашем случае мы использовали письмо, изображенное на рис. 2.2. Именно на такое письмо «клюнула» наш бухгалтер.

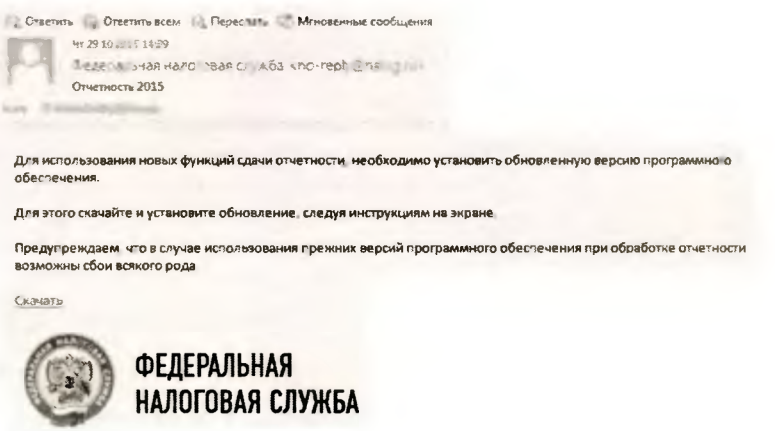


Рис. 2.2. Пример письма

После установки трояна на компьютер жертвы вы сможете полностью контролировать его (рис. 2.3).

Что мы можем? Мы можем ради интереса просмотреть список процессов компьютера, в котором, ясное дело, не будет нашего трояна (рис. 2.4). Мы можем просмотреть файловую систему (рис. 2.5).

Конечно, самое главное, ради чего все это затевалось, – список паролей, сохраненных в браузере (рис. 2.6). Среди этих паролей был сохранен пароль к почте Gmail (см. рис. 2.6) – цель достигнута, мы получили доступ к почтовому ящику!

Приведенный способ – только один из многих подобных. Существуют разные трояны. Некоторые не имеют рассмотренной только что панели управления, а просто сохраняют интересующую вас информацию в текстовый файл и передают по e-mail на ваш почтовый ящик.



Рис. 2.3. Управление компьютером жертвы посредством ZeuS

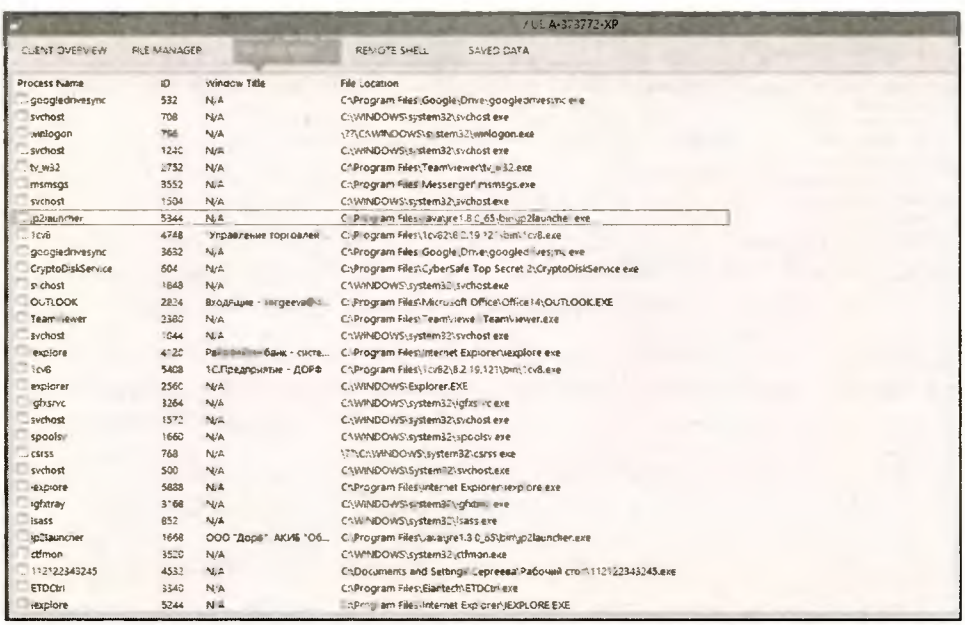


Рис. 2.4. Список процессов на компьютере жертвы (конфиденциальная информация по понятным причинам закрашена)



Рис. 2.5. Файловая система на компьютере жертвы



Рис. 2.6. А вот и пароли!

Примечание. Цель этой книги – защита информации, а не ее взлом или еще какие-либо противоправные действия, именно поэтому создание собственного трояна не рассматривается в книге. Вам нужно знать, что такой способ возможен, и проявлять бдительность каждый раз, когда вы переходите по ссылкам, которые получены даже из проверенных источников!

2.2. Взлом по номеру телефона

Суть этого способа заключается в следующем. Злоумышленнику нужно знать номер телефона жертвы, указанный при регистрации почтового ящика. При сбросе пароля почтовая служба требует ввести последние символы номера телефона (или выбрать номер телефона из списка). На этот номер будет отправлено SMS с кодом подтверждения сброса пароля. Затем злоумышленник отправляет второе SMS с требованием указать код из предыдущего SMS. Пользователь, ничего не подозревая, отправляет код из первой SMS. Самый большой недостаток этого способа в том, что первая SMS придет от Google, а вторая – с неизвестного номера. Успех этого способа зависит от сообразительности жертвы.

Последовательность действий такая:

- Нужно попытаться выполнить вход в аккаунт Google жертвы.
- Поскольку пароль мы не знаем, Google предложит нам его восстановить.
- Далее, если у вашей жертвы был привязан к аккаунту Android-телефон, то Google предложит отправить оповещение на мобильный. Примечательно, но смартфон не издал ни единого звука, а просто отобразил оповещение. Если он не будет перед глазами у пользователя, есть вероятность, что он его не заметит. Если же пользователь нажмет «Нет», то не отчаивайтесь: повторите данный процесс несколько раз (позже поймете, зачем).
- После отправки оповещения появится страница с инструкциями, внизу будет ссылка на классическую страницу сброса пароля по SMS. Отправьте SMS жертве.
- Жертва получит SMS через несколько секунд. С другого телефона отправьте примерно такое сообщение:

```
Предотвращена попытка входа в аккаунт Google. Перешлите
код подтверждения Google для разблокировки аккаунта.
```



Рис. 2.7. Вот такое сообщение получит жертва

Далее все зависит от смекалки пользователя. С одной стороны, пользователь может обратить внимание на неизвестный номер. С другой стороны, поставьте себя на место среднестатистического пользователя. Сначала он получает уведомление о сбросе пароля, потом SMS с кодом подтверждения, а после – сообщение о том, что замечена подозрительная активность. Конечно, можно все немного усложнить и завести короткий номер, с которого и будет отправлена SMS. Получить короткий номер с названием службы, например, Google Security, не проблема. Это только повысит вероятность успеха.

Получение доступа к почтовому ящику – это еще не все. Чтобы жертва не догадалась, что ее ящик увели, после сброса пароля нужно создать временный пароль и отправить его по SMS, а самим тем временем сделать переадресацию на «хакерский» ящик. Так можно получить контроль над ящиком, не вызвав особых подозрений.

Данный способ придуман не мною, и было бы некрасиво приписывать его авторство себе. Изначально с данным способом я познакомился в блоге

компании Symantec, в котором даже есть видео, демонстрирующее этот способ наглядно:

http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access

Как говорится, лучше один раз увидеть, чем сто раз услышать.

2.3. Физический доступ к компьютеру

Если у вас есть доступ к компьютеру жертвы, то можете считать, что почту вы уже взломали. Вы можете запустить на компьютере или кейлоггер (клавиатурный шпион), или программу для «восстановления» паролей почтовых учетных записей.

Суть кейлоггера в том, что в специальный файл он записывает все, что пользователь вводит с клавиатуры. Вам останется только второй раз подойти к компьютеру, чтобы забрать результирующий файл (или получить его по почте – есть и такие шпионы).

К преимуществам кейлоггера относится то, что он записывает все подряд. Поэтому кроме паролей можно получить еще много интересной информации о своей жертве. Но и недостатков у них очень много. Самый существенный – большинство кейлоггеров успешно определяются антивирусами, и если на компьютере жертвы установлен антивирус, использовать кейлоггер не получится. Ведь не всегда есть возможность отключить антивирус.

Второй недостаток вытекает из его достоинства. В результирующий файл помещается много лишней информации. Мало собрать информацию с клавиатуры, нужно еще отыскать среди всего лишнего то, что нужно, – пароль.

Третий недостаток – если жертва использует почтовый клиент, а не веб-интерфейс, то кейлоггер вообще не поможет. Скорее всего, пароль уже введен в почтовый клиент и запомнен, поэтому жертва не вводит его каждый раз при проверке почты. Следовательно, кейлоггер запишет в файл все, что вводит пользователь, кроме того, что нужно вам.

Есть и еще один недостаток – если выбранный кейлоггер не поддерживает отправку результирующего файла по e-mail, то придется еще один раз подходить к компьютеру. Пример кейлоггера – SniperSpy[2] – на случай, если вы захотите им воспользоваться.

Программы для «восстановления» паролей почтовых учетных записей позволяют сразу получить все интересующие вас пароли без необходи-

2 http://www.sniperspy.com/

мости чтения мегабайтов текста в поиске нужного вам пароля. К тому же на них никак не реагирует антивирус. Одна из таких программ – это Mail PassView[3]. Она позволяет восстановить пароли следующих почтовых учетных записей:

- Outlook Express
- Microsoft Outlook 2000 (POP3 and SMTP Accounts only)
- Microsoft Outlook 2002/2003/2007/2010/2013/2016 (POP3, IMAP, HTTP and SMTP Accounts)
- Windows Mail
- IncrediMail
- Eudora
- Netscape 6.x/7.x
- Mozilla Thunderbird
- Group Mail Free
- Yahoo! Mail – если пароль сохранен в приложении Yahoo! Messenger
- Hotmail/MSN mail – если пароль сохранен в приложении MSN Messenger
- Gmail – если пароль сохранен в приложениях Gmail Notifier, Google Desktop или Google Talk

3 http://www.nirsoft.net/utils/mailpv.html

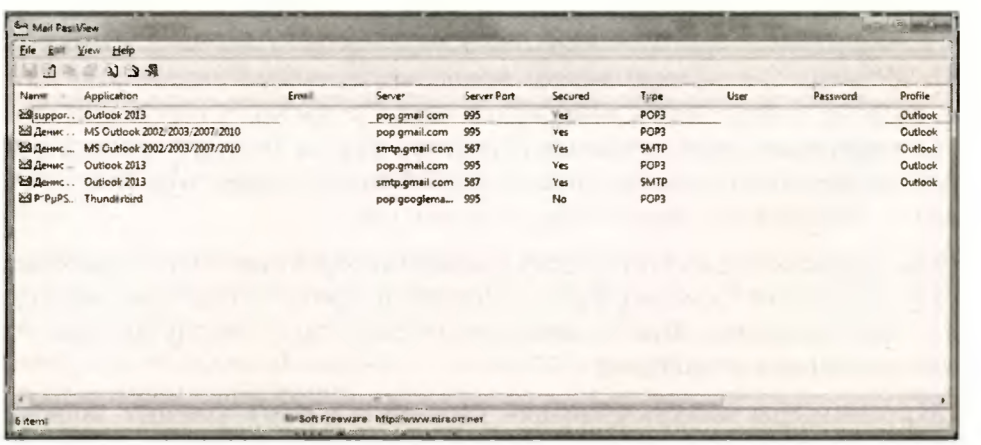


Рис. 2.8. Программа Mail PassView

Результат работы программы изображен на рис. 2.8. Пароли, как и адреса e-mail, затерты по понятным причинам.

Mail PassView – не единственная программа в своем роде. Существуют и другие программы:

- Outlook Password Decryptor (http://securityxploded.com/outlookpassworddecryptor.php) – позволяет восстановить пароли из Outlook, в том числе самых последних версий (Outlook 2016, работающей под управлением Windows 10);
- PstPassword (http://www.nirsoft.net/utils/pst_password.html) – еще одна программа для восстановления паролей, сохраненных в Outlook;
- WebBrowserPassView (http://www.nirsoft.net/utils/web_browser_password.html) – программа для восстановления паролей, хранящихся в браузере. Поддерживаются браузеры IE, Chrome, Opera, Safari, Firefox.

Все, что нужно, – это знать, какой почтовый клиент использует жертва. Найти программу для «восстановления» пароля из этого почтового клиента – не проблема. Если же жертва использует веб-интерфейс для чтения своего почтового ящика, тогда лучше использовать программу WebBrowserPassView. Она поддерживает все версии Windows, начиная с 2000 и заканчивая 10. Старые версии вроде 98/ME не поддерживаются.

Мною была протестирована и эта утилита. Программа успешно восстановила все пароли, хранящиеся в браузерах IE, Firefox, Chrome и Opera (Safari не

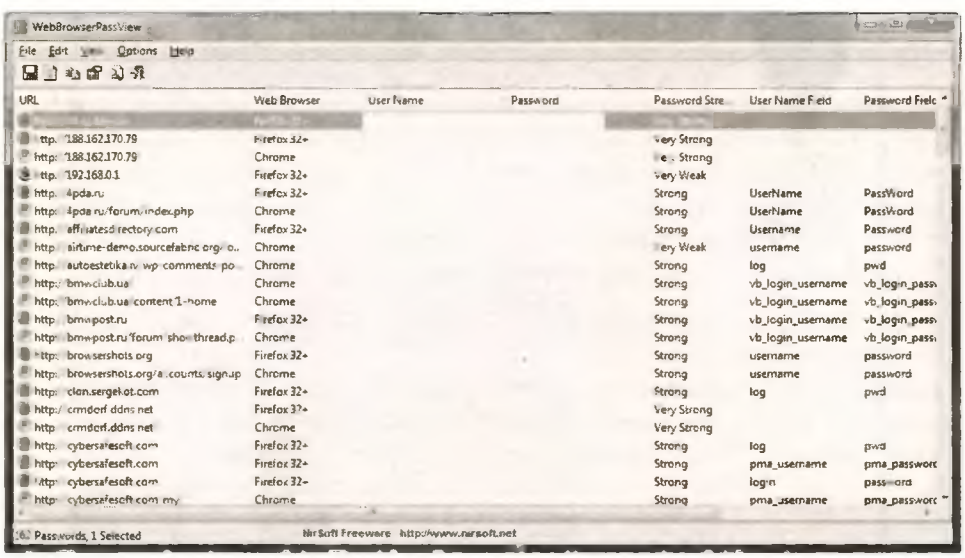


Рис. 2.9. Программа WebBrowserPassView

проверялся, но, думаю, и там будет полный «порядок»), см. рис. 2.9. Даже если вы не найдете среди этого списка пароль от почтового ящика, сей список будет тоже полезен – ведь люди часто используют одни и те же пароли для разных служб.

> **Примечание.** Программу WebBrowserPassView можно использовать и в более мирных целях, например, когда вы забыли свой же пароль, сохраненный в браузере. Собственно, для этого она и разрабатывалась.

2.4. Социальная инженерия или просто обман

Об этом способе не писал только ленивый. Много было уже сказано. Вам кажется, что этот способ не такой эффективный, как о нем говорят? Вы ошибаетесь.

Относительно недавно была взломана почта директора ЦРУ Джона Бреннана. Абсурдность ситуации в том, что почту взломал не «матерый» хакер,

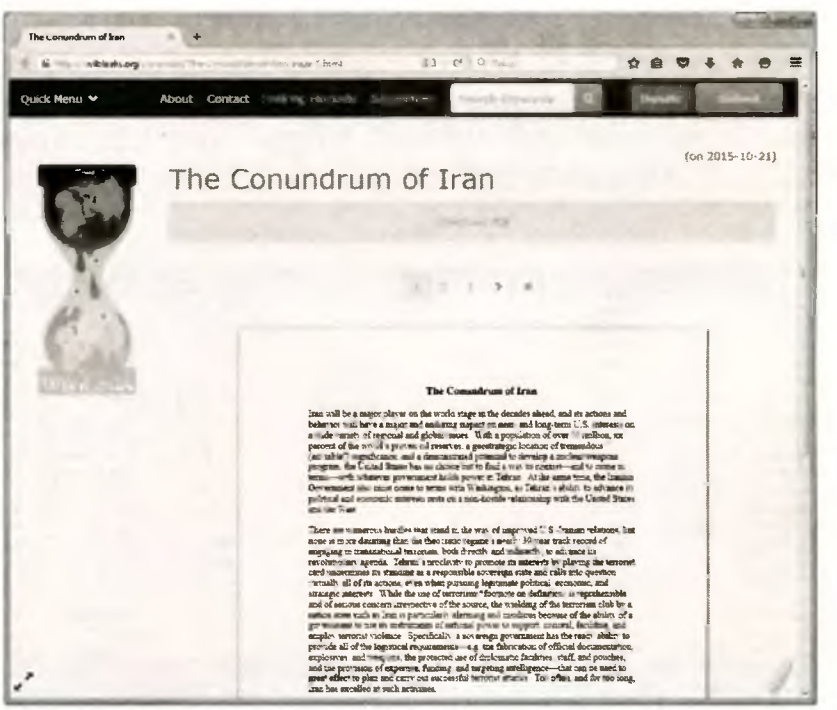


Рис. 2.10. Письма директора ЦРУ, опубликованные Wikileaks

а обычный подросток, правильно собрав информацию о своей «жертве». Подросток сначала связался с сотовым оператором, представившись сотрудником технической поддержки, уточнил детали аккаунта Бреннана.

После этого он позволил в AOL и, представившись Бреннаном, попросил сбросить его пароль. Поскольку он знал всю необходимую информацию (номер почтового аккаунта, последние цифры банковской карты, 4-значный PIN-код, номер телефона), пароль был сброшен, и никто ничего не заподозрил.

Чуть позже Wikileaks опубликовал письма директора ЦРУ[4], см. рис. 2.10.

Преимущество этого способа в том, что не нужно обладать никакими специальными знаниями, и этот способ под силу любому. Успех этого метода зависит от смекалки «нападающего» – сможет ли он найти нужную информацию или нет.

2.5. Модное слово «фишинг»

Попросим пользователя самого сообщить нам свой пароль. Нет, этот способ не подразумевает физического насилия, и ни один из пользователей в результате эксперимента не пострадает. Во всяком случае, физически.

Суть этого метода в следующем: нужно создать поддельную версию страницы авторизации того сервиса, который вы хотите взломать. Например, если вы хотите получить пароль от почты GMail.com, тогда нужно создать такую же страницу входа.

Далее нужно заманить пользователя на поддельную страницу. Это можно сделать несколькими способами:

- Отправить ему сообщение якобы от имени администрации того сервиса. В сообщении указать, что-то вроде «Вы давно не заходили в свой почтовый ящик. Если вы не воспользуетесь им до <Д>.<М>.<Г>, он будет удален.». Рисуем кнопочку Войти, нажав которую, пользователь попадет на вашу страницу авторизации.
- Отправить сообщение со ссылкой, которая должна заинтересовать пользователя. Когда он перейдет по ней, он увидит сообщение о необходимости входа для просмотра содержимого. Сейчас многие сервисы позволяют войти с помощью учетной записи GMail или одной из социальных сетей. Так что пользователь может ничего и не заподозрить.

4 https://wikileaks.org/cia-emails/The-Conundrum-of-Iran/page-1.html

Очень часто описывается только «общее направление». Сейчас мы попробуем реализовать его и посмотреть на реакцию обычных пользователей. Способ довольно непростой, и для его реализации понадобятся как навыки программирования на PHP, так и некоторые финансовые вложения. Ведь нам понадобится хостинг с поддержкой PHP (для выполнения PHP-сценария и размещения формы авторизации) и доменное имя, «похожее» на имя взламываемого сервиса. Конечно, опытный пользователь сразу заметит подлог, но неопытный пользователь (или просто в спешке) может ничего не заметить.

Итак, мы создали форму авторизации, похожую на форму входа в Google. Результат наших страданий изображен на рис. 2.11. Страница полностью идентична странице входа в Google. Вот только обратите внимание на строку адреса. Вы сразу не заметили? Возможно, реальный пользователь тоже не заметит подлога. Создать такую страницу очень просто – выполните команду **Save as** в браузере.

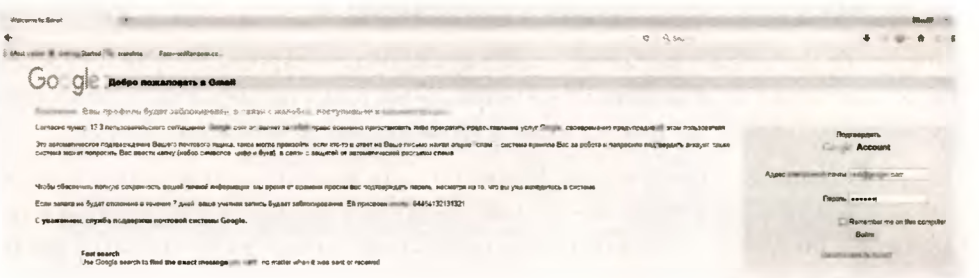


Рис. 2.11. Поддельная версия страницы входа в Gmail

Далее мы отправили некоторым сотрудникам сообщение о том, что их почтовый ящик будет заблокирован. Обратите внимание, что дизайн письма даже отдаленно (если не считать логотипа) не напоминает дизайн, используемый Google. Но, как показала практика, для наших пользователей этого было достаточно. Можно было бы взять исходный код письма, которое отправляет Google, сделать все более качественно. В реальных условиях злоумышленник так и сделает – будьте в этом уверены.

Что произошло дальше? Дальше пользователи прочитали письмо, перешли по ссылке и наивно ввели имя пользователя и пароль, которые были переданы сценарию. Сценарий принимает эти данные и записывает в текстовый файл. Написать такой сценарий сможет любой новичок, владеющий основами PHP. Примерный код сценария (это не тот сценарий, который использовали мы) приведен в листинге 2.1.

Листинг 2.1. Простейший сценарий записи паролей

```
<?php
    $login = $_POST['Login'];                    // введенный логин
    $pass = $_POST['password'];                  // пароль

    // Записываем полученные данные
    $text = "Login = $login\nPassword = $pass\n";

    $filelog = fopen("log.txt","a+");  // открываем файл
    fwrite($filelog,"\n $text \n");    // записываем строку
    fclose($filelog);                  // закрываем

    // перенаправляем пользователю на страницу входа в google,
       чтобы
    // меньше было подозрений
    header('Location: https://accounts.google.com/ServiceLog
in?service=mail&passive=true&rm=false&continue=https://mail.
google.com/mail/&ss=1&scc=1&ltmpl=default&ltmplcache=2&emr=1&o
sid=1#identifier ');
    ?>
```

Результат работы нашего сценария будет примерно таким:

```
some_user@gmail.com
123456

user_john_doe@gmail.com
topsecret
```

Понятное дело, логины и пароли здесь вымышленные.

Для отправки сообщения использовалась почта Yahoo!, чтобы не бороться с антиспамом. Но можно было бы пойти и по иному пути. Например, найти сервер SMTP со свободной отправкой писем (без авторизации). Как правило, это будет неправильно настроенный SMTP-сервер какой-то небольшой организации. Списки таких серверов регулярно обновляются на специальных ресурсах. Думаю, не составит особого труда найти такой список[5]. Далее можно развернуть на локальном компьютере веб-сервер[6] с поддержкой PHP. Тогда у вас будет доступ к php.ini и можно будет указать SMTP-сервер, через который функция mail() будет отправлять письма.

5 https://www.arclab.com/en/kb/email/list-of-smtp-and-pop3-servers-mailserver-list.html

6 https://bitnami.com/stack/wamp/installer

С другой стороны, можно попытаться отправить сообщение и через собственный хостинг (не обязательно устанавливать локальный веб-сервер). Все зависит от его настроек. Мы, например, для выполнения сценария отправки нашего сообщения использовали наш хостинг. На нем функция mail() выполнилась без особых нареканий. Понятно, что если просмотреть все заголовки письма, «след» приведет к нам. Но для нас сейчас это не важно. Сейчас важно, чтобы в почтовом клиенте поле «From» содержало то, что нам нужно. В первом способе мы поступили именно так, то есть для отправки сообщения использовали функцию mail().

Стандартная PHP-функция mail()[7] позволяет с легкостью указать как текст письма, так и его заголовки. Например:

```
$headers = 'From: Security Service <no-reply@example.com>'
."\r\n" .
    'Reply-To: no-reply@example.com'    "\r\n";

mail($to, $subject, $message, $headers);
```

Письма, отправленные таким образом, миновали антиспам Google (не попали в папку Спам) и нормально отображались как в почтовом клиенте (проверялось в Outlook и The Bat!), так и в веб-интерфейсе. Конечно, перед отправкой сообщения жертве лучше отправить его на свой ящик и убедиться, что письмо отображается правильно, как минимум, что почтовый клиент правильно определяет кодировку. Если это не так, в $headers нужно добавить заголовки, описывающие кодировку письма.

Теперь о результатах. Определенные результаты при использовании этого метода все же были получены. Некоторые из пользователей проверяемой компании оставили свои реальные пароли. Некоторые не отреагировали на это письмо и обратились к администратору. А некоторые догадались, в чем дело, и вместо пароля ввели абракадабру. Но все же несколько реальных паролей были получены, так что этот метод работает, несмотря на весь скептицизм.

2.6. Восстанавливаем пароль

Теперь попробуем вспомнить то, что никогда не знали, – пароль от почтового ящика жертвы. Очень часто почтовые службы позволяют восстановить забытый пароль. А чтобы убедиться, что пользователь, пытающийся восстановить доступ к ящику, является его владельцем, почтовая служба задает контрольный вопрос, указанный при регистрации почтового ящика. Если вы пытаетесь взломать ящик знакомого вам человека, то есть вероятность,

7 http://php.net/manual/bg/function.mail.php

что вы уже знаете ответ на этот вопрос. Если же вы взламываете пароль чужого человека, то первое, что нужно сделать, – это заняться изучением жертвы.

Чем больше вы соберете информации о жертве, тем проще будет взломать почтовый ящик. Информацию можно собирать разными способами – можно втереться в доверие к самой жертве и выведать как бы случайно у него нужную вам информацию (например, девичью фамилию матери), а можно подружиться с друзьями жертвы. Благо социальные сети позволяют быстро найти не только жертву, но и ее друзей.

2.7. Кража Cookies

Еще один неплохой способ получения доступа к почтовому ящику – это кража Cookies. Конечно, он эффективен, если жертва хранит свои пароли в браузере. Даже если вы не получите пароль к почтовому ящику, вы можете получить пароли к другим сервисам. Пользователи часто используют одни и те же пароли для доступа к разным сервисам. Поэтому если вы найдете пароль к одному сервису (например, к блогу, форуму), вы можете попытаться его использовать при входе в почтовый аккаунт. Есть вероятность, что он подойдет.

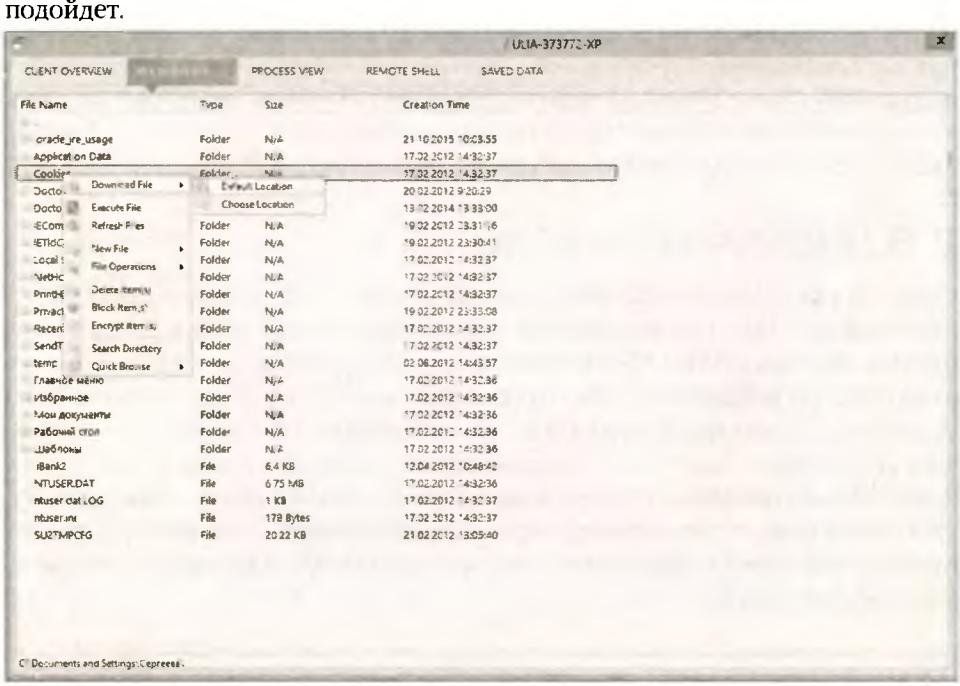


Рис. 2.12. Использование трояна для кражи Cookies

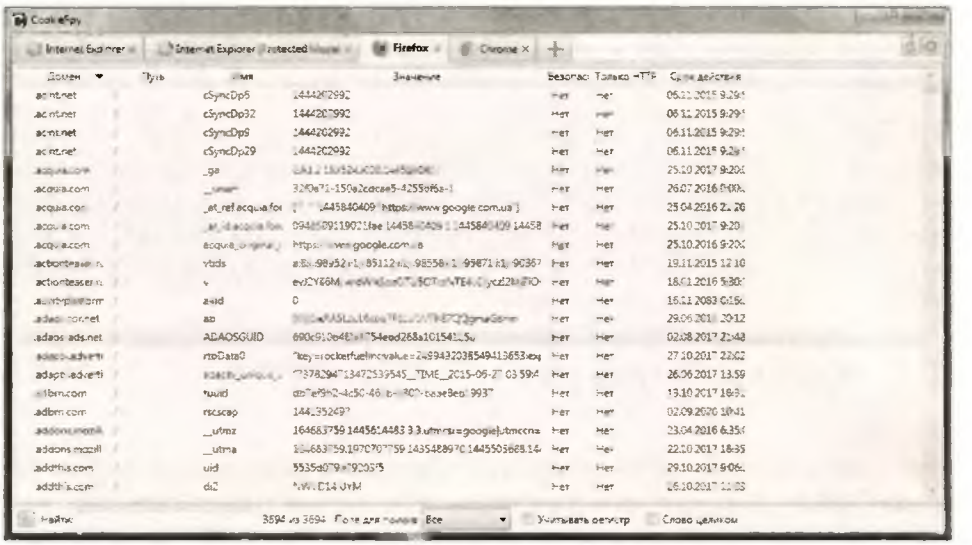


Рис. 2.13. Программа CookiesSpy

Как украсть «куки»? Существуют различные способы – от использования трояна (см. рис. 2.12) до банального копирования на флешку или свой FTP, если вы оказались за компьютером жертвы. Под рукой нет приложения для получения паролей? Не беда! Можно просто скопировать каталог с Cookies и проанализировать на своем компьютере. Для анализа Cookies можно использовать самые разные утилиты, одна из которых CookieSpy[8], которая поддерживает не только установленные, но и portable-браузеры, что позволяет «подсунуть» программе каталог с Cookies (рис. 2.13).

2.8. XSS-уязвимости

Один из способов взлома электронной почты – это использование XSS-уязвимостей. Вот только вряд ли можно назвать его эффективным. Во-первых, все найденные XSS-уязвимости в популярных почтовых сервисах очень быстро устраняются. Во-вторых, учитывая «во-первых», искать XSS-уязвимость придется самому (ведь все найденные уязвимости уже закрыты). А на поиск потребуется определенное время. Да и реализация атаки через XSS-уязвимость требует повышенной квалификации. Как вариант, этот метод можно рассмотреть сугубо из академического интереса. Но если нужно побыстрее взломать почту, тот же социальный инженеринг окажется более эффективным.

8 http://www.cookiespy.com/

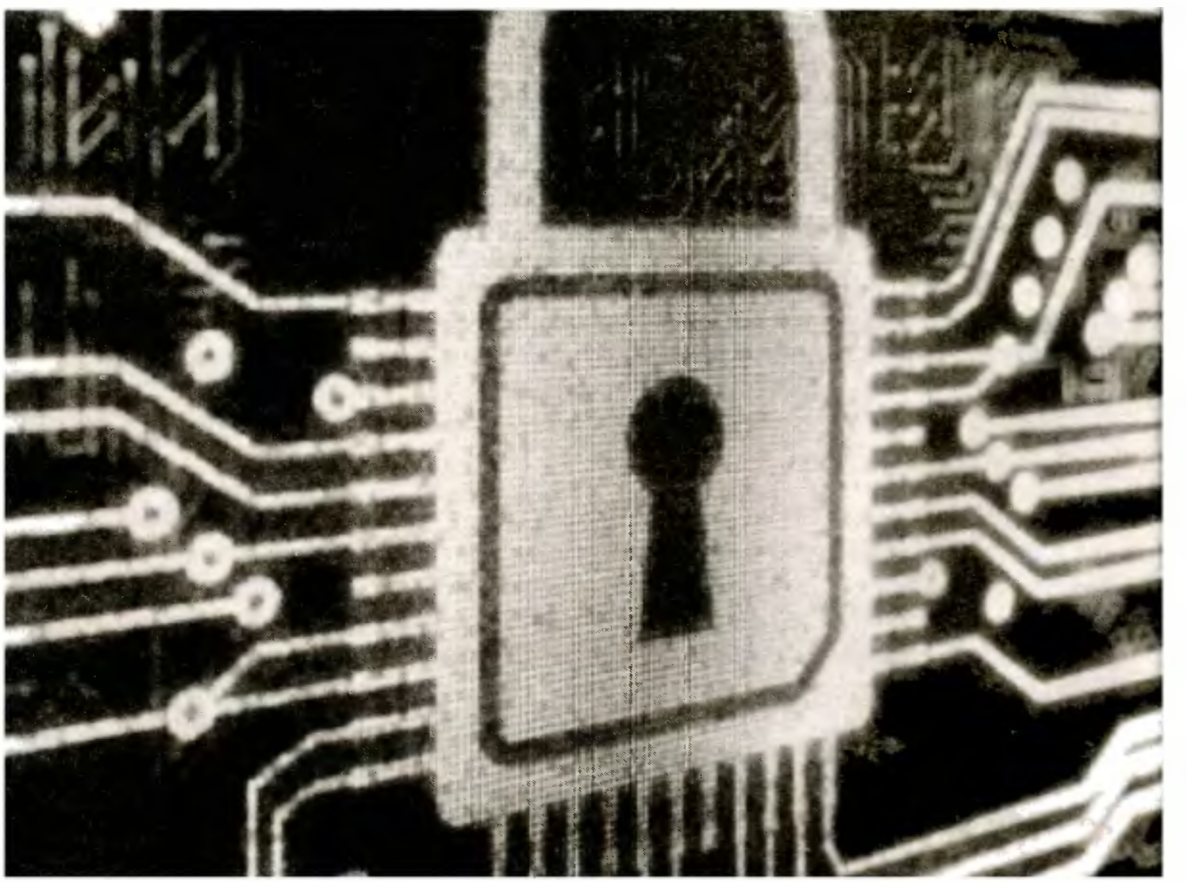
2.9. Метод грубой силы

Самый неэффективный способ. Он заключается в переборе пароля по списку. Программа просто пытается подобрать пароль методом «тыка» (он же метод Коши). Конечно, в идеальных условиях у нее это рано или поздно получится. Но практически все сервисы заблокируют почтовый ящик после 3-5 неудачных попыток. Поэтому вряд ли у вас получится использовать «метод грубой силы». Если вам таки хочется попытаться, тогда можете попробовать использовать утилиту Brutus, использование которой обсуждается на hackerthreads[9].

Есть и еще одна довольно популярная утилита – THC-Hydra[10], позволяющая взломать самые различные сервисы: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC и XMPP.

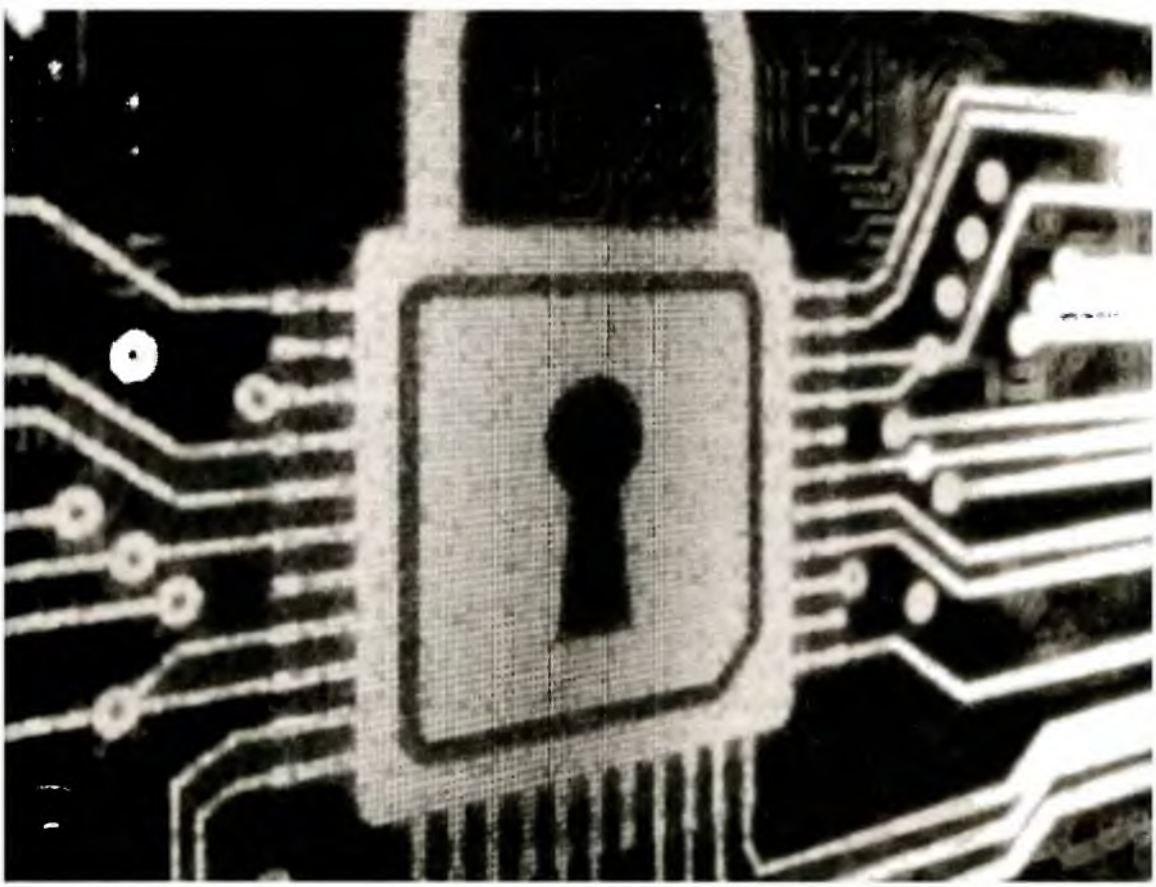
На этом всё. В следующей главе мы рассмотрим, как можно защитить электронную почту от взлома и перехвата.

9 http://www.hackerthreads.org/Topic-47150
10 https://www.thc.org/thc-hydra/



Глава 3.

Защита электронной почты



3.1. Немного теории. S/MIME, PKI и PGP

При написании этой книги я старался объяснять вещи максимально просто, не погружаясь во всевозможные технические дебри. Однако иногда для полноценной работы с той или иной технологией пользователю нужно знать ее особенности и всевозможные нюансы. И такой случай настал.

В первой главе было показано, что использование стандарта S/MIME является самым надежным способом защиты электронной почты. Так оно и есть. Но вы должны знать, что это не панацея, есть и другие способы.

Для начала нужно разобраться, что такое S/MIME. S/MIME (Secure/ Multipurpose Internet Mail Extensions) – стандарт для шифрования и подписи в электронной почте с помощью открытого ключа. Такое определение вы можете найти на просторах Интернета, в той же Wikipedia. Звучит довольно гордо – «стандарт». Но на самом деле S/MIME – это PKI приложение, используемое для цифровой подписи, а также шифрования почтовых и других сообщений.

«Погружаемся» глубже. Теперь вы открыли еще один новый для себя термин – PKI, или Инфраструктура открытых ключей (англ. PKI – Public Key Infrastructure). Сейчас разберемся, что это такое. В первой главе вы узнали, что такое симметричная и асимметричная криптография. Классический метод криптографии использует блоки данных, называемые «секретными ключами». С помощью секретных ключей можно зашифровать и расшифровать информацию, но только в случае, если вы знаете метод шифрования и у вас есть ключ. То есть один и тот же ключ используется как для шифрования, так и для расшифровки сообщения.

Но есть и асимметричная криптография, которая базируется на использовании пары ключей – «закрытого ключа» и «открытого ключа». Эти ключи должны создаваться вместе, с использованием специальных алгоритмов.

Любая информация, зашифрованная открытым ключом, может быть расшифрована только с использованием соответствующего «закрытого ключа».

PKI является технологией, основывающейся на такой асимметричной криптографии. В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- Закрытый ключ должен быть известен только его владельцу.
- Удостоверяющий центр создает электронный документ – сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается в сертификате.
- Никто никому не доверяет, но все доверяют удостоверяющему центру, выдавшему сертификат.
- Удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом

Дополнительную информацию (если, конечно, вы заинтересовались) о S/MIME и PKI[1] вы найдете в Интернете. Информации море, и найти ее не составит труда. А мы переходим к другому неизвестному пока термину – PGP.

PGP (Pretty Good Privacy) – еще одна технология обеспечения безопасности, а именно шифрования и цифровой подписи. На данный момент существуют обе технологии (обе используют принцип открытых ключей) защиты электронной почты – PKI (в лице S/MIME) и PGP. Обе технологии одинаково популярны. Посмотрим, какая между ними разница.

В основу PGP положен стандарт OpenPGP, который содержит:

- сведения о владельце сертификата;
- открытый ключ владельца сертификата;
- ЭЦП владельца сертификата;
- период действия сертификата;
- предпочтительный алгоритм шифрования.

В основу PKI положен стандарт X.509, который содержит:

- открытый ключ владельца сертификата;

1 Настоятельно рекомендую прочитать https://www.safe-mail.net/support/eng/help/protectsecure/pki.html

- серийный номер сертификата;
- уникальное имя владельца;
- период действия сертификата;
- уникальное имя издателя;
- ЭЦП издателя и идентификатор алгоритма подписи.

Казалось бы, эти технологии подобны. Но есть одна фундаментальная разница между ними: сертификат PGP создается только лично (самоподписанный сертификат), сертификат X.509 может получаться от центра сертификации, а также быть самоподписанным. Именно по этой причине я использую стандарт S/MIME – ведь есть третья сторона, которая выступает гарантом, что тот, с кем вы обмениваетесь корреспонденцией, – тот, за кого он себя выдает на самом деле.

Конечно, можно долго спорить, что надежнее – PKI или PGP, – особенно с фанатами PGP (кстати, раз уж такое дело, то и PGP мы тоже рассмотрим, но только в Linux, – как правило, пользователям Linux нравится именно больше PGP, но о ней мы поговорим в следующей главе). Но не считаю, что на полемику нужно тратить время. Книга задумывалась практической, и поэтому должна содержать краткие и понятные инструкции, а не рассуждения о том, какая технология теоретически надежнее.

3.2. Как будем защищать почту

В первой главе этой книги были рассмотрены различные способы защиты электронной почты. Было показано, что самым надежным и универсальным средством является использование стандарта S/MIME.

Да, есть и другие средства, но все они обладают определенными недостатками. Взять ту же программу PGP Desktop (как вы догадались, эта программа использует технологию PGP). Во-первых, она платная, и стоит довольно-таки дорого для обычного домашнего пользователя. Во-вторых, дешифровка происходит «на лету», а в самом файле Outlook или любого другого почтового клиента расшифрованные сообщения хранятся в открытом виде, а это означает, что их может прочитать любой пользователь. Конечно, можно создать криптодиск и хранить почтовую базу в нем, но зачем такие сложности? Ведь можно просто настроить S/MIME. Все, что вам нужно, – это создать сертификат (публичный и приватный ключ) и настроить ваш почтовый клиент. При этом нет разницы, какой это будет клиент, – главное, чтобы он поддерживал S/MIME. Операционная система тоже не важна. Вы можете сгенерировать сертификаты в Windows, а использовать их для настройки почтовых клиентов в MacOS, Linux и Android (или наоборот, ска-

жем, сгенерировать сертификат в Android и использовать их в любой другой ОС). При этом не будет привязки к конкретной программе (PGP Desktop) и к конкретной операционной системе.

Осталось только одно – выбрать программу для генерирования сертификата S/MIME. Здесь выбор за вами: вы можете или использовать какую-то стороннюю программу, или «родную» – openssl. Пользователям Linux ничего устанавливать не придется – команда openssl доступна по умолчанию. А вот Windows-пользователи могут скачать OpenSSL для Windows по адресу:

https://code.google.com/archive/p/openssl-for-windows/downloads

3.3. Использование OpenSSL

Сгенерировать ключи можно с помощью команды openssl:

```
openssl genrsa -out rootCA.key 4096
openssl genrsa -out privateKey.pem -aes256 4096
openssl rsa -in privateKey.pem -pubout -out publicKey.pem
```

Первая команда генерирует корневой сертификат (4096 бит), вторая – приватный (закрытый) ключ длиной 4096 бит. Третья команда генерирует по этому закрытому ключу публичный (открытый) ключ.

Позволю себе некоторые технические подробности относительно шифрования. При использовании симметричного шифрования зашифровать и расшифровать файл file.txt можно так (сообщение электронной почты, по сути, тот же файл, формируемый почтовым клиентом):

```
openssl enc -aes-256-cbc -salt -in file.txt -out file.enc
openssl enc -d -aes-256-cbc -in file.enc -out file.txt
```

Ранее мы сгенерировали RSA-пару ключей (открытый и закрытый). Так уж устроен RSA, что зашифровать данные длиной более 4 Кб не получится. Что делать? Есть способ обойти это – информация сначала шифруется симметричным алгоритмом (подобно использованному выше) с использованием одноразового ключа. Затем этот одноразовый ключ шифруется публичным ключом. При расшифровке одноразовый ключ расшифровывается закрытым. Именно такой способ и используется в почтовых клиентах, ведь информация часто превышает 4 Кб.

Для шифрования и расшифровки файла используются опции -encrypt и -decrypt соответственно команды openssl. Дополнительную информацию вы сможете найти в руководстве (man) по команде openssl.

3.4. Использование CyberSafe Top Secret

Если пользователи Linux привыкли к командной строке, и она их не смущает (к тому же под рукой есть удобная справочная система man), то Windows-пользователям вряд ли нравится такое положение дел. Хочется какой-то оболочки. И такая оболочка найдена – CyberSafe Top Secret. Данное приложение использует библиотеку OpenSSL для генерирования сертификатов и шифрования данных. Другими словами, вы получите те же ключи, но управлять ключами гораздо удобнее с помощью этой программы. К тому же она позволяет публиковать открытые ключи на сервере ключей, что предельно упрощает обмен ключами между пользователями. Уже не нужно передавать вашим собеседникам свой публичный ключ – они могут ввести ваш e-mail в поле поиска, и ваш публичный ключ будет импортирован на их компьютер.

Итак, разберемся, как сгенерировать свои личные ключи. Перейдите в раздел **Ключи и сертификаты, Личные ключи** программы (рис. 3.1). В разделе **Все ключи** отображаются все ключи, в том числе и публичные ключи других пользователей, импортированные вами. А в разделе **Личные** содержатся только ваши ключи – те, которые вы генерировали самостоятельно. Если у вас уже есть ключ, сгенерированный другой программой, его можно импортировать, нажав кнопку **Import**.



Рис. 3.1. Ваши ключи

Основной мой адрес – dhsilabs@gmail.com. Ради демонстрации настройки шифрования я зарегистрировал адрес dhsilabs2@mail.ru. Теперь нужно создать сертификат для него. Нажмите кнопку **Создать**. В появившемся окне (рис. 3.2) введите e-mail, пароль, выберите срок действия сертификата, выберите размер ключа (в битах) и включите флажок **Опубликовать после создания**.

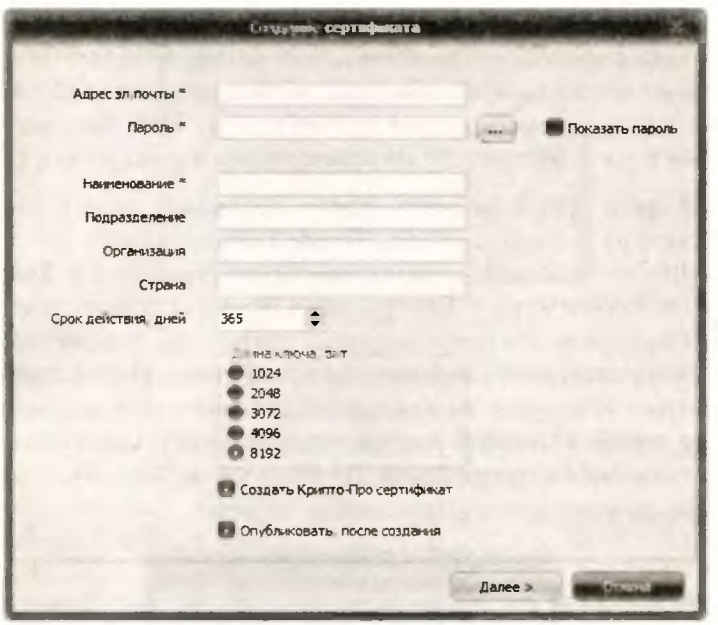


Рис. 3.2. Создание сертификата

Теперь разберемся, что есть что. С паролем, e-mail и прочими информационными параметрами все ясно. А вот параметр **Срок действия** позволяет указать срок действия сертификата в днях. Если у вас легкая степень параноии, то нужно создавать сертификаты на 1-2 года и потом заново их перегенерировать. Но Google подписывает свои приложения на Google Play сертификатами со сроком годности 10 000 дней.

Что произойдет, если выйдет срок годности? Просто программы, в которых предусмотрен контроль срока годности, будут сообщать, что срок годности сертификата истек, напоминая вам о необходимости создания нового сертификата. Однако данные, зашифрованные этим сертификатом, все еще можно будет расшифровать. Основная проблема в том, что сертификатом с истекшим сроком годности нельзя будет зашифровать сообщение. То есть вам нужно будет сгенерировать новый сертификат, которым вы, к сожалению, не сможете расшифровать старые сообщения, зашифрованные более

ранним сертификатом. Поэтому установите количество дней 3650 (10 лет) и длину сертификата 4096 или 8192 (если у вас мощный компьютер, например, с процессором i5 или лучше). Длины ключа в 4096 бит хватит, чтобы никто в течение 10 лет не подобрал пароль к вашему сертификату.

Итак, со сроком годности сертификата мы разобрались, теперь поговорим о размере ключа. Ранее было сказано, что на данный момент минимально допустимым является размер ключа 2048 бит. Если вы работаете с очень секретной информацией, установите длину ключа 4096 бит или даже 8192 бит. Однако на медленных компьютерах, в том числе на мобильных устройствах, лучше использовать ключи с размером до 4096 бит, иначе процесс шифрования и расшифровки будет происходить довольно медленно.

Включив флажок **Опубликовать после создания**, вы опубликуете публичный ключ на сервере ключей. Позже будет показано, как можно легко импортировать ваш ключ. Собственно, нажмите кнопку **Далее**. Нужно подождать, пока сертификат будет создан. Время создания зависит от расторопности вашего компьютера и длины ключа. Как только создание сертификата будет завершено, нажмите кнопку **Готово**. После этого появится окно, в котором нужно ввести код подтверждения публикации, отправленный на ваш e-mail. Откройте ваш почтовый ящик и скопируйте из полученного письма код подтверждения. После этого вы увидите окно о том, что ваш сертификат успешно опубликован на сервере.



Рис. 3.3. Ввод кода подтверждения при публикации сертификата

Далее выберите его и нажмите кнопку **Экспорт**. В появившемся окне (рис. 3.4) нужно ввести пароль от сертификата. Далее выберите все, что будет доступно, и выберите папку для экспорта. Экспорт сертификата необходим для настройки почтового клиента. Конечно, для настройки того же Outlook достаточно выбрать PFX и CER файлы, но мы сделаем полный экспорт с целью резервного копирования. На рис. 3.5 находится список полученных в результате экспорта файлов.

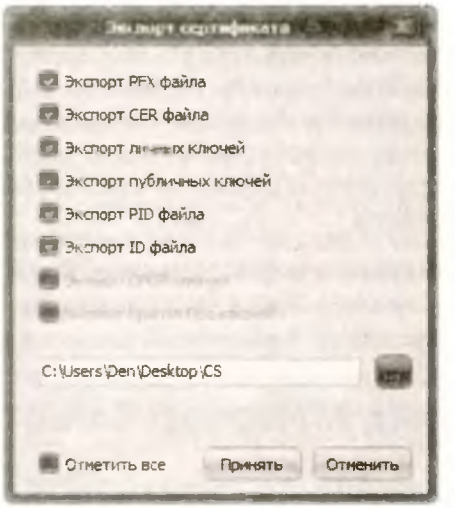


Рис. 3.4. Экспорт сертификата



Рис. 3.5. Результат экспорта

Итак, у нас сгенерировано два сертификата – один для dhslabs@gmail.com, другой для dhslabs2@mail.ru. В реальности это два разных пользователя, поэтому сертификаты будут генерироваться на разных компьютерах – А и Б соответственно. Затем на компьютере А нужно импортировать публичный ключ для dhslabs2@mail.ru, а на компьютере Б – публичный ключ для dhslabs@gmail.com, чтобы пользователи на компьютерах А и Б могли зашифровать сообщения, адресованные друг другу. Для импорта сертификата достаточно нажать кнопку **Поиск** и ввести нужный e-mail. После импорта сертификата другого пользователя с сервера ключей (или через кнопку **Импорт** – если вы не доверяете серверу ключей) его тоже нужно экспортировать, чтобы можно было указать в адресной книге почтового клиента (указать, что конкретный сертификат принадлежит определенному пользователю).

При генерировании своих личных ключей (если у вас несколько почтовых адресов) все ключи можно сгенерировать на одном компьютере, затем их экспортировать и передать на другие устройства. Например, если у вас на разных устройствах используются разные почтовые адреса. Не обязательно устанавливать программу на все устройства (да и это невозможно сделать физически: как вы установите Windows-программу на MacOS – вряд ли она будет работать правильно).

После создания и обмена ключами программа CyberSafe Top Secret больше не нужна и ее можно закрыть. Далее будет показано, как настроить почтовые клиенты.

3.5. Настройка Microsoft Outlook

Далее будет показано, как настроить шифрование в почтовом клиенте Microsoft Outlook 2013/2016. В более старых версиях Microsoft Office шифрование настраивается аналогично, но несколько иначе. Принцип будет тот же, но команды интерфейса и их расположение – другими. Подробные инструкции вы без проблем найдете в Интернете.

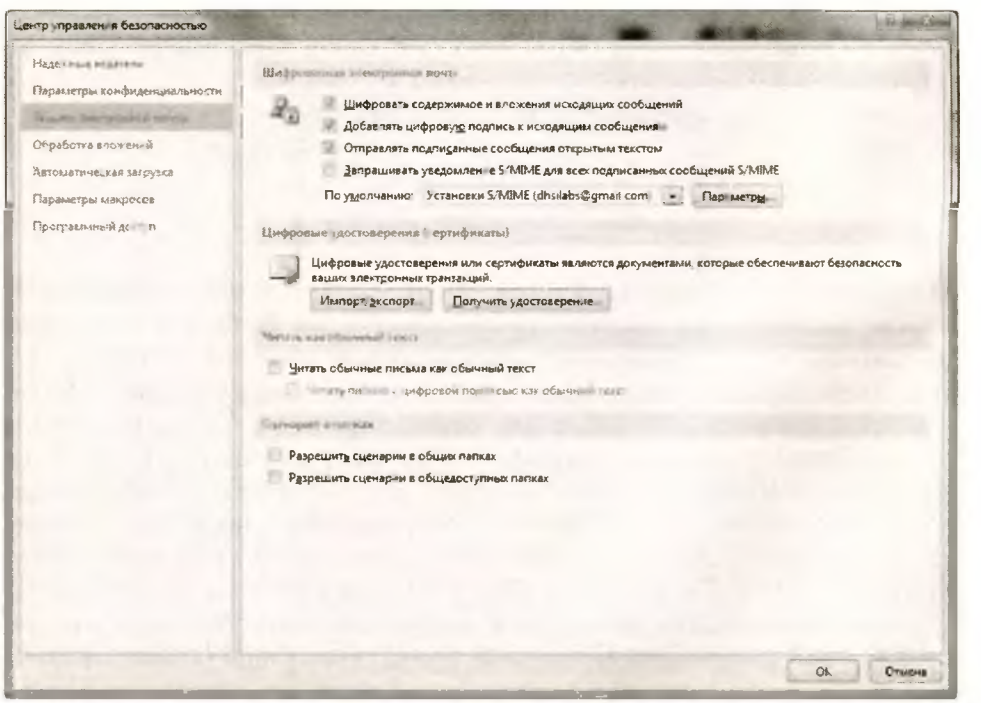


Рис. 3.6. Включаем шифрование писем

Первым делом нужно установить экспортированный сертификат в формате PKCS#12 в хранилище Windows. Для этого дважды щелкаем на PFX-файле и следуем инструкциям мастера импорта сертификатов. Поскольку этот сертификат содержит ваш закрытый ключ, в процессе импорта потребуется ввести пароль, который был указан при его создании.

После этого запускаем Microsoft Outlook. Выберите команду меню **Файл, Параметры, Центр управления безопасностью**. Нажмите кнопку **Параметры центра управления безопасностью**. В появившемся окне перейдите в раздел **Защита электронной почты** (рис. 3.6). Включите параметры **Шифровать содержимое и вложения исходящих сообщений** и **Добавлять цифровую подпись к исходящим сообщениям**. Первый параметр обеспечивает шифрование содержимого и вложений письма, а второй – добавляет цифровую подпись к каждому письму. Подробно о цифровой подписи мы поговорим в следующей главе.

Теперь из списка установленных в хранилище сертификатов нужно выбрать тот, который будет использоваться для шифрования и создания цифровой подписи. Для этого здесь же нажимаем **Параметры** и выбираем свой сертификат (рис. 3.7), нажав кнопку **Выбрать** напротив **Сертификат шифрования** и **Сертификат подписи**. Поскольку сертификат уже импортирован в хранилище Windows, он появится в окне выбора.

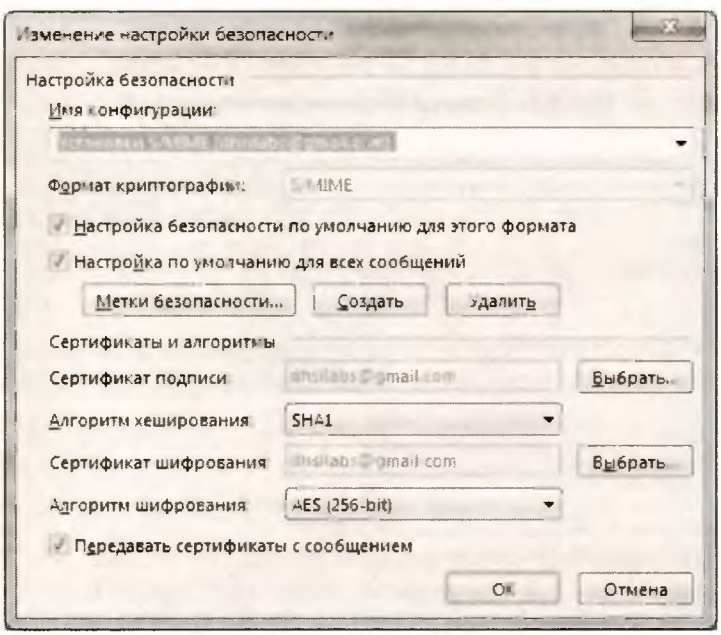


Рис. 3.7. Параметры безопасности

Собственно, на этом все. Нажмите кнопку **OK**, а затем еще раз – кнопку **OK** для закрытия окна настроек. Ваш почтовый клиент настроен на шифрование. Но чтобы была возможность отправлять зашифрованные письма конкретному адресату, вам нужно импортировать его ключ в почтовый клиент. В моем случае я буду отправлять зашифрованные письма по адресу dhsilabs@gmal.com. Следовательно, мне нужно импортировать публичный сертификат для этого адреса в почтовый клиент. Разберемся, как это сделать.

Перейдите на вкладку **Главная**, выберите **Создать элемент, Контакты** (рис. 3.8). Далее введите имя контакта и адрес электронной почты (рис. 3.9).

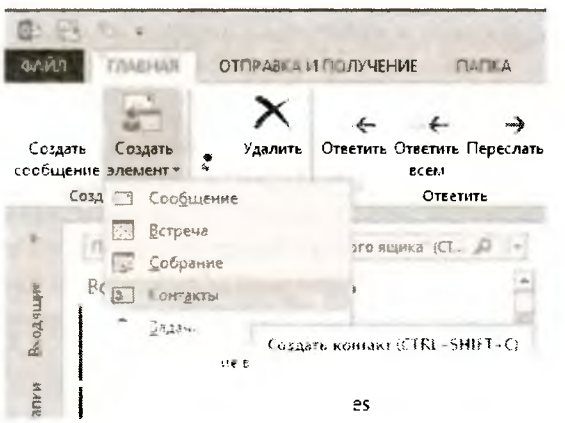


Рис. 3.8. Команда создания нового контакта



Рис. 3.9. Создание нового контакта



Рис. 3.10. Пустой список сертификатов

После этого нажмите кнопку **Certificates** – она находится на вкладке **Contacts**, рядом с кнопкой **General**. Вы увидите пустой список сертификатов (рис. 3.10).

Нажмите кнопку **Импорт** и перейдите в каталог, в который вы экспортировали открытый ключ пользователя. Напомню последовательность действий:

- Найти и импортировать открытый ключ пользователя в CyberSafe посредством кнопки **Поиск**.
- Экспортировать открытый ключ в какую-то папку с помощью кнопки **Экспорт.**
- В Outlook нажать кнопку **Импорт** (рис. 3.10) и выбрать CER-файл сертификата (в моем случае нужно выбрать файл dhsilabs@gmail.com.cer).

На рис. 3.11 изображен результат наших стараний – сертификат пользователя связан с его контактом в Outlook. Для сохранения контакта обязательно нажмите кнопку **Save & Close**.

Теперь осталось все проверить. Создайте новое сообщение. Все как обычно: вводите получателя, тему, текст и нажимаете кнопку **Отправить**. Если сертификат был связан с контактом, почтовый клиент автоматически зашифрует сообщение. Если сертификата нет, почтовый клиент предложит отправить незашифрованное сообщение. Управлять шифрованием и под-



Рис. 3.11. Сертификат для контакта импортирован в Outlook

письмо можно на вкладке **Параметры** (рис. 3.12). Если выключить режим **Шифровать**, то сообщение будет отправлено без шифрования, если выключить режим **Подписать**, сообщение будет отправлено без подписи.



Рис. 3.12. Новое сообщение

Теперь откроем браузер и войдем в почтовый ящик. Посмотрим, было ли зашифровано сообщение. Как видно из рис. 3.13, сообщение зашифровано, текст сообщения скрыт, а сообщение содержит вложение smime.p7m. Расшифровав этот файл, можно будет увидеть сообщение.

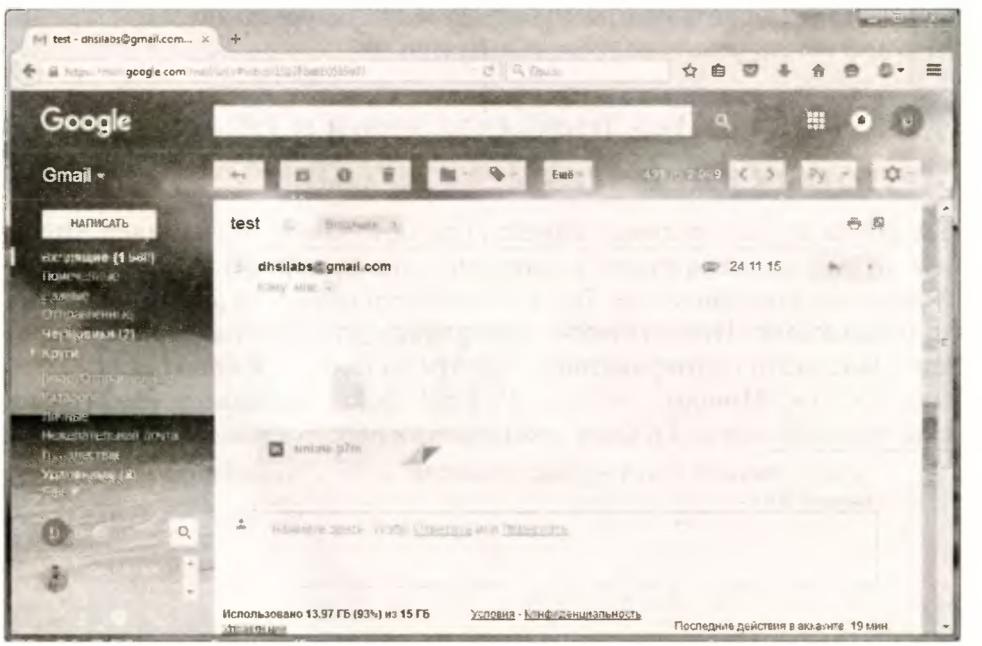


Рис. 3.13. Сообщение зашифровано

На «той» стороне тоже нужно настроить почтовый клиент подобным образом и импортировать открытый ключ пользователя, написавшего сообщение. После этого можно будет расшифровать его сообщение и отправить ему ответ в зашифрованном виде. Посмотрите на рис. 3.14. На нем отображается зашифрованное сообщение. В списке сообщений зашифрованные сообщения отмечаются замком. При просмотре самого зашифрованного сообщения в верхнем правом углу рабочей области выводятся два значка – замок и медаль. Замок, как мы уже знаем, означает зашифрованное сообщение, а медаль – подписанное.

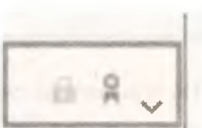


Рис. 3.14. Зашифрованное сообщение

Вот теперь действительно все. Может, такая настройка вам показалось сложной, но это только в первый раз. Да и после того, как вы настроите сертификаты, вам вообще ни о чем не нужно будет беспокоиться. Вы просто пишете письма, а почтовый клиент их автоматически зашифровывает и расшифровывает письма, адресованные вам. Все довольно просто. Конечно, можно установить плагин CyberSafe Mail Encryption, но зачем платить деньги за то, что можно получить бесплатно?

3.6. Настройка шифрования в других почтовых клиентах

Настройка других почтовых клиентов осуществляется аналогично. Принцип тот же – сначала нужно установить свой сертификат, потом сертификаты других пользователей. Так, в Thunderbird нужно открыть **Управление сертификатами (Инструменты, Настройки, Дополнительные, Сертификаты, Просмотр сертификатов**[2]), перейти на вкладку **Ваши сертификаты**, нажать кнопку **Импорт** и выбрать PCKS12-файл сертификата (файл с расширением .pfx или .p12), далее нужно ввести пароль и нажать **OK**.

2 По умолчанию в новых версиях Thunderbird меню не отображается. Для его показа нажмите F10

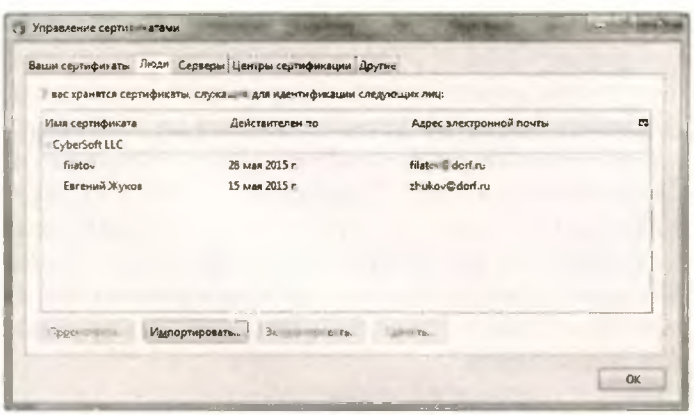


Рис. 3.15. Управление сертификатами

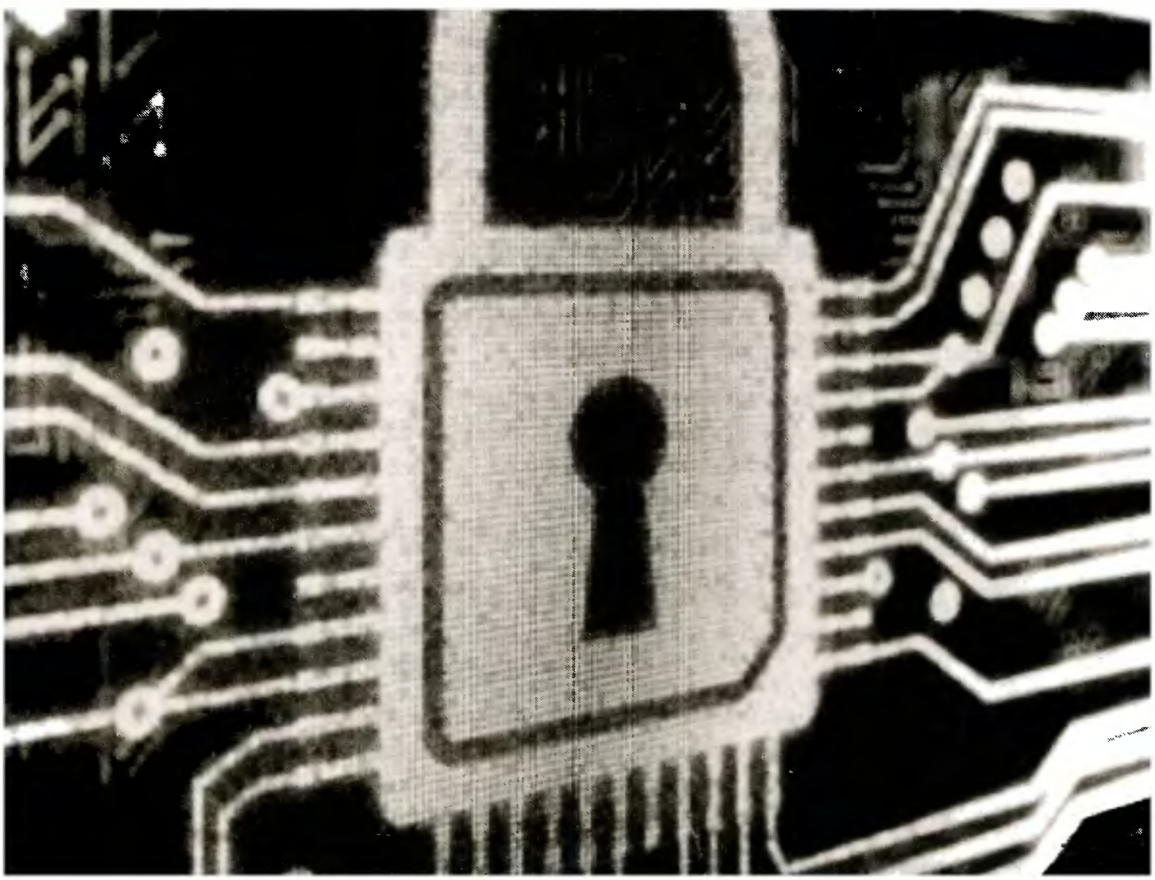
В почтовый клиент The Bat! встроены средства создания PGP-ключей. То есть ключ можно создать прямо из The Bat! и никакие другие программы не нужны. Только это будет не PKI (S/MIME) сертификат, а PGP. Конечно, при желании можно настроить The Bat! и на работу с S/MIME-сертификатами, только вот их придется генерировать самостоятельно. О настройке шифрования в The Bat! можно прочитать по адресу:

https://www.ritlabs.com/en/support/help/75/

В следующей главе мы поговорим об электронной подписи и заодно рассмотрим программу GPG (PGP) в Linux, как я обещал.

Глава 4.

Электронная подпись



4.1. Что такое электронная подпись?

Все мы привыкли к термину «электронная цифровая подпись», однако сейчас все чаще используется его сокращенный вариант – электронная подпись. В этой главе будут рассмотрены случаи применения электронной подписи в небольшой компании. Частным лицам электронная подпись нужна значительно реже. Однако сначала нужно разобраться, что такое электронная подпись.

Есть довольно непростое определение электронной подписи. Электронная подпись – информация в электронной форме, присоединенная к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией и используемая для определения лица, подписывающего информацию.

Другими словами, электронная подпись – это некоторая информация, позволяющая установить авторство документа и гарантировать, что документ не был изменен после его подписания.

4.2. Случаи использования электронной подписи в небольшой компании

4.2.1. Внутренний документооборот

Самый распространенный вариант внутреннего документооборота предприятия – это служебные записки. Больше нет смысла распечатывать документ и подписывать его собственноручно, если можно подписать его цифровой подписью и отправить дальше по цепочке.

Электронная подпись здесь экономит не только время, но и деньги – снижается расход бумаги и тонера принтера. Конечно, себестоимость одного распечатанного листа бумаги, может, и не сильно высока, но за год можно

сэкономить вполне приличную сумму, и это уже не говоря о времени, которое сегодня стоит дорого.

Как правило, на предприятии используются сетевые принтеры. Сетевой принтер может быть расположен в другом кабинете или вообще на другом этаже. Сотруднику, распечатавшему служебную записку, нужно выйти из своего кабинета, добраться до принтера и найти среди остальных документов свою записку. На все про все тратится 10-15 минут, а если учитывать человеческий фактор (разговоры с сотрудниками в соседнем кабинете), то гораздо больше. В итоге эти 10-15 минут могли бы быть потрачены более продуктивно, чем поиск распечатанного документа.

Второй пример – это процесс согласования договора. Представим, что сотрудник Иванов подготавливает договор и отправляет его на согласование руководителю. Принцип такой же, как и со служебной запиской, – зачем тратить время на печать договора, если можно подписать его электронной подписью? Руководитель вносит изменения в договор, подписывает его и отправляет Иванову. Учитывая, что изменений будет много (ведь ошибки все равно неизбежны), использование электронной подписи опять экономит много времени и средств.

В больших корпоративных сетях, где у руководителя и даже у рядового сотрудника Иванова могут быть недоброжелатели, электронная подпись – это надежный способ убедиться в авторстве документа и его неизменности (что никто без ведома Иванова или его руководителя не внес в него какие-то изменения).

Вы можете возразить, мол, есть права доступа, и видно, кто последний раз редактировал документ. Зачем нужна электронная подпись? Все как бы правильно, если бы не одно но. В любой системе есть пользователь с максимальными правами – администратор, который может не только изменить сам документ, но и его атрибуты (в том числе время/дату изменения, автора последнего изменения и т.д.).

4.2.2. Обмен документами с филиалами и партнерами

При обмене информацией с удаленными филиалами и партнерами компании обычно используется электронная почта. И здесь можно использовать электронную подпись, чтобы ваши партнеры и сотрудники удаленных филиалов могли быть уверены в том, что это сообщение отправили именно вы, а не кто-то, кто хочет вами казаться.

Да, пока нет практики заключения договоров полностью в электронном виде. Все равно еще необходима мокрая печать и подпись. Поэтому скрепить договор с партнером в полностью электронном виде не получится. Но

зато вы можете безопасно обмениваться сообщениями с вашими партнерами и не сомневаться, что кто-то подделает ваше сообщение или сообщение партнера.

Что же касается обмена документами с удаленными филиалами, то здесь можно использовать электронную подпись, как и при внутреннем документообороте. Сейчас документооборот между филиалами проходит в полуцифровой форме. А именно: документ сначала нужно распечатать, затем его должен подписать руководитель, после чего секретарь руководителя его сканирует и отправляет по электронной почте в удаленный филиал, где он опять распечатывается.

Электронная подпись позволяет сократить этот процесс: документ подписывается электронной подписью и отправляется в удаленный филиал, где получатель может проверить электронную подпись и убедиться, что документ был подписан именно руководителем.

4.2.3. Некоторые проблемы внедрения электронной подписи

Пока еще человеку трудно привыкнуть к электронной подписи, и к ней не относятся как к чему-то серьезному. Пока на документе не будет стоять «мокрая» подпись, его по-прежнему не считают подписанным. Сотрудники все еще будут использовать копии бумажных документов, терять свои закрытые ключи, не считая их чем-то важным. Как преодолеть психологический барьер? Как преодолеть то самое «без бумажки ты букашка, а с бумажкой человек»?

Оказывается, выход есть, и он заключается в еще одной бумажке. Нужно внутри предприятие принять «положение об электронном документообороте». Все сотрудники должны ознакомиться с ним и скрепить принятие этого положения своей подписью, пока что не электронной. Тогда сотрудники поймут, что все серьезно, – ведь их просят поставить подпись. После этого они начнут пользоваться электронной подписью, станут серьезно относиться к своим закрытым ключам и т.д.

Помимо психологического барьера есть еще один – образовательный. Опытному сотруднику со стажем, которому до выхода на пенсию осталось несколько лет, довольно трудно будет объяснить, что такое электронная подпись и как ее правильно использовать. Он относительно недавно освоил работу с обычной электронной почтой, а тут асинхронная криптография, открытые и закрытые ключи и т.д. Вот это и есть основная проблема, с которой я столкнулся относительно недавно на собственном опыте.

Решение есть, но оно не такое простое, как в первом случае. На первых порах задачу обучения работе с электронной подписью можно возложить на

плечи IT-отдела. Если ничего не получится, тогда уже можно перейти к услугам сторонних специалистов. Ведь есть же тренинги по работе с компьютером, офисными приложениями, электронной почтой. Аналогично можно найти курсы, посвященные современному документообороту.

Как и со всеми нововведениями, нужно быть готовым к волне неприятия. Но когда сотрудники поймут, насколько хороша электронная подпись, они перестанут работать по старинке. Чтобы облегчить переход на электронную подпись, нужно в том самом положении, о котором только шла речь, предусмотреть некоторый переходной период, когда еще можно пользоваться обычными подписями. Только не нужно устанавливать слишком большой срок, в противном случае все будут продолжать пользоваться обычными подписями.

Есть еще одна проблема, но она технического характера, следовательно, решается довольно просто. Для работы электронной подписи нужен удостоверяющий центр (УЦ) электронной подписи или центр сертификации.

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

Следовательно, УЦ придется или создать собственный, или же использовать внешние центры.

Основная задача УЦ – выдача сертификатов шифрования и подтверждение подлинности ключей шифрования.

4.3. Работа с электронной подписью посредством почтового клиента

Работать с электронной подписью очень и очень просто. Более того, вам даже ничего не придется настраивать, поскольку всю необходимую настройку вы уже выполнили в предыдущей главе. Да, все, что нужно для работы с электронной подписью, – это сгенерировать сертификаты и настроить почтовый клиент на шифрование и подпись, что и было проделано в предыдущей главе!

Чтобы ваше сообщение было подписано, достаточно включить режим **Подписать** на вкладке **Параметры** (рис. 4.1). Подписанные сообщения, адресованные вам, отмечаются медалью (рис. 4.2). При щелчке на ней происходит проверка электронной подписи, в результате которой сообщается, верна ли подпись или нет.



Рис. 4.1. Параметры сообщения

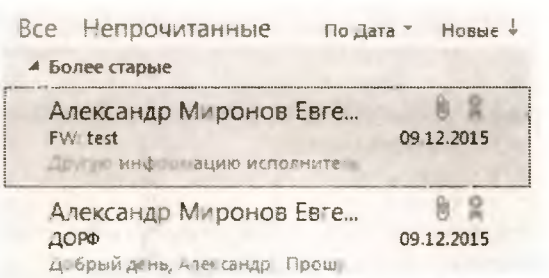


Рис. 4.2. Пример подписанных сообщений

Все достаточно просто, как видите. В других почтовых клиентах работа с электронно-цифровой подписью осуществляется аналогично. Так, в Thunderbird нужно включить переключатель **Подписать это сообщение**, если хотите подписать сообщение, и/или включить переключатель **Шифровать это сообщение**. Оба параметра находятся в меню **Защита** (рис. 4.3) окна создания нового сообщения.

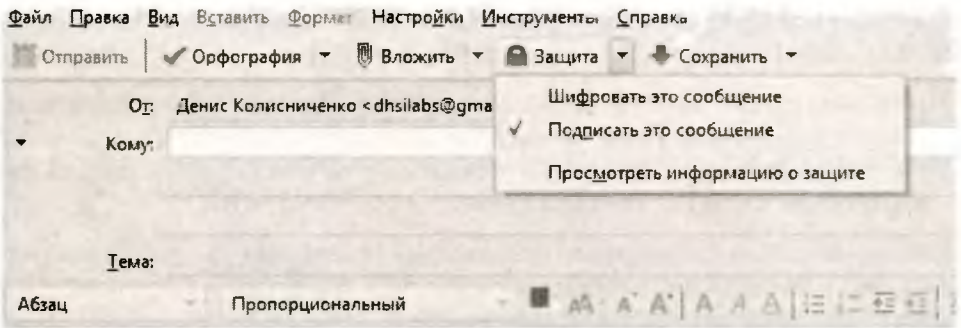


Рис. 4.3. ЭЦП в Thunderbird

4.4. Работа с цифровой подписью в Linux

Самый простой способ использовать электронную подпись в Linux – это использовать кросс-платформенные почтовые клиенты. Так, вы можете установить тот же Mozilla Thunderbird, добавить сертификаты и подписывать/шифровать сообщения подобно тому, как вы это делали в Windows.

Но это самый простой путь. А мы легких путей не ищем, поэтому сейчас мы рассмотрим сугубо Linux-способ, а именно программу PGP, точнее, GnuPG (GPG). Это открытый форк коммерческой программы PGP. GnuPG полно-

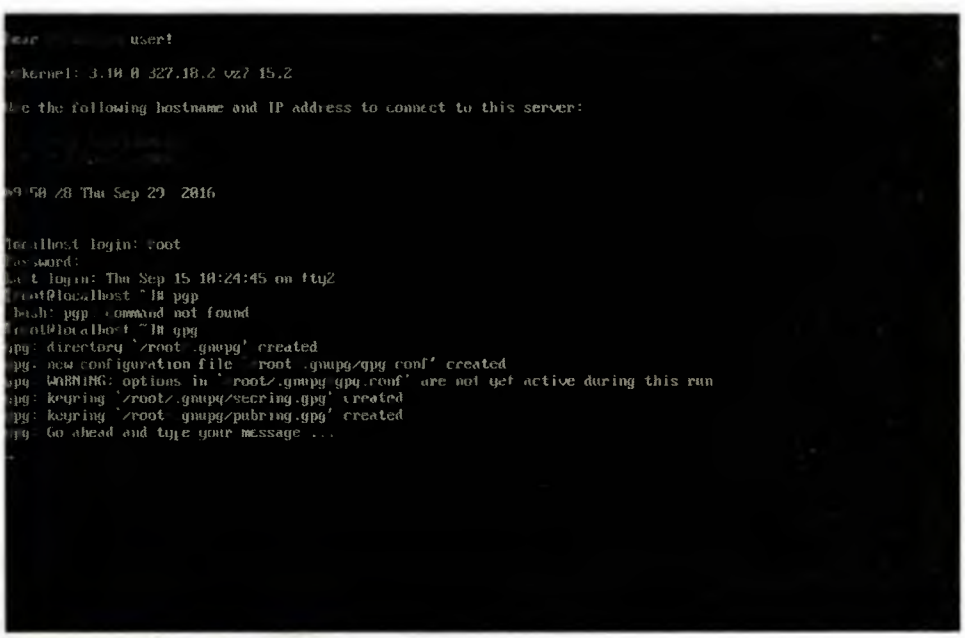


Рис. 4.4. Команда gpg

стью соответствует стандарту OpenPGP и может применяться для проверки подлинности получаемых программ и документов.

Программа входит в состав большинства дистрибутивов и даже устанавливается по умолчанию. Если она не установлена по умолчанию, тогда нужно установить пакет pgp или pgpv. Также можно установить пакеты gpgp и kgpg – это оболочки GnuPG, соответственно, для GNOME и KDE.

Сейчас мы рассмотрим пример использования этой программы. Будем считать, что у нас есть две учетных записи – root и den (имена пользователей могут быть другими в вашем случае).

Войдите в систему как пользователь root, перейдите в домашний каталог и введите команду gpg. На рис. 4.4 показан результат выполнения этой команды. Кстати, обратите внимание, что команды pgp в системе нет, а команда gpg – есть.

Программа просит нас ввести текст. Ничего вводить не нужно, нажмите Ctrl + C. Нам просто нужно, чтобы программа создала в домашнем каталоге все необходимые для нормальной работы подкаталоги.

Теперь нужно сгенерировать ключи. Для этого используется команда gpg --gen-key. Первый вопрос программы – используемый алгоритм (рис. 4.5).

```
[root@localhost ~]# gpg --gen-key
gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Denis
Email address: dhsilabs@gmail.com
Comment: My key
You selected this USER-ID:
    "Denis (My key) <dhsilabs@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? c
Comment: home
You selected this USER-ID:
    "Denis (home) <dhsilabs@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? _
```

Рис. 4.5. Выбор алгоритма шифрования

По умолчанию используется RSA как самый надежный. Есть смысл выбрать именно его.

Вкратце об алгоритмах:

- RSA and RSA – алгоритм RSA будет использоваться для шифрования и подписи.
- DSA and Elgamal – для подписи будет использоваться DSA, Elgamal – для шифрования.
- DSA (sign only) – будет использоваться алгоритм DSA, но только для подписи.
- RSA (sign only) – будет использовать алгоритм RSA, но только для подписи.

После выбора алгоритма программа попросит ввести длину ключа. Учитывая мощность современных компьютеров, минимальная длина ключа должна быть не менее 2048 битов, иначе ваше сообщение относительно быстро расшифруют. По умолчанию как раз используется длина ключа 2048 битов. Допустимая длина ключа варьируется в зависимости от алгоритма. Для RSA допустимые значения – от 1024 до 4096 (1024, 2048, 4096).

Следующий шаг – ввод срока действия ключа:

- – неограниченный срок действия;
- n – ключ действителен n дней;
- <n>w – ключ действителен n недель;
- <n>m – ключ действителен n месяцев;
- <n>y – ключ действителен n лет.

После этого вы увидите дату окончания действия ключа, и программа спросит, все ли правильно. Если все введенные данные верны, нажмите клавишу <Y>.

Далее программа попросит вас ввести ваше имя, адрес e-mail и комментарий для ключа (рис. 4.6).

Следующий шаг – это ввод пароля для ключа. Постарайтесь придумать хороший пароль. В пароле должны быть цифры, символы разного регистра и, желательно, специальные символы.

После ввода пароля и его подтверждения вам предстоит усердно понажимать клавиши на клавиатуре – это необходимо для создания случайных байтов. Нужно ввести как минимум 192 символа (рис. 4.7).



Рис. 4.6. Ввод пароля для ключа



Рис. 4.7. Генерируются случайные байты

Затем вы увидите сообщение, что ключ создан (рис. 4.8).

Самое время экспортировать ключ:

```
$ gpg --export -ao root.asc
```

```
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 3D754C35 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
pub   2048R/3D754C35 2016-09-29
      Key fingerprint = 11B9 C54A 46B6 2ECC 8B75  EFED 06CD 5DDE 3D75 4C35
uid                  Denis (home) <dhsilabs@gmail.com>
sub   2048R/E1F9E7A8 2016-09-29
```

Рис. 4.8. Ключ создан

Полученный таким способом ключ называется открытым ключом. Вам нужно разослать его всем пользователям, с которыми вы планируете обмениваться важной информацией. Можно также выложить его на Web-сайте.

Теперь зарегистрируйтесь под вторым пользователем (den) и аналогичным образом создайте ключ для него. Ключ нужно экспортировать в файл den.asc.

После этого следует обменяться ключами – т. е. ключ пользователя den скопировать в домашний каталог пользователя user2 и наоборот:

```
su
# cp /home/root/root.asc /home/den
# cp /home/den/den.asc /home/root
Затем нужно подписать ключи. От имени первого пользователя
(т. е. пользователя root) введите команду:
gpg --sign den.asc
```

Программа запросит пароль. Нужно ввести пароль, который вы вводили при создании ключа пользователя root.

Войдите в систему как пользователь den и подпишите ключ root.asc:

```
gpg --sign root.asc
```

Теперь проверим, как работает GnuPG. Пока вы находитесь в консоли под именем den, введите команду:

```
echo «Hello, Root» > message.txt
```

Как вы уже догадались, команда создаст файл message.txt. Теперь зашифруем сообщение для пользователя root:

```
[den@localhost den]$ gpg -sear dhsilabs@gmail.com message.txt
```

Вместо электронного адреса адресата можно использовать его фамилию, например,

```
[den@localhost den]$ gpg -sear "Denis" message.txt
```

Программа попросит ввести пароль ключа пользователя den.

Программа зашифрует файл и сохранит его под именем message.txt.asc. Его нужно скопировать в домашний каталог пользователя root и уже от его имени ввести команду:

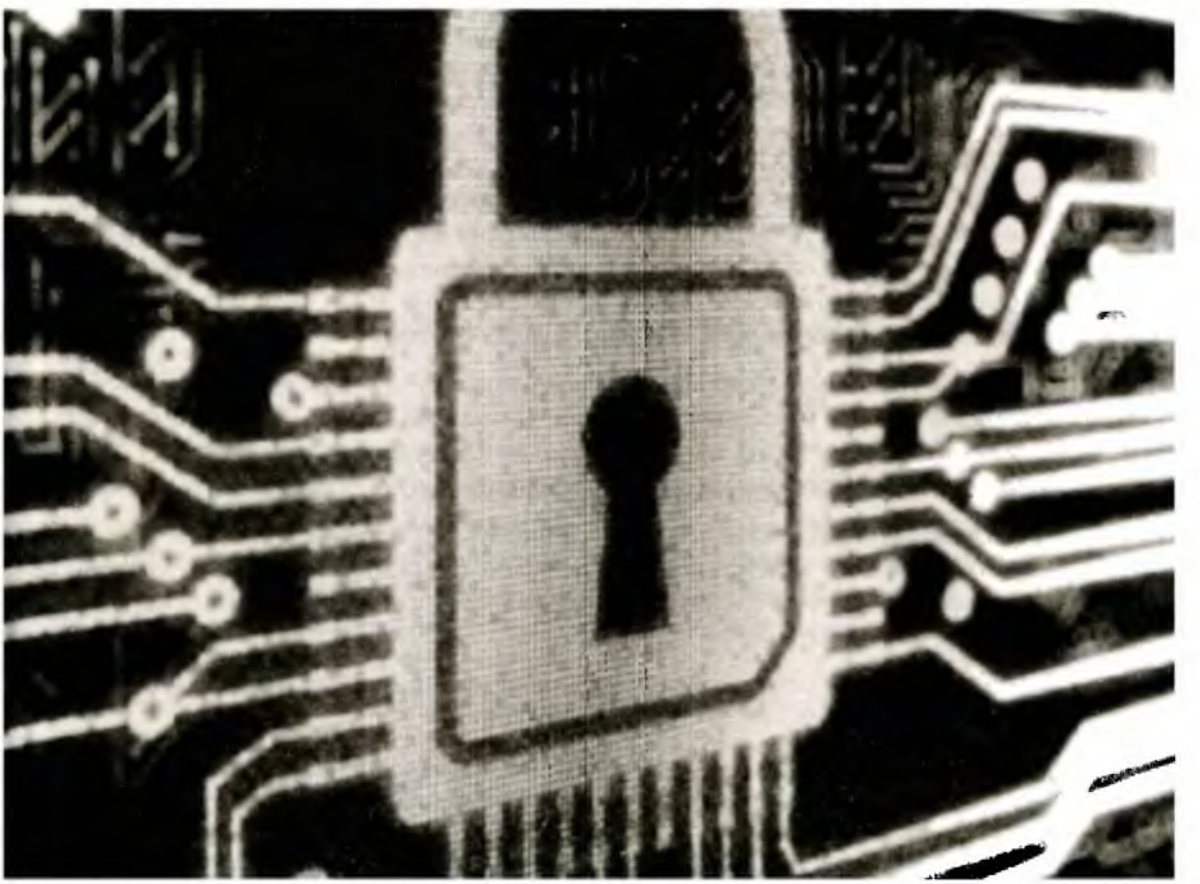
```
gpg -d message.txt.asc > message.txt
```

Программа запросит пароль ключа пользователя root и расшифрует файл. В итоге в домашнем каталоге пользователя root появится файл message.txt с текстом «Hello, Root».

На этом все. Надеюсь, процесс шифрования и подписи документов в Linux оказался не слишком сложным.

Часть 2. Защита передаваемых данных и анонимность в Интернете

Глава 5. Как стать анонимным в Интернете



5.1. Постановка целей

Интернет уже давно не анонимный. За вами следят все – сотовый оператор, интернет-провайдер, поисковая машина, посещаемые сайты и т.д. Все собирают информацию о пользователях. При этом собирается самая разная информация – от IP-адреса до пола, возраста, места нахождения, каких-либо предпочтений (как правило, для отображения подходящей только вам рекламы). Не замечали ли вы, что, например, когда вы заходите на сайт какого-либо интернет-магазина и смотрите необходимый вам товар, то потом в поисковиках и на других сайтах в рекламных блоках появляется реклама именно интересующего вас товара. Магия? Нет, просто тот же Google собирает информацию о пользователях: он «видит» что вы интересовались, скажем, фотоаппаратом Canon, а затем реклама этого фотоаппарата показывается вам в блоках AdWords на разных сайтах.

Если поисковики и различные сайты собирают информацию о пользователях в основном в рекламных целях – чтобы предложить именно то, что вам интересно, и повысить продажи, то провайдеры, сотовые операторы и некоторые другие стороны собирают информацию о вас совсем с другой целью.

Вам надоела тотальная слежка? Тогда нужно подумать о том, как обеспечить анонимность. Но прежде вам нужно задумать, зачем вам нужна анонимность. От ответа на этот вопрос зависит способ обеспечения анонимности.

Вот некоторые основные причины, почему многие задумываются об анонимности:

1. Необходимо разово изменить IP-адрес на любой другой. Цели могут быть разными, например, отладка своего сайта или просто нежелание, чтобы ваш IP-адрес записался в журналы сайта.

2. Необходимо изменить IP-адрес на постоянной основе. Если вы желаете скрывать свой IP-адрес постоянно, тогда этот вариант для вас.
3. Есть необходимость смены IP-адреса на адрес с определенной страны. Не секрет, что некоторые сайты ограничивают доступ к контенту по региону. Регион определяется по IP-адресу. Изменив IP-адрес, вы можете получить доступ к недоступному ранее для вас контенту.
4. Вы хотите скрыть от провайдера и любых третьих лиц, какие сайты вы посещаете, и хотите зашифровать передаваемые по сети данные. Первые три способа обеспечивают просто смену IP-адреса, но ваш провайдер будет видеть, какие узлы вы посещаете. Если вы совершите что-то незаконное, то вас будет относительно просто отследить. В этом случае отслеживание конечного пользователя становится довольно непростой задачей.
5. Есть необходимость не только скрыть от провайдера HTTP-трафик, но и любой другой передаваемый трафик. Другими словами, вы хотите защитить не только информацию, передаваемую по протоколу HTTP (сайты), но и почту, сообщения в мессенджерах и т.д.

5.2. Выбор способа обеспечения анонимности

5.2.1. Разовое сокрытие IP-адреса и анонимайзеры

Теперь разберемся, какой способ лучше всего подходит для вас. Если вам нужно разово скрыть IP-адрес, то лучше всего подойдет сайт-анонимайзер, например, https://2ip.ru/anonim/.

Работает он так: вы заходите на сайт и вводите адрес сайта, который хотите посетить анонимно. Сценарий на анонимайзере получает введенный пользователем адрес, получает запрошенную пользователем веб-страницу и отображает ее в браузер. Получается, что пользователь видит то же самое, как если бы он зашел без анонимайзера, но при этом сайт «видит» IP-адрес не пользователя, а анонимайзера.

К достоинствам анонимайзеров можно отнести простоту использования. Просто ввел веб-адрес и скрыл свой IP. Если разово нужно скрыть свой адрес – это оптимальный вариант.

Однако у них есть и недостатки. Первый – не обеспечивается защита передаваемых данных. Ваши данные передаются по сети все еще «как есть», то

есть в открытом виде (конечно, если «на том конце» не используется https). Второй – не всегда можно выбрать IP-адрес нужной страны. На сайте https://2ip.ru/anonim/, например, возможен выбор страны, поэтому он подойдет для способов 1 и 3 (если нужная страна есть в списке).

Третий – анонимайзеры не предоставляют никаких гарантий, что не собирают информацию о вас и не передают третьим лицам. То есть сам анонимайзер может шпионить за вами. Именно поэтому анонимайзеры нельзя использовать, если вам нужна анонимность и безопасность. Да и ваш провайдер будет все равно видеть, какие сайты вы посещаете, поскольку введенный вами адрес обычно передается в качестве параметра URL сайта анонимайзера.

5.2.2. Постоянное сокрытие IP-адреса и анонимные прокси

Для постоянного сокрытия IP-адреса можно использовать анонимные прокси-серверы. Списки таких серверов постоянно публикуются в Интернете. Все, что вам нужно сделать, – найти такой прокси-сервер и указать его в настройках вашего браузера. Например, в Google Chrome для этого нужно выполнить следующие действия:

1. Откройте меню браузера.
2. Выберите команду **Настройки.**
3. Перейдите по ссылке **Показать дополнительные настройки** внизу окна.
4. В разделе **Сеть** нажмите кнопку **Изменить настройки прокси-сервера** (рис. 5.1).
5. Появится окно, которое также можно вызвать из Панели управления – **Свойства: Интернет**.
6. Нажмите кнопку **Настойка сети**. В появившемся окне отметьте флажок **Использовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений)**.
7. Введите IP-адрес прокси-сервера и его порт. Как правило, порт указывается в списке прокси или в отдельной колонке или через двоеточие, например, 192.168.2.100:3128 (здесь 3128 – номер порта). Стандартные номера портов для прокси: 3128, 8080

О том, как настроить другие браузеры, вы сможете прочитать в руководстве по этим браузерам или найти соответствующие инструкции в Интернете.

К преимуществам анонимных прокси можно отнести то, что в отличие от анонимайзера, вы уже не забудете зайти на очередной сайт без анонимайзе-



Рис. 5.1. Параметры Google Chrome

ра, – доступ ко всем сайтам будет осуществляться через анонимный прокси, следовательно, ни один из посещаемых вами сайтов не увидит ваш реальный IP-адрес.

Недостатков у этого способа довольно много. Во-первых, ваши данные все еще могут быть перехвачены, поскольку использование анонимного прокси не означает шифрование передаваемых данных. Во-вторых, сегодня прокси-сервер может работать, а завтра – нет. Дело в том, что обычно анонимные прокси – это плохо настроенные прокси-серверы, которые позволяют подключаться к ним всем пользователям. Рано или поздно администратор обнаружит ошибку в конфигурации и закроет доступ.

В-третьих, скорость доступа будет низкой. Анонимный прокси может находиться очень далеко, да и его пропускной канал никак не рассчитан на то, что к нему будут обращаться тысячи пользователей, которые нашли его IP-адрес в списке анонимных прокси.

В-четвертых, страну изменить никак не выйдет. Например, если вы нашли анонимный прокси-сервер во Франции, а вам нужен немецкий IP-адрес, то изменить IP не выйдет – у вас всегда будет французский IP (пока вы не найдете немецкий прокси-сервер).

Но самый большой недостаток в следующем: не все то золото, что блестит, так и не всякий прокси, к которому вы можете подключиться, анонимный. Некоторые прокси передают узлу в заголовках запроса ваш IP-адрес. К тому же нет никакой гарантии, что такие прокси не ведут журнал посещений и не передают эту информацию третьим лицам.

В общем, перед использованием анонимного прокси нужно убедиться, является ли он анонимным. Подключитесь к своему сайту и посмотрите, какие заголовки передает прокси-сервер сайту. Если обнаружите свой IP-адрес, ищите другой прокси. К тому же при использовании анонимных прокси-серверов я бы порекомендовал использовать открытые DNS-серверы или программы вроде DNSCrypt – программы для шифрования DNS-трафика[1]. Ведь провайдер все равно сможет узнать, к каким узлам вы обращались, исследовав ваш DNS-трафик. А так его можно будет зашифровать или же использовать публичные DNS-серверы 8.8.8.8 и 8.8.4.4. Чем меньше информации вы отдаете провайдеру, тем лучше.

5.2.3. Изменение региона, сокрытие IP и шифрование данных

Представим, что вы уехали в отпуск в другую страну, пытаетесь просмотреть новости, но сайт телеканала сообщает, что видео недоступно для вашего региона. Решить эту проблему можно несколькими способами:

- Найти анонимный прокси, находящийся в «целевой» стране.
- Использовать сеть Tor: в настройках можно выбрать IP-адрес из любой страны.
- Использовать VPN-сервис.

С анонимным прокси все понятно из предыдущего раздела. А вот сеть Tor и VPN – это новые способы обеспечения анонимности.

Оба способа обеспечивают смену IP-адреса, при том что есть возможность выбора целевой страны. Кроме простой смены IP-адреса и Tor, и VPN шифруют передаваемые данные.

При использовании этих способов:

- Удаленный сайт никогда не узнает ваш IP-адрес.
- Провайдер не узнает, какие сайты вы посещали.
- Третья сторона не сможет перехватить передаваемые данные. Точнее, перехватить-то сможет, но они будут в зашифрованном виде.

1 http://www.dkws.org.ua/index.php?page=show&file=a/hacker/dnscrypt/dnscrypt

Сеть Tor является оптимальной для случаев 2, 3 и 4. Для случая 5 тоже можно использовать сеть Tor, однако с некоторыми оговорками. Когда происходит подключение к VPN-сервису, весь трафик всех сетевых программ, будет передаваться внутри VPN-канала, то есть весь трафик будет защищен. В случае с Tor, защищены будут только те программы, которые получится настроить на использование Tor, то есть как минимум указать адреса прокси-серверов. Но некоторые программы нельзя «торифицировать». Подробно об этом мы поговорим в следующей главе, а об VPN-сервисах – в главе 7.

С другой стороны, если вам нужна определенная страна, то не всегда получится найти VPN-сервис, который бы позволил выбрать сервер, находящийся в той стране. В этом случае проще использовать Tor, поскольку его сеть более развита (рис. 5.2). Далее мы рассмотрим эти оба способа более подробно, поэтому не волнуйтесь – вы сможете выбрать оптимальный для себя способ.

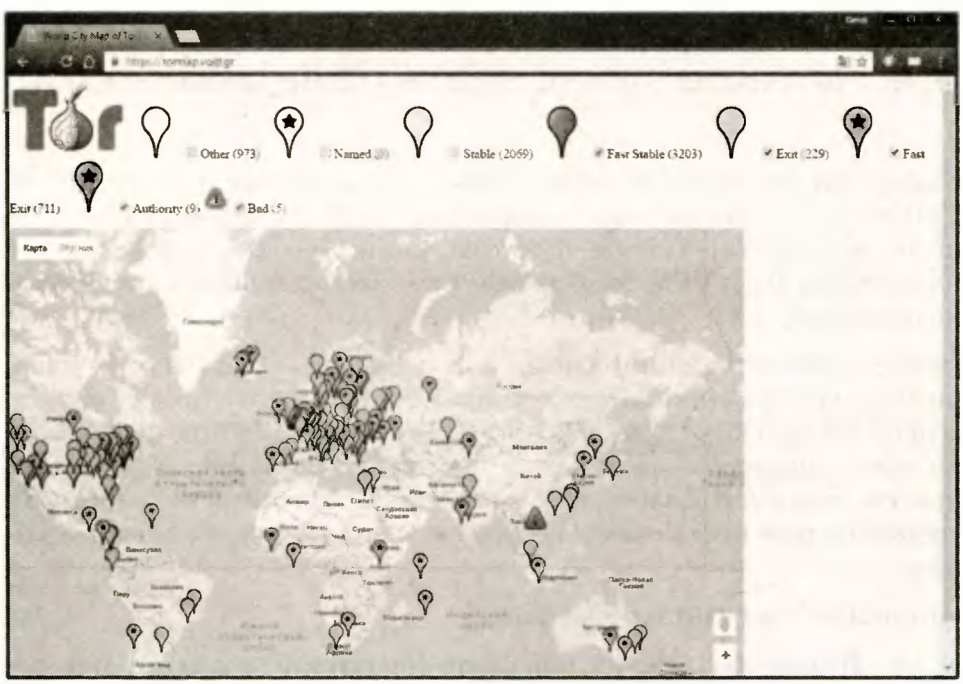


Рис. 5.2. Карта сети Tor (2016 г.)

5.3. Подводим итоги

Подведем итоги по способу обеспечения анонимности:

- Случай 1 – анонимайзер.
- Случай 2 – анонимный прокси (не самый лучший выбор).
- Случаи 2 – 4 – сеть Tor или VPN-сервис.
- Случай 5 – VPN-сервис.

Пока вы не перешли к чтению следующей главы, нужно отметить, что VPN-сервисы, как правило, платные. Вы платите или за используемый трафик, или за время использования (день, неделя, месяц, год) сервиса. Сеть Tor абсолютно бесплатна. Если платить не хочется, то нужно использовать Tor, только перед этим вам нужно знать некоторые нюансы Tor, о которых мы поговорим в следующей главе. В ней же будет приведено сравнение Tor и VPN, чтобы вы могли окончательно определиться с выбором средства защиты от слежки.

5.4. Что еще нужно знать об анонимности

Разберемся, что еще может стать угрозой для анонимности пользователя. Если оборудование провайдера, журналы удаленного сайта и злоумышленников, которые перехватывают трафик, можно «обойти» с помощью использования Tor и VPN, то об одной угрозе часто забывают – это браузер пользователя.

Браузер собирает и хранит данные о пользователе – кэш (по сути, копии страниц и изображений, которые загружал пользователь), Cookies, пароли, журнал посещенных страниц. Все это поможет «рассекретить» пользователя, если компьютер попадет в руки третьих лиц (сценарий, когда на компьютере будет установлена программа-шпион, которая может передавать третьей стороне информацию о действиях пользователя, мы не рассматриваем).

Что делать? А вариантов несколько:

- Использовать режим инкогнито (приватный режим). В этом режиме не сохраняется история, Cookies, пароли и другая служебная информация. Однако помните, что использование этого режима не освобождает вас от использования средства обеспечения анонимайзера вроде VPN-сервиса или анонимного прокси. Поскольку про-

вайдер или администратор вашей локальной сети все равно сможет увидеть посещенные вами узлы.

- Периодически очищать кэш и историю браузера. Например, в Google Chrome для этого нужно нажать Ctrl + Shift + Del, выбрать все доступные пункты и нажать кнопку **Очистить историю** (рис. 5.3).
- Использовать браузер Tor – этот браузер не собирает и не хранит никакой информации о пользователях.

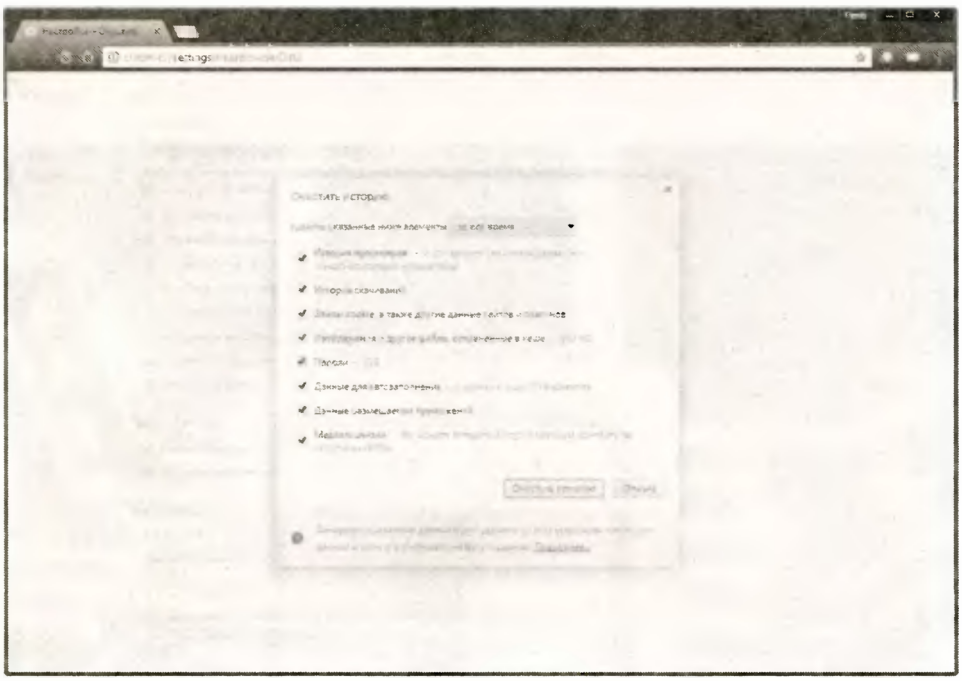
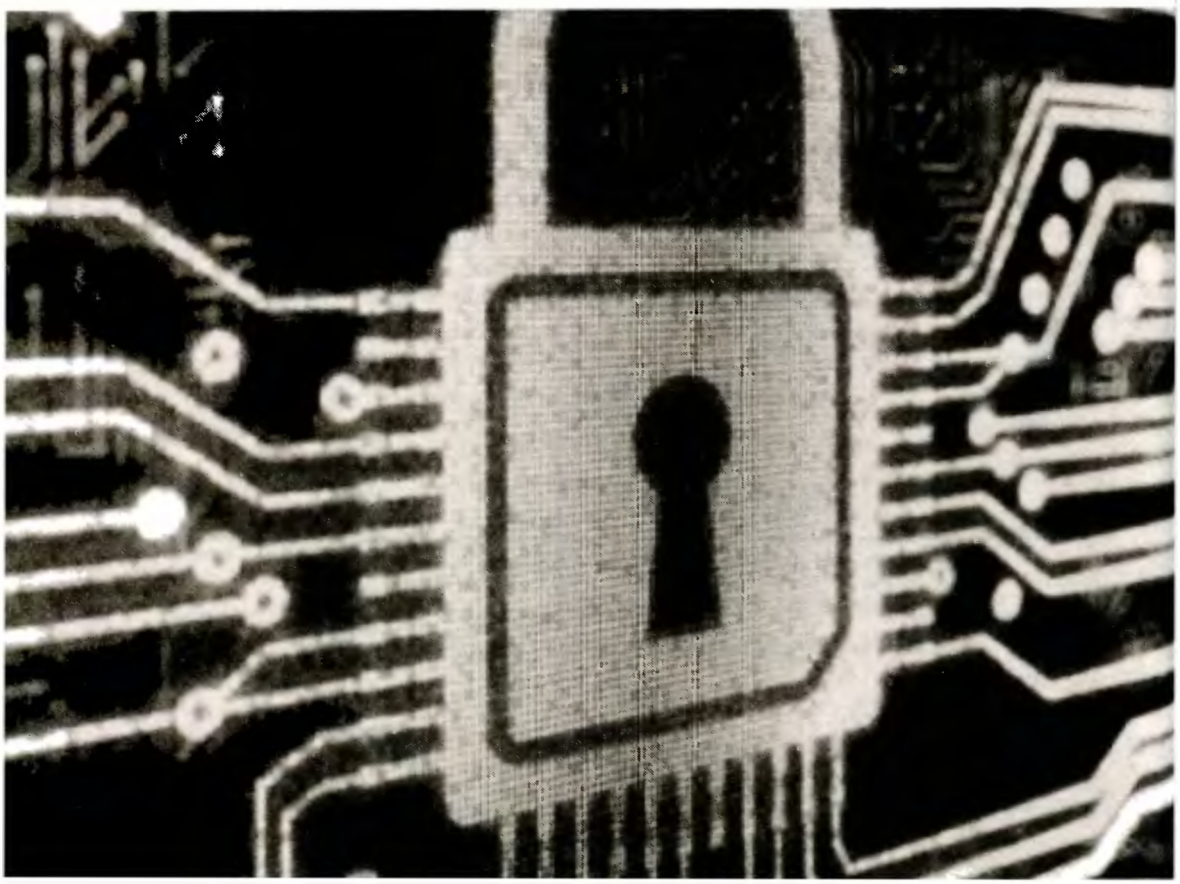


Рис. 5.3. Очистка истории в Google Chrome

Глава 6.

Проект Tor



6.1. Принцип работы Tor

Использовать Tor очень просто, именно поэтому само использование будет рассмотрено в самом конце этой главы. Важно разобраться, как работает Tor, в каких случаях он поможет, а в каких – нет.

Представим, что нам нужно не только скрыть свой IP-адрес от удаленного узла, но и выполнить следующие «задачи»:

- Сменить свой IP-адрес так, чтобы он выглядел как IP-адрес из определенной страны.
- Скрыть посещаемые узлы от глаз администратора вашей сети или провайдера.
- Обойти брандмауэр корпоративной сети, запрещающий посещение тех или иных сайтов (например, сайтов социальных сетей).
- Зашифровать передаваемые данные, защитив их тем самым от перехвата.

Именно для решения всех этих задач и была создана сеть Tor (The Onion Router). Проект Tor – это бесплатное и свободно распространяющееся программное обеспечение для анонимизации трафика. Исходный код Tor открыт, поэтому каждый желающий может проверить отсутствие черных ходов для спецслужб – их нет. Однако у Tor есть некоторые недостатки и ограничения, о них мы поговорим позже.

Сет Tor обеспечивает анонимизацию и защищает пользователя от слежки – как удаленного сайта, так и провайдера/сотового оператора. Все передаваемые по сети Tor данные шифруются, что исключает прослушивание.

Рассмотрим принцип работы. Сеть Tor состоит из множества узлов. При подключении к сети Tor автоматически выбирается начальный узел и вся

дальнейшая цепочка узлов, в том числе и выходной узел. Пусть вы подключились к узлу А. Вы передаете ему свои данные – а именно адрес узла, который вы хотите посетить, и, возможно, другую информацию. Узел А передает эту информацию узлу Б, тот, в свою очередь, узлу В и т.д. В конечном счете данные будут переданы последнему узлу (выходному узлу) в цепочке, а тот уже передаст их конечному узлу – сайту, который вы хотите просмотреть.

Обратите внимание, что:

- В самом начале (еще до передачи данных узлу А) вся информация шифруется и далее уже передается в зашифрованном виде. Расшифровка происходит на выходном узле. На участке от выходного узла до сайта назначения информация передается в незашифрованном виде. Но, как правило, попытки перехвата (оборудованием провайдера или злоумышленником, который хочет перехватить именно ваши данные) происходят в начале цепочки (от компьютера до узла А), а там они уже зашифрованные.
- Обратно информация передается также в зашифрованном виде и по той же цепочке. Расшифровка происходит уже на локальном компьютере.
- Ни один узел в цепочке, кроме узла А (первый узел), не знает ваш IP-адрес. Начиная с узла Б, все узлы в качестве источника данных видят только IP-адрес предыдущего узла, а в качестве получателя – IP-адрес следующего узла. Другими словами, ни один из узлов в цепочке даже не знает, кто вы и какой сайт вы хотите открыть.
- Поскольку вы обращаетесь к узлу А (первый узел цепочки Tor), а не к сайту напрямую, то это позволяет обойти брандмауэр локальной сети. Ведь вы подключаетесь не к facebook.com, а к какому-то узлу с IP-адресом вроде 185.56.34.11 (первый адрес, который пришел в голову). Администратор физически не сможет запретить все узлы Tor. А запрещать доступ именно к этому узлу (185.56.34.11) нет смысла, поскольку при следующем подключении будет выбран другой узел.
- Сайт, который вы хотите посетить, видит только IP-адрес последнего (выходного) узла цепочки, ваш IP-адрес не увидит ни сайт назначения, ни даже сам выходной узел.
- Теоретически возможен перехват трафика на участке от последнего (выходного) узла до сайта назначения. Но в этом случае нужно проследить всю цепочку Tor, а она может состоять из десятков узлов, – с технической точки зрения сделать это довольно сложно. Если вы хотите сделать перехват трафика на этом участке невозможным, используйте HTTPS-версию сайта, если она, конечно, доступна.

- В процессе работы с Tor вы можете сменить цепочку, например, если скорость передачи данных по текущей цепочке мала и сайты открываются медленно.
- Вы можете выбрать страну, в которой находится выходной узел.

6.2. Что лучше – Tor или VPN?

В принципе, все, что предлагает Tor, можно получить и с помощью VPN: и шифрование трафика, и сокрытие своего IP-адреса, и обход брандмауэра местной сети. Так что лучше использовать – VPN или Tor?

Огромное преимущество VPN заключается в следующем. При подключении к VPN весь трафик всех приложений будет проходить через VPN, чем гарантируется еще большая анонимность. В случае с Tor нужно настраивать каждое сетевое приложение на работу с Tor. Подробные инструкции по настройке того или иного приложения на Tor можно найти в Интернете. Но все равно у Tor есть ограничения, а именно:

- Нельзя загружать торренты через Tor. Дело в том, что Torrent-клиенты, даже если они настроены на Tor, все равно делают прямые соединения. В трекер-запросе GET клиент все равно отправляет ваш реальный IP-адрес.
- Нельзя использовать плагины браузера вроде Flash, RealPlayer, Quicktime – они могу обойти Tor и соединиться напрямую. Именно поэтому данные плагины не работают в Tor Browser.

В случае с VPN всех этих проблем у вас нет. Вы можете запускать любое сетевое программное обеспечение – торренты, Skype, Viber, почтовые клиенты, и весь трафик будет идти через VPN-соединение. Еще к преимуществам VPN можно отнести скорость доступа. Практически скорость вашего Интернета будет такой же, как в случае с обычным соединением. А вот сеть Tor будет более медленной. Конечно, для просмотра сайтов ее пропускной способности более чем достаточно, но раньше ее скорость оставляла желать лучшего. Это связано с тем, что первый узел цепочки Tor может быть географически далеко от вас. В крайнем случае, можно сменить цепочку – далее будет показано, как это сделать.

Но у VPN есть и недостатки. Прежде всего, все VPN-сервисы платные. Так, за PIA, который будет рассмотрен в следующей главе, нужно платить 3.33 доллара в месяц (при оплате за год), и это еще сравнительно дешево. Есть и более дорогие сервисы. Проект Tor бесплатен. Вообще бесплатен. Вам не нужно за него платить.

Есть и второй недостаток VPN. Многие VPN-сервисы работают в рамках Digital Millennium Copyright Act, а это означает, что если вы будете использовать VPN в противозаконных целях, информация о вас будет передана куда следует. Отсюда можно сделать вывод, что все VPN-сервисы следят за своими пользователями.

Окончательное решение, конечно же, будет за вами. Если вы не собираетесь совершать ничего противозаконного, а лишь хотите избавиться от слежки со стороны провайдера и готовы платить за это деньги, то можете выбрать VPN. Лично я предпочитаю использовать Tor со всеми его недостатками и достоинствами. Во-первых, бесплатно. Во-вторых, никакой слежки.

6.3. Комбинируем VPN и Tor

При желании трафик Tor можно пустить через VPN-соединение. То есть вы сначала устанавливаете VPN-подключение, а затем запускаете Tor. Такая комбинация может использоваться, если вы хотите скрыть свою активность от администраторов VPN-сервиса. Однако следует учитывать особенности использования Tor: нужно настроить используемые приложения на Tor и отказаться от использования некоторых специфических приложений вроде Torrent-клиентов.

Но в этом случае теряется все удобство использования VPN-сервиса. Хотя при желании вы можете организовать и такой режим работы. Подробно о нем рассказано в следующей статье:

https://habrahabr.ru/post/204266/

6.4. Что делать с DNS-трафиком?

Необходимо позаботиться и о DNS-трафике. Не забывайте, что его тоже нужно защитить. Часто ваши DNS-запросы оказываются незашифрованными и отправляют как есть. Выходит, ваш провайдер не сможет просмотреть, какие данные вы передаете, но может просмотреть, какие сайты вы посещаете. Поэтому нужно позаботиться о защите вашего DNS-трафика.

Самый простой способ – настроить DNS на использование серверов Google – 8.8.8.8 и 8.8.4.4. В этом случае трафик хотя бы не будет проходить через DNS провайдера, и если не использовать средства перехвата трафика, то отследить вас через DNS провайдера будет невозможно. Но если идет глобальный перехват трафика, то все равно трафик DNS, хоть и к серверам Google, все равно будет незащищенным. Так что это нельзя назвать защитой.

Второй способ – это использовать программу DNSCrypt, об этом вы можете прочитать в следующей статье:

http://www.dkws.org.ua/index.php?page=show&file=a/hacker/dnscrypt/dnscrypt

Третий способ – использовать операционную систему Whonix. В ней все торифицировано, в том числе и DNS-трафик, который перенаправляется на DNS-порт Tor. Вообще, Whonix – это «заточенный» под анонимность дистрибутив Linux. Познакомиться с ним можно по адресу:

https://www.whonix.org/

6.5. Использование Tor

Скачать Tor можно по адресу:

https://www.torproject.org/download/download-easy.html.en

Скачайте инсталлятор Tor – он будет установлен на ваш рабочий стол (по умолчанию). При первом запуске нужно будет выбрать, как подключаться к сети Tor (рис. 6.1). В большинстве случаев нужно просто нажать кнопку **Соединиться**. Потом сетевые параметры можно будет изменить.



Рис. 6.1. Сетевые настройки Tor

Далее нужно подождать, пока будет выполнено подключение к сети Tor (рис. 6.2). Если провайдер не блокирует Tor, то подключение пройдет довольно быстро. После этого будет запущен браузер Tor (рис. 6.3).

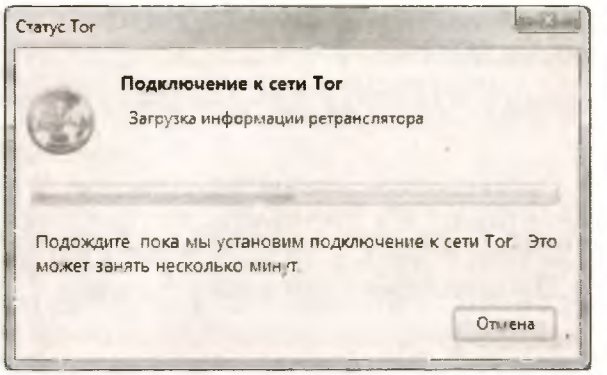


Рис. 6.2. Подключение к Tor



Рис. 6.3. Браузер Tor

После этого можно начинать использование браузера, как обычно – трафик будет анонимизирован. Но так не интересно. Давайте проверим ваш IP-адрес. Откройте страницу https://geoiptool.com/ru/. Вы увидите свой текущий IP-адрес – именно этот адрес увидят все узлы, к которым вы будете подключаться по протоколам HTTP/HTTPS (рис. 6.4). Также откройте любой другой браузер и тоже откройте эту страницу. В любом другом браузере будет показан ваш реальный IP-адрес – это доказательство тому, что любой трафик, кроме того, который идет через Tor, не защищен.

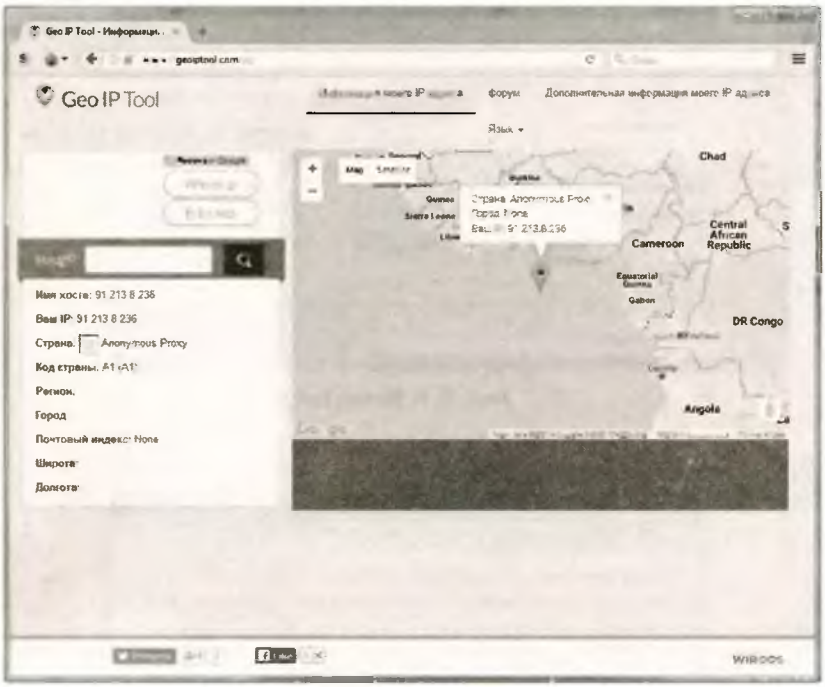


Рис. 6.4. Ваш новый IP-адрес – 91.213.8.236

Теперь вернитесь в окно Tor Browser и нажмите луковицу (рис. 6.5). Во-первых, вы увидите цепочку Tor для этого сайта – первые два узла находятся в США, третий – в Украине.

Команды меню следующие:

- **Новая личность** – браузер Tor будет перезапущен, для всех теперь вы – абсолютно новый пользователь.
- **Новая цепочка Tor для этого сайта** – если вы не хотите перезапускать браузер, а хотите сменить цепочку, например, потому что текущая работает медленно или есть необходимость поменять конечный IP-адрес.
- **Настройки сети Tor** – открывает сетевые настройки, где вы сможете сконфигурировать Tor, если провайдер блокирует Tor или же компьютеру нужен локальный прокси для доступа к Интернету (рис. 6.6). Также это окно поможет, если брандмауэр позволяет подключаться только к определенным портам. В этом случае можно пустить трафик Tor через эти порты, например, через 80 и 443 – эти порты, как правило, всегда открыты.

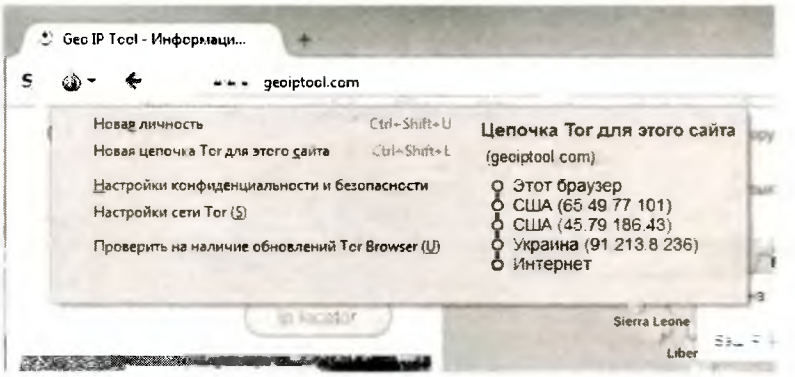


Рис. 6.5. Меню Tor

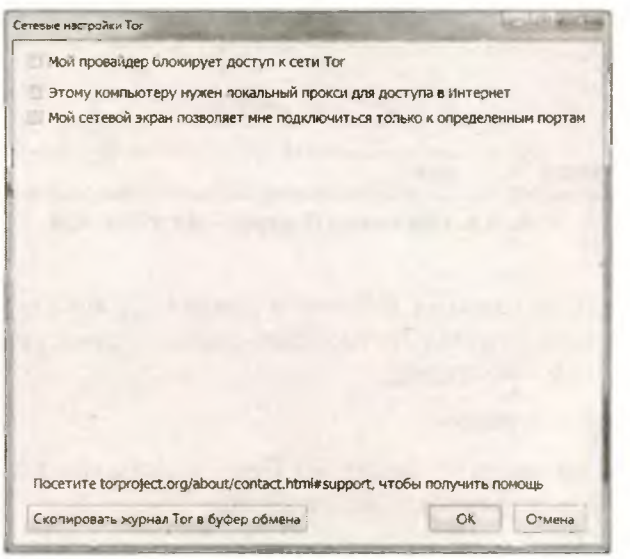


Рис. 6.6. Настройки Tor

- **Настройки конфиденциальности и безопасности** – открывает одноименное окно. В нем можно установить настройки конфиденциальности, но как правило, здесь ничего изменять не нужно – по умолчанию не сохраняется ни история посещений, ни Cookies, блокируются расширения браузера и изменяются сведения, отличающие вас от других пользователей Tor (рис. 6.7).

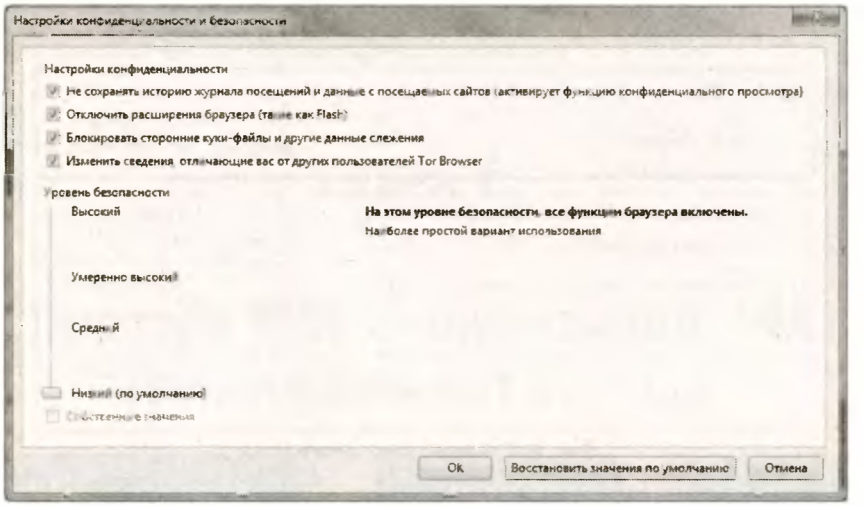


Рис. 6.7. Настройки конфиденциальности

Теперь разберемся, как изменить выходной узел. Предположим, вы уехали в отпуск и хотите просмотреть местные новости, а сайт телеканала сообщает, что видео недоступно для просмотра в вашем регионе. Изменить выходной узел просто. Откройте файл конфигурации C:\Users\<Имя>\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\torrc (путь может отличаться у вас, если вы установили Tor в каталог, отличный от предлагаемого по умолчанию) и добавьте в него строчку:

ExitNodes {код страны}

Например:

ExitNodes {ru}

После этого перезапустите браузер и просмотрите цепочку Tor. Как видите (рис. 6.8), теперь конечный узел будет расположен в России.

В следующей главе мы рассмотрим, как использовать популярный VPN-сервис PIA.

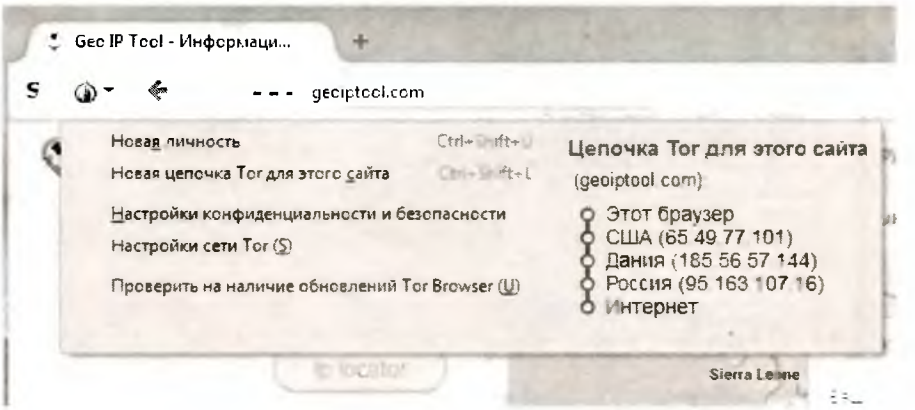
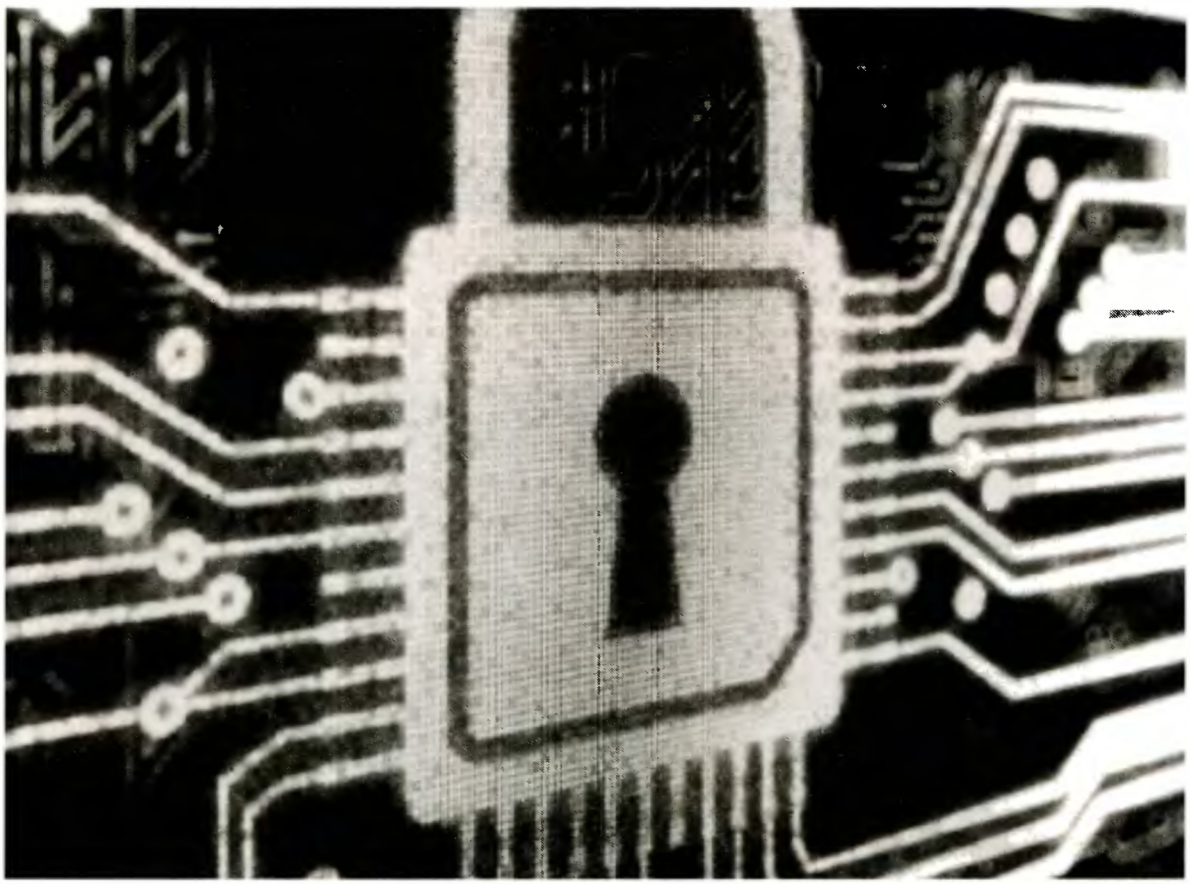


Рис. 6.8. Смена выходного узла

Глава 7.

Простой VPN-анонимайзер: PIA (Private Internet Access)



7.1. Как работает PIA

В прошлой главе были объяснены преимущества и недостатки VPN-сервисов, поэтому повторяться не стану. PIA, или Private Internet Access понравится начинающим пользователям: установил, выбрал «точку выхода» (конечный узел, который будут «видеть» посещенные вами узлы), и всё – вы защищены.

Больше ничего не нужно настраивать – ни сам VPN, ни сетевые приложения. Все передаваемые вами данные будут зашифрованы, провайдер ничего не увидит, любые третьи лица ничего не увидят, а конечные узлы (к которым вы обращаетесь) будут видеть не ваш IP-адрес, а тот, который вы выбрали при подключении.

Не нужно забывать, что PIA – это платный сервис, поэтому при его использовании главное – не забыть вовремя пополнять свой аккаунт, иначе вы не сможете пользоваться сервисом.

7.2. Как установить PIA

Перейдите по адресу https://rus.privateinternetaccess.com/pages/downloads и скачайте клиент для Windows (рис. 7.1). Запускать установочный файл pia-v65-win.exe нужно от имени администратора. Лучше всего откройте командную строку с правами администратора (нажмите Win + Z и найдите соответствующую команду в появившемся меню) и запустите установку из командной строки – так вы будете видеть процесс установки.

В процессе установки вам нужно будет нажать кнопку **Установить** в запросе на установку программного обеспечения (рис. 7.3).

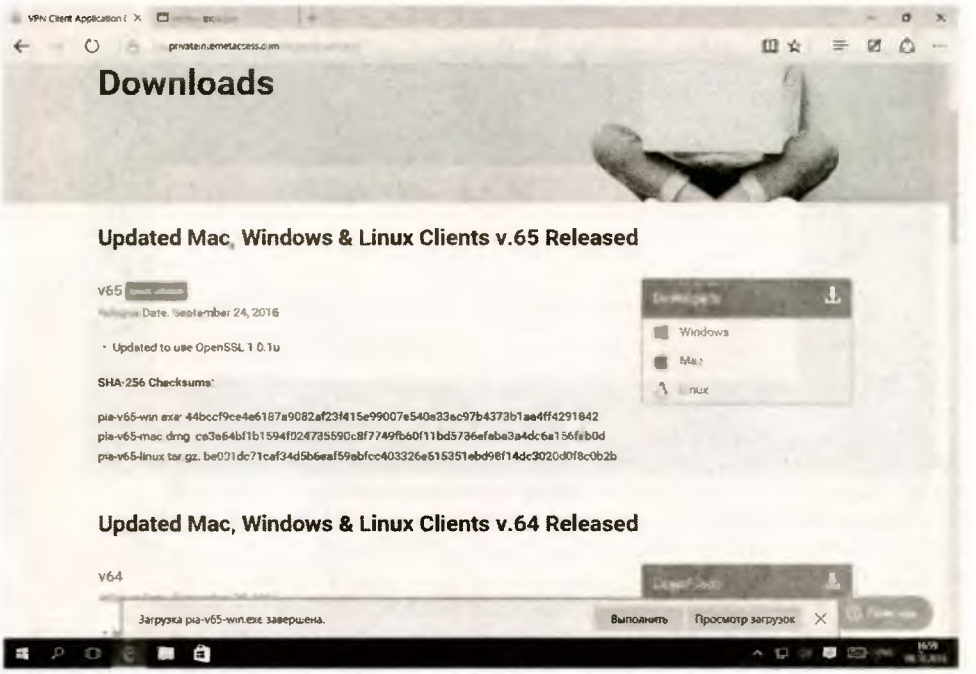


Рис. 7.1. Клиент загружен

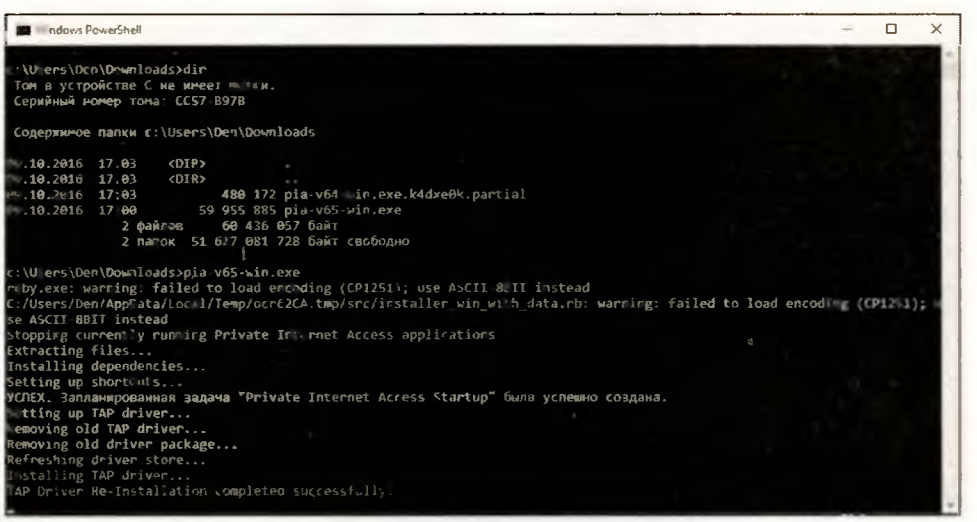


Рис. 7.2. Процесс установки

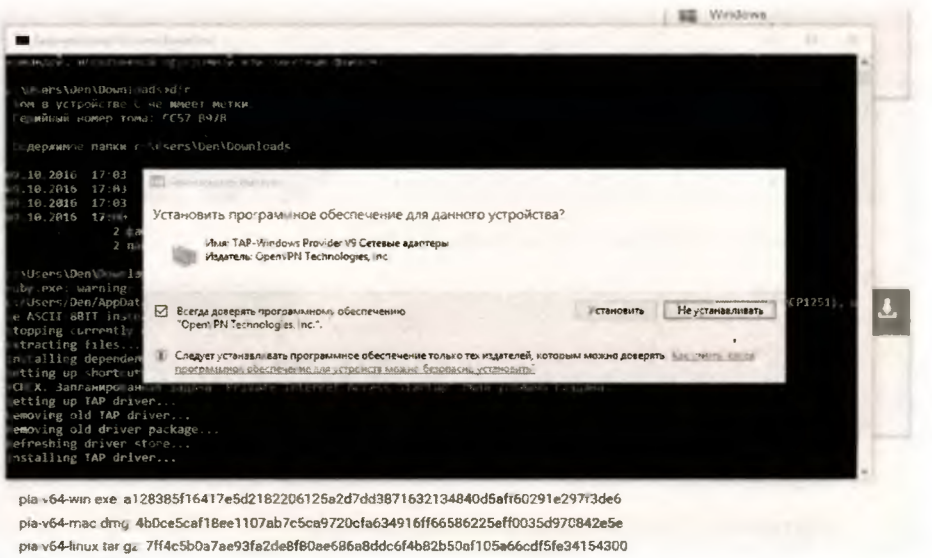


Рис. 7.3. Нажмите кнопку Установить

После установки будет открыто окно, в котором нужно ввести логин и пароль, полученные при регистрации на сайте https://rus.privateinternetaccess.com. Зарегистрироваться на сайте можно во время установки клиента.

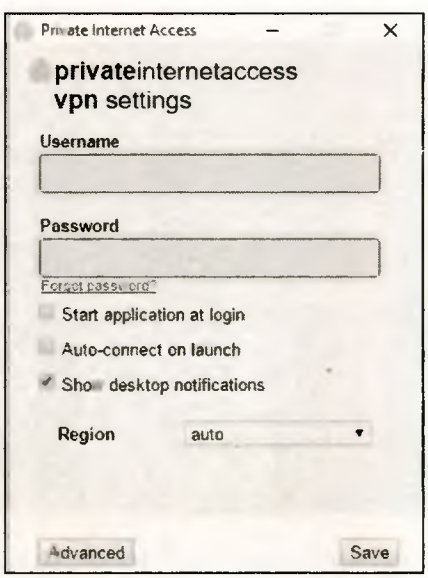


Рис. 7.4. Окно входа

Если хотите использовать PIA постоянно, отметьте флажки **Start application at login** и **Auto-connect on launch**. Первый флажок включит запуск приложения при входе в систему, а второй – обеспечит автоматическое подключение к VPN-серверу.

7.3. Использование PIA

Собственно, если вы отметили те два флажка, то вам уже больше ничего не нужно делать. Можно открывать браузер и другие сетевые программы и анонимно использовать Интернет.

Примечание. Преимущество Tor в том, что каждый новый запуск браузера создает новую личность – браузер Tor не сохраняет ни Cookies, ни пароли, ни историю – в отличие от обычных браузеров, которые вы будете использовать с PIA. По хранящимся в браузере данным вас можно будет «вычислить». Именно поэтому я рекомендую или очистить все хранимые в браузере данные, или же установить другой браузер и использовать его только тогда, когда работаете через VPN.



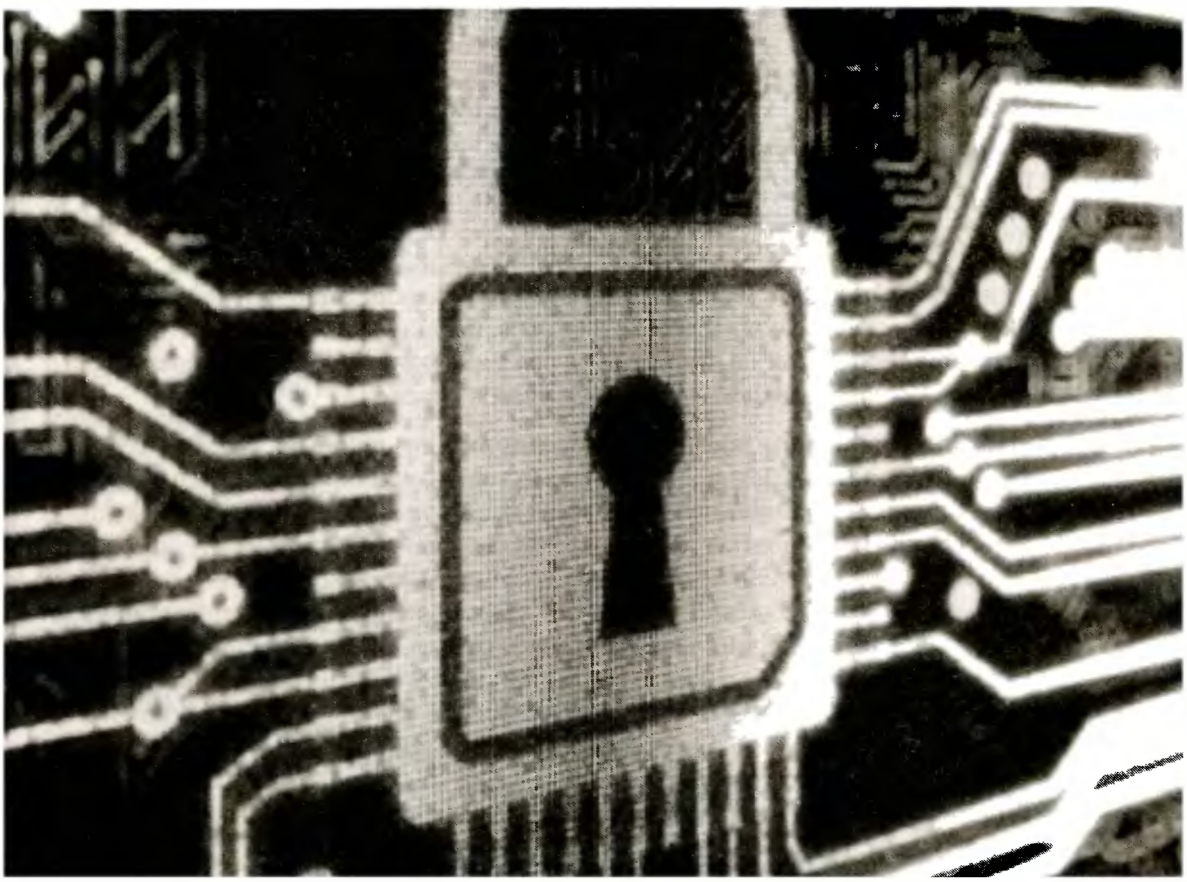
Рис. 7.5. Подключение к VPN

Если вы не хотите, чтобы PIA подключался автоматически, тогда подключаться придется вручную. В области уведомлений найдите значок PIA и выберите VPN-сервер, к которому вы хотите подключиться, например, US Texas. После подключения все будут думать, что вы находитесь в Техасе.

Если в списке вы не нашли нужного вам VPN-сервера, используйте команду More, чтобы получить дополнительные варианты.

Глава 8.

Защита от вирусов в Интернете



Сначала небольшой экскурс в антивирусные продукты. Если помните, раньше были только антивирусы-сканеры. Вы запускаете программу, она сканирует все файлы на жестком диске, и если находит вирус, предлагает его вылечить (если это возможно) или удалить файл. Затем появились программы-мониторы. Если сканер не предлагает защиты в реальном времени, то такая возможность появилась в программах-мониторах. Если вы запустите вирус, то сканер не сможет его определить до запуска самого сканера. А монитор может распознать вирус и заблокировать его запуск. Обычно при этом пользователь видит запрос, что сделать с вирусом – поместить в карантин, в исключение, вылечить, удалить и т.д.

Современный классический антивирус как раз и представляет собой модули сканера и монитора. Также может быть проактивная защита – это когда антивирус не уверен на 100%, что перед ним вирус, но по поведению программы может определить, что она является опасной.

Однако современные вирусы уже давно вышли за пределы исполнимых файлов Windows. Теперь есть и сетевые вирусы (как правило, распространяются по электронной почте), и вирусы, загружаемые с интернет-сайтов, и др. Особую опасность представляет незащищенное интернет-соединение – по нему пользователь может загрузить вирусы и другие вредоносные программы. Конечно, они при запуске могут быть распознаны монитором, но лучше избавиться от них еще на этапе загрузки на компьютер – не доводя до их запуска. Новые типы угроз породили новые типы антивирусных продуктов – Internet Security. Такие продукты включают в себя брандмауэр (раньше для более качественной защиты приходилось устанавливать два продукта – антивирус и брандмауэр, так как стандартный брандмауэр Windows хоть и весьма хорош, но не дотягивает до специальных решений), а также модули, позволяющие защитить ваш компьютер от различных типов сетевых угроз.

В данной главе мы попытаемся выбрать самый качественный IS-продукт. Мы не будем описывать, как использовать тот или иной продукт, – это очень тривиально. По сути, IS используются по принципу – установил и забыл. Такие продукты работают в фоне и обеспечивают безопасность компьютера. Если будет необходимо вмешательство пользователя, например, будет обнаружен вирус, то пользователь увидит соответствующий запрос. Обновление продуктов тоже осуществляется автоматически, главное, чтобы было соединение с Интернетом.

Данная глава будет более интересной – мы произведем тестирование следующих продуктов:

- Kaskersky Internet Security
- Dr.Web Security Space
- Eset Smart Security
- Defender

Последний продукт – это штатный антивирус Windows, который вместе со штатным брандмауэром может считаться подобием IS-продукта. Другими словами, проверим, насколько защищена сама Windows – без антивируса. Все продукты, кроме последнего, будут запущены в Win 7. Последний же будет работать под управлением Win 10 – есть надежда, что «десятка» лучше защищена, и даже с таким решетом, как Defender, вирусы не пройдут.

8.1. Как будет производиться тестирование

Первым делом нужно определить, что мы будем проверять:

- обнаружение вируса;
- блокировка запуска вируса;
- лечение заражения.

Первый тест будет производиться при отключенной защите – в режиме сканера. Для второго и третьего тестов монитор антивируса будет включен.

После всего этого мы обновим базы и посмотрим на обнаружение вирусов, сравним с предыдущим результатом. Так как вирусов много, «экспонаты» для проверки запуска будут отобраны самим антивирусом. Будут запущены те вирусы, которые не будут удалены в результате детект-теста.

Глупо пытаться запустить вирус, который есть в антивирусной базе, – любой антивирус заблокирует его запуск. Интереснее всего запустить вирус,

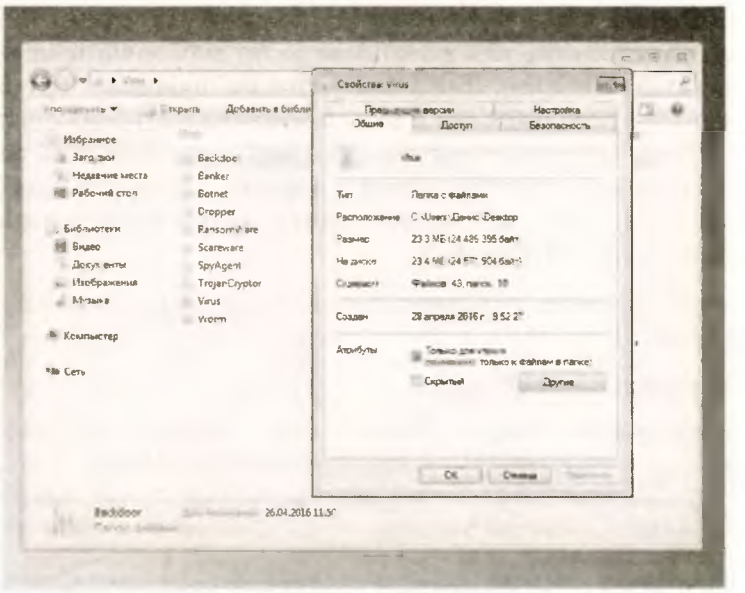


Рис. 8.1. Моя подборка вирусов

который антивирус «не знает». Есть ли у антивируса экстрасенсорные (эвристические) способности?

Совершенно случайно все вирусы в моей подборке были разделены на группы – Backdoor, Worm, Virus и т.д. (см. рис. 8.1). Как видите, есть из чего выбрать.

Все операционки свежие (были специально установлены для написания этой главы), а Интернет был отключен сразу после установки антивируса, чтобы была 100% гарантия, что базы останутся старыми.

8.2. Kaspersky Internet Security

Начнем тестирование со всем известного антивируса Касперского, а именно Kaskersky Internet Security. Как видно из рис. 8.2, антивирус был установлен 6 дней назад (осталось 24 дня бесплатного использования).

Отключаем антивирус, распаковываем архив с вирусами. Антивирус мы не активируем, но запускаем выборочную проверку (чтобы он не стал проверять все подряд, а сконцентрировался на одной папке) и проверяем папку Virus. Помню, когда-то мне в 20-литровую канистру на заправке умудрились заправить 23 литра. Так и в случае с Касперским – в папке из 49 файлов он умудрился найти 80 (рис. 8.3). Видимо, в один файл упаковано не-



Рис. 8.2. Kaskersky Internet Security

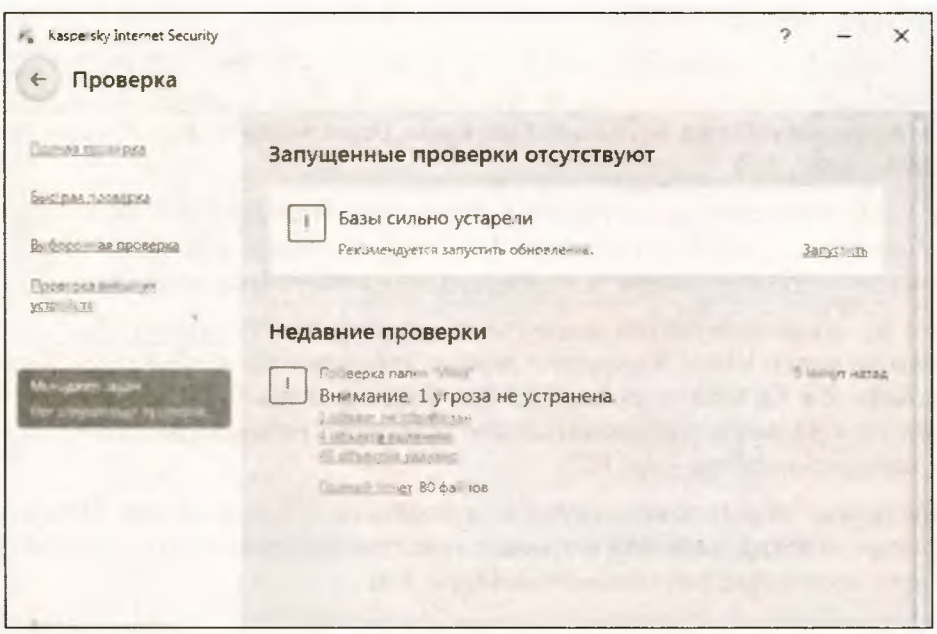


Рис. 8.3. Результат проверки



Рис. 8.4. Подробный отчет

сколько «зараз», и антивирус видит каждую из них. Посмотрим подробный отчет (рис. 8.4).

Как видно из рис. 8.4, было найдено 45 угроз (из 49). Вирус Trojan.Win32.Waldek.jsu почему-то не был ни удален, ни помещен в карантин. Он просто не был обработан, хотя был обнаружен. Всего в папке Virus осталось 11 файлов (рис. 8.5).

Больше всего вирусов осталось в папке RansomWare (рис. 8.6). Как видно со скриншота, файлы с номерами 2, 4, 7 и 8 антивирус вообще не тронул. Интересно будет посмотреть на обнаружение после обновления баз.

Что ж, теперь активируем защиту и пытаемся запустить «выжившие» вирусы из папки Virus. Я запустил первые два файла из папки RansomWare (номера 2 и 4). Файл с номером 2 был распознан как PDM:Trojan.Win32.Generic. Антивирус распознал опасное поведение, «точно характеризующее ее как вредоносную» (рис. 8.7).

Предложил исцелить компьютер с перезагрузкой. Соглашаемся. Начался процесс лечения, антивирус отменил действия вредоносной программы и попутно устранил файл с номером 4 (рис. 8.8).

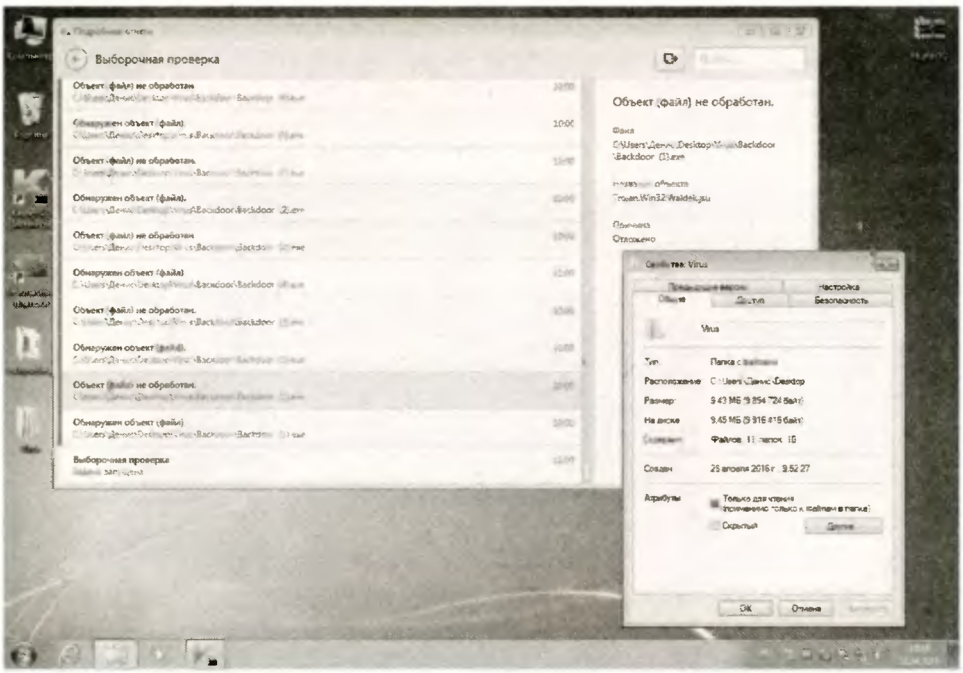


Рис. 8.5. Осталось 11 файлов

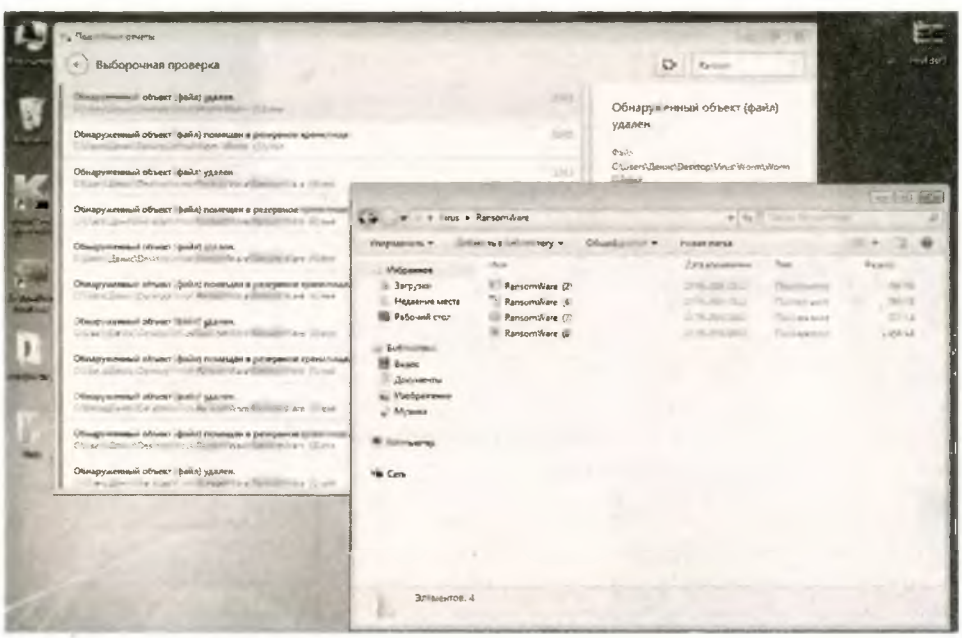


Рис. 8.6. Еще результаты Касперского

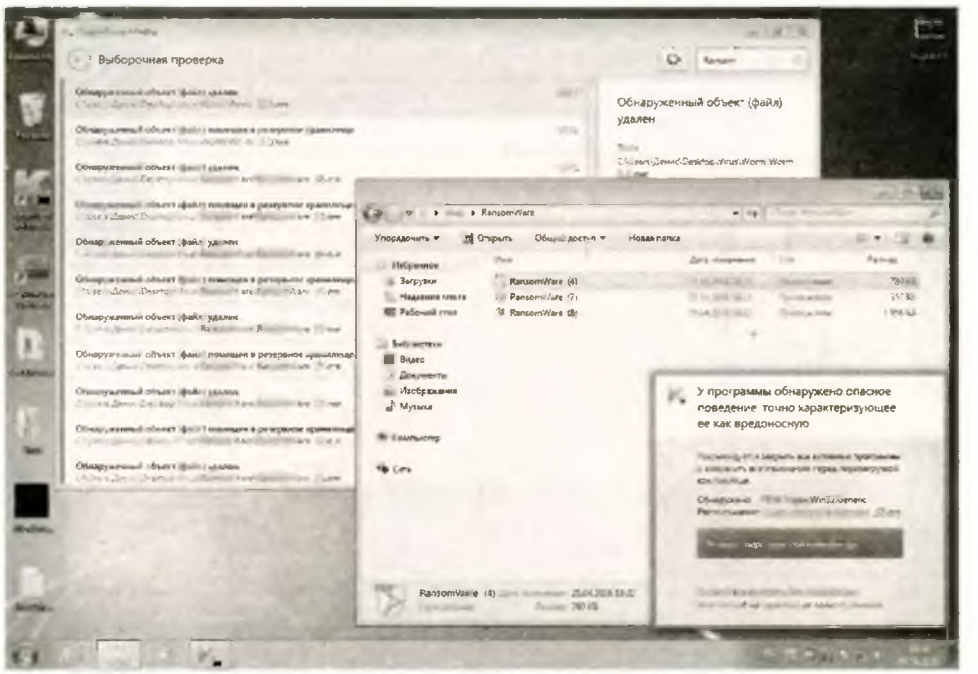


Рис. 8.7. Заблокирован запуск программы

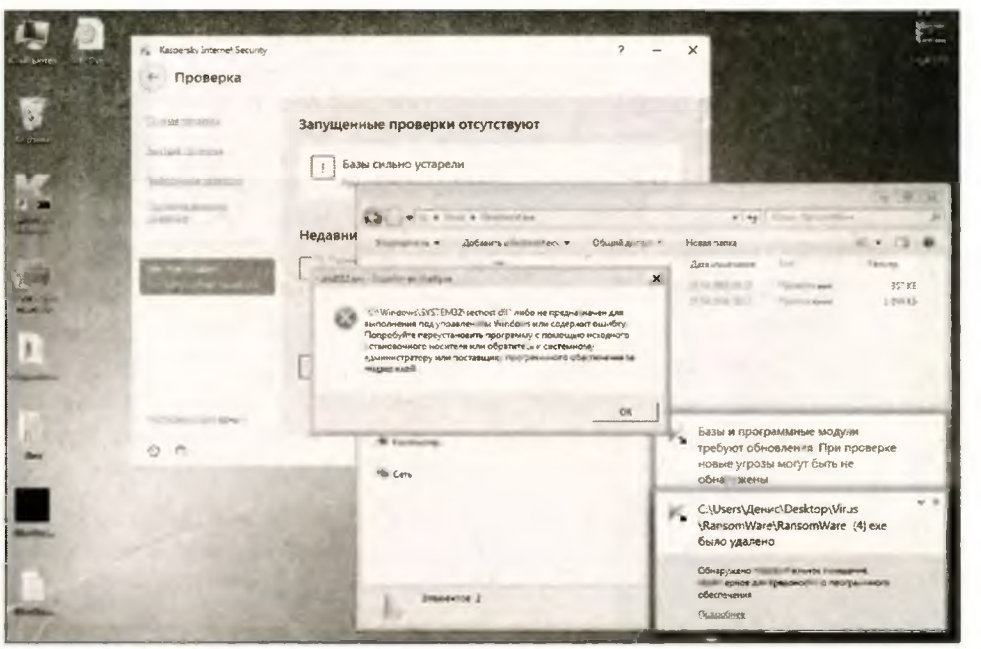


Рис. 8.8. Процесс лечения системы

Результаты лечения мне не понравились. После перезагрузки я не получил чистую систему. Что-то пыталось загрузиться, на рабочем столе остались файлы, созданные вирусом (рис. 8.9). Кое-что антивирус вычистил, но мне кажется, что не все. Попутно антивирус, конечно, пытается лечить созданные вирусами объекты (рис. 8.10).



Рис. 8.9. Результат лечения



Рис. 8.10. Антивирус обнаружил еще зараженные объекты

Продолжаю запускать файлы из папки RansomWare (номера 7 и 8). Сразу после запуска этих файлов, как и в предыдущем случае, моментальной реакции антивируса не последовало, что позволяет программам размножаться. Антивирус начал реагировать уже после того, как вирусы начали отправлять электронные письма (ничего у них не вышло – у меня ни почтового клиента, ни соединения с Интернетом!), рис. 8.11.

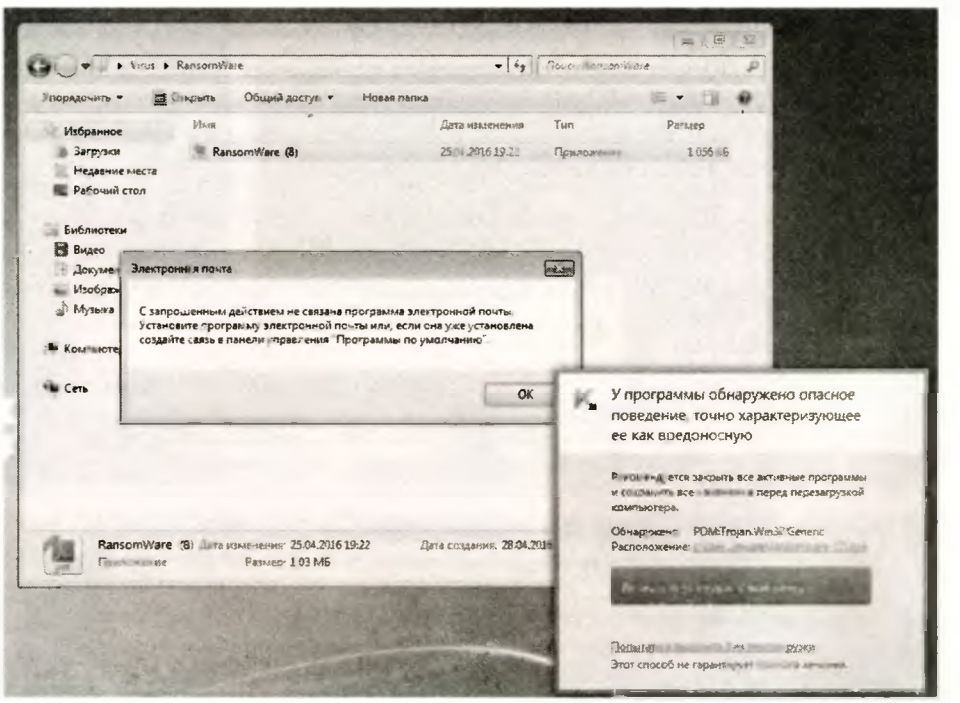


Рис. 8.11. Запоздавшая реакция антивируса

Интересно, но на файл с номером 8 антивирус Касперского так и не отреагировал. Идем «дальше». Из папки Scareware запускаю единственный файл с таким же названием. Жду несколько минут. От антивируса реакции никакой, а вирус тем временем, скорее всего, делает свои темные дела.

Из папки TrojanCryptor запускаю файл с именем TrojanCryptor (1). Шифровальщик – тяжелая артиллерия. Реакции антивируса тоже не последовало. Зато появилось окошко, изображенное на рис. 8.12.

> **Примечание.** Троян запустился, реакции от антивируса вроде бы нет, но данные остались незашифрованными, как и в случае еще с одним участником этого теста. А вот один из антивирусов допустил шифрование данных, что и будет показано далее.



Рис. 8.12. Окно трояна

Из папки Virus запускаю файлы с номерами 4 и 8. Далее из папки Worm запускаю файлы с номерами 6 и 8. Первый почему-то не запустился (ошибки допускают не только разработчики обычных программ, но и вирусописатели). А на второй Касперский никак не отреагировал.

Запускаю полную проверку компьютера. Ее цель – определить зараженные вирусами объекты и попытаться вылечить компьютер. После перезагрузки посмотрим, что получилось у антивируса. Честно говоря, результаты меня не порадовали. Антивирус сообщил, что угроз не обнаружено (рис. 8.13). Хотя вредоносные программы на компьютере остались. Глубоко копать не стал – просто открыл msconfig и посмотрел, что автоматически запускается. Как видим, антивирус «вычистил» далеко не все.

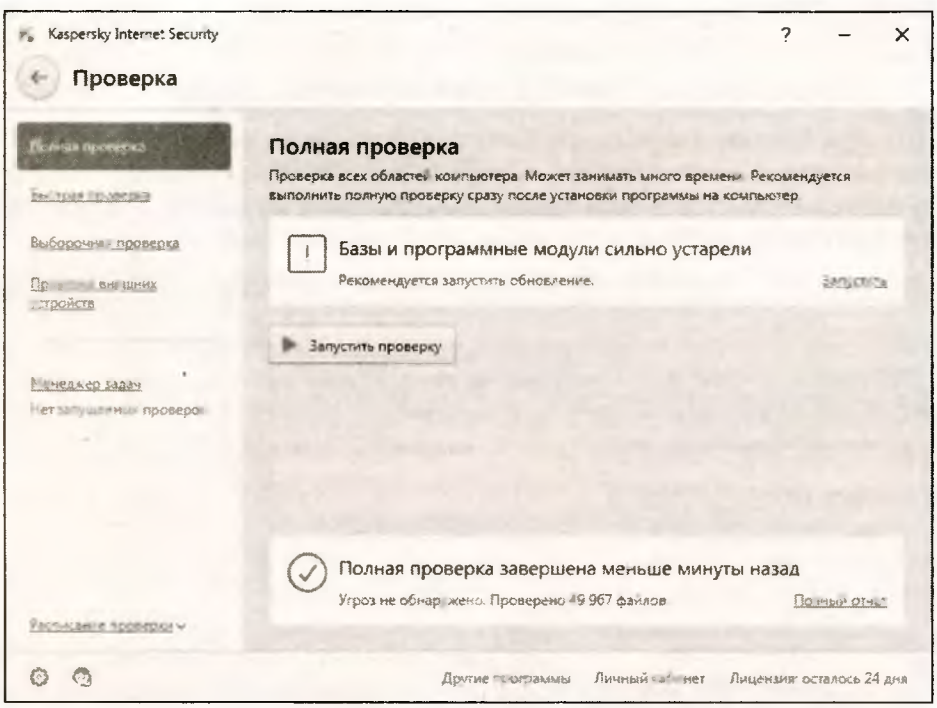


Рис. 8.13. Угроз не обнаружено

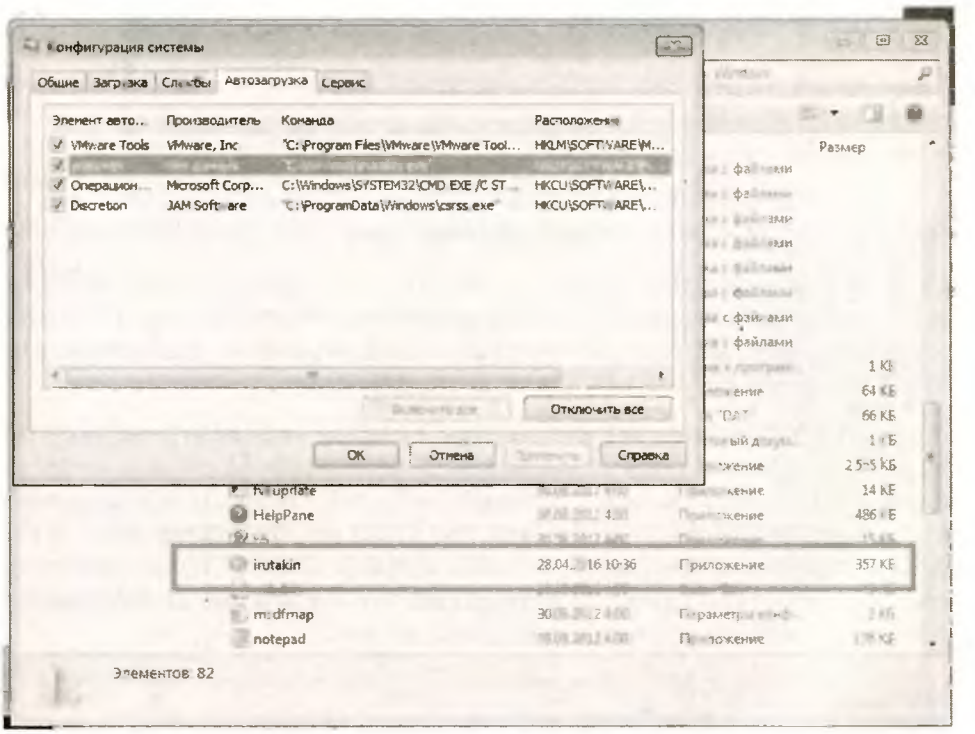


Рис. 8.14. Не все удалено

При перезагрузке компьютера Касперский сообщил, что он все-таки вздумал вылечить мой компьютер – обнаружен активный процесс лечения, в результате которого был-таки удален файл Ransomware (8).exe, а также файл worm (8).exe (рис. 8.15).

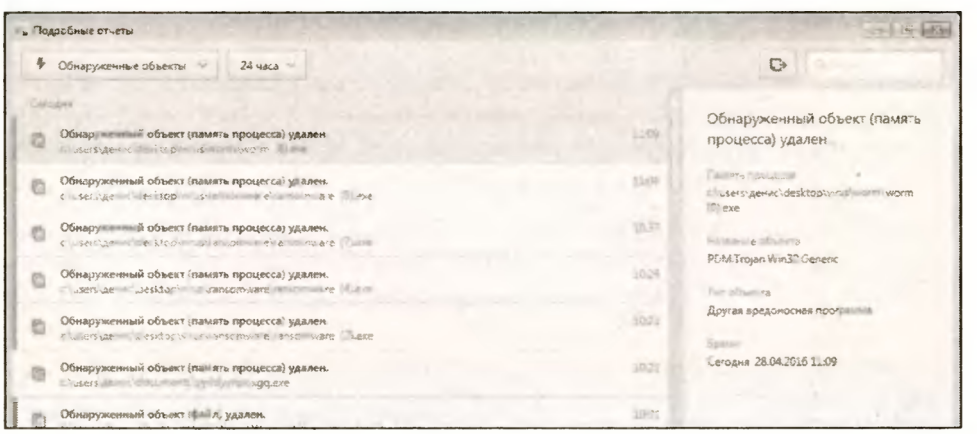


Рис. 8.15. Антивирус опомнился

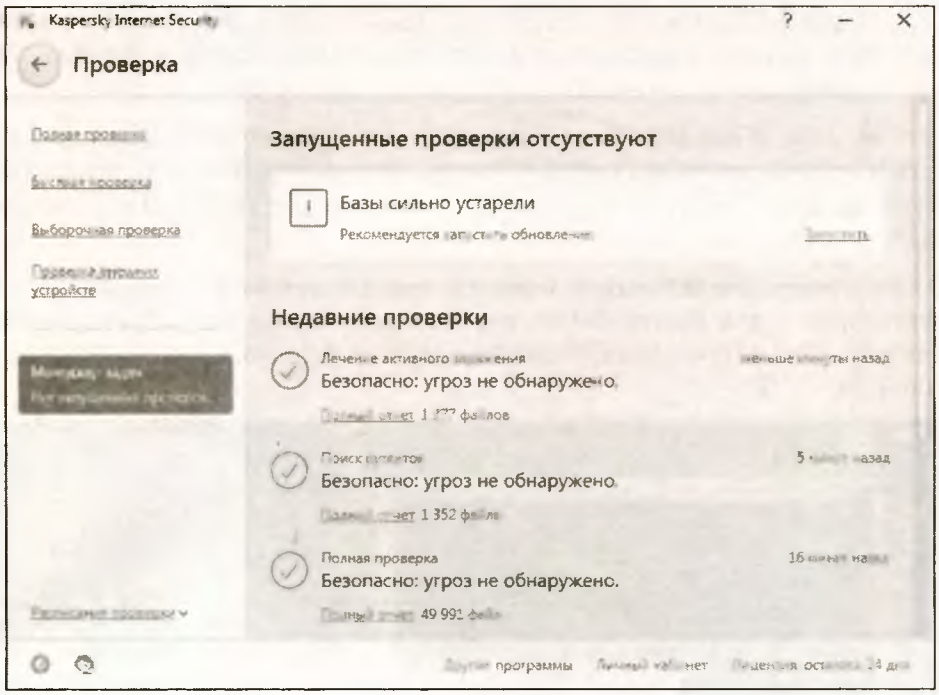


Рис. 8.16. Опять угроз нет

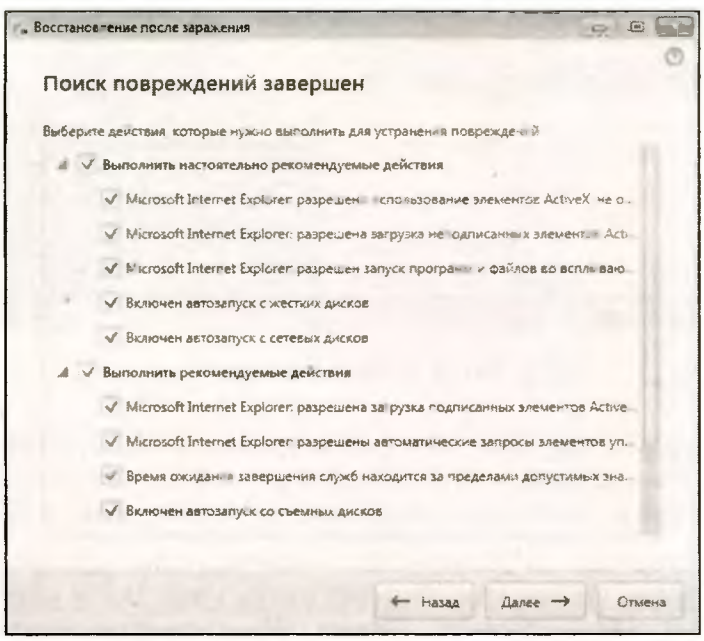


Рис. 8.17. Мастер восстановления после заражения

Честно говоря, мне не очень понятен алгоритм работы антивируса, но главное, что некоторые вредоносные файлы он вычистил. После лечения активного заражения опять сообщил, что угроз нет (рис. 8.16).

Что ж, пора обновлять базы. Базы обновлены, компьютер перезагружен. После перезагрузки был запущен мастер восстановления после заражения, предложивший исправить некоторые моменты (рис. 8.17). После работы мастера опять перезагружаю компьютер.

Мастер кое-что восстановил, а кое-что нет. Да, автозапуск очищен. Но не полностью – как видно на рисунке 8.18, кое-что все еще пытается запуститься. Файлы -!RecOveR!*, созданные по всему диску, тоже не были вычищены.

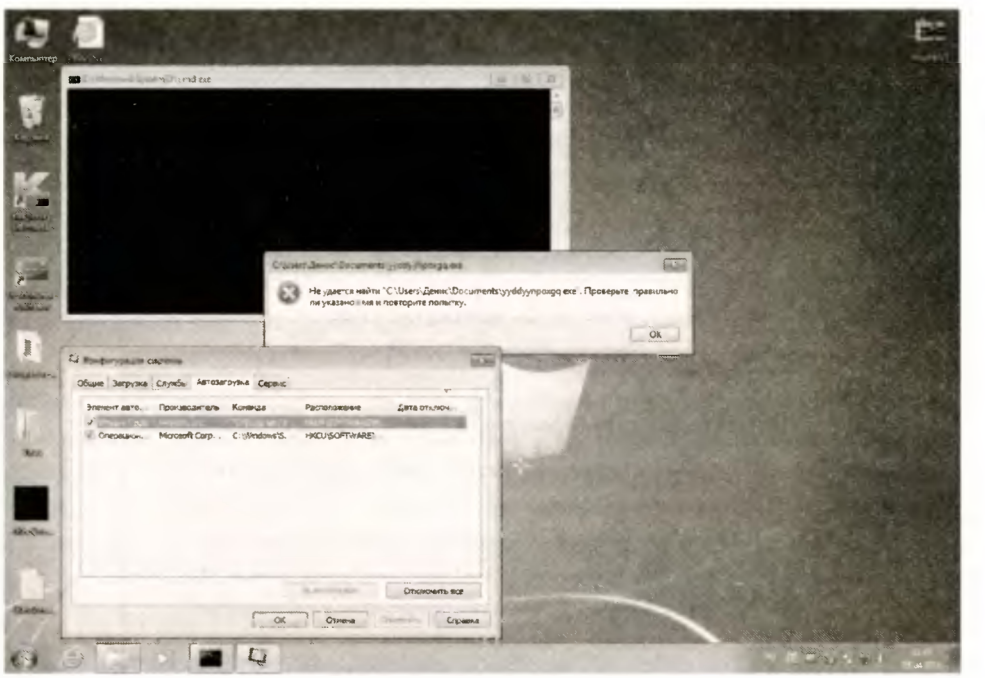


Рис. 8.18. Не все вычищено

Даю антивирусу еще один шанс и опять запускаю полную проверку – на этот раз с новыми базами. Угроз обнаружено не было, множественные файлы, созданные вирусом, так и остались на компьютере (рис. 8.19).

Теперь повтор теста на обнаружение. Отключаю защиту, распаковываю архив и запускаю выборочную проверку папки Virus. После обновления баз Касперский нейтрализовал все угрозы (49), обнаружил он, правда, аж 51

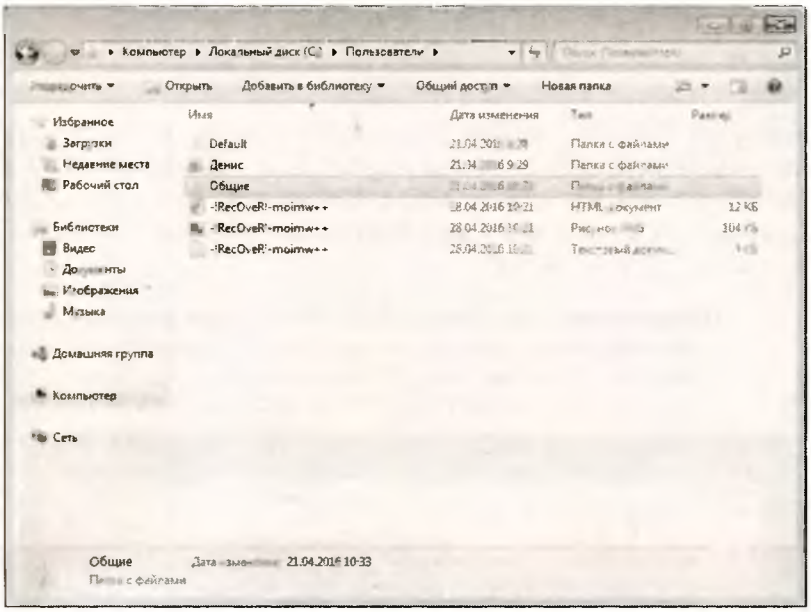


Рис. 8.19. Множественные файлы, созданные вирусом

угрозу в 49 файлах, видимо, в каких-то файлах содержится несколько угроз. В общем, что и следовало ожидать.

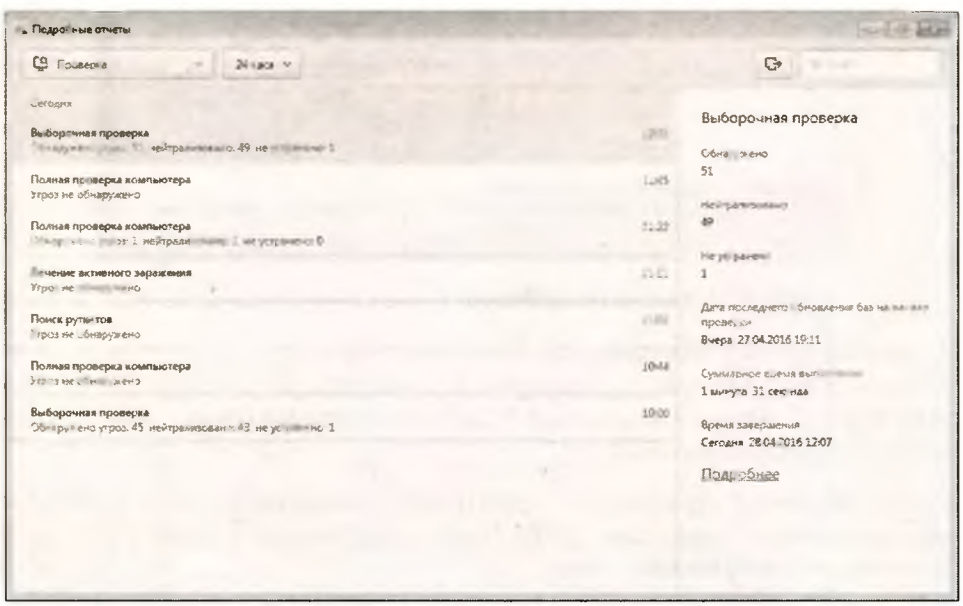


Рис. 8.20. После обновления баз все угрозы устранены

8.3. Dr.Web Security Space

В линейке Dr.Web был выбран настоящий монстр, установочный файл которого «весит» 466 Мб, – Security Space. Как и антивирус Касперского, Dr.Web был установлен неделю назад. Посмотрим, что у него получится. Результат оказался хуже, чем у антивируса Касперского, – было обнаружено всего 34 угрозы (рис. 8.21).

> **Примечание.** При установке Dr. Web не было выбрано подключение к облачным сервисам, то есть сравнивался функционал самого антивируса, но толку бы от них все равно не было – на момент сканирования и лечения компьютер просто не подключался к Интернету.

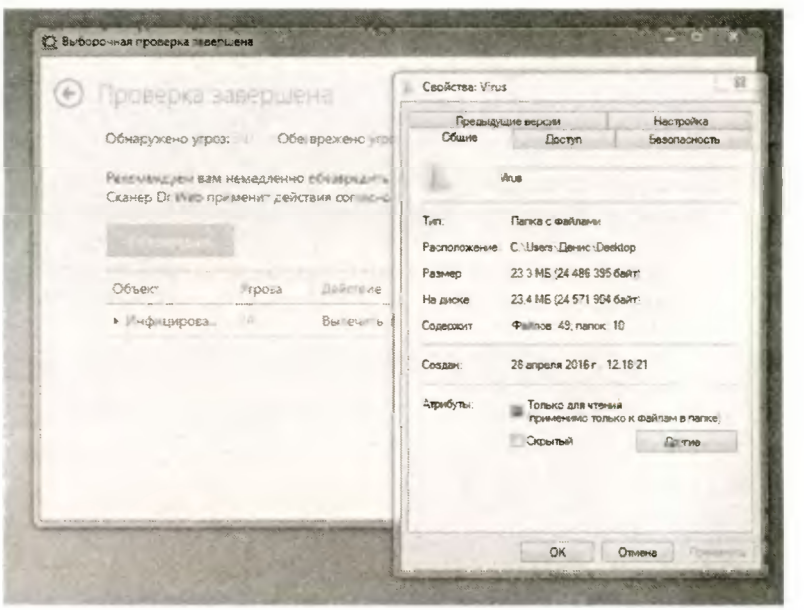


Рис. 8.21. Тест на обнаружение: обнаружено 34 угрозы из 49

Нажимаю кнопку **Обезвредить**. Антивирус обезвредил 34 угрозы, в папке Virus осталось 18 файлов. Нехитрый математический подсчет 49 – 34 дает результат 15, откуда взялось еще 3 файла? Просто некоторые файлы антивирус «вылечил» (рис. 8.23).

Далее антивирус предложил перезагрузить компьютер, дабы завершить обезвреживание угроз (рис. 8.24). После перезагрузки в папке Virus осталось столько же файлов.

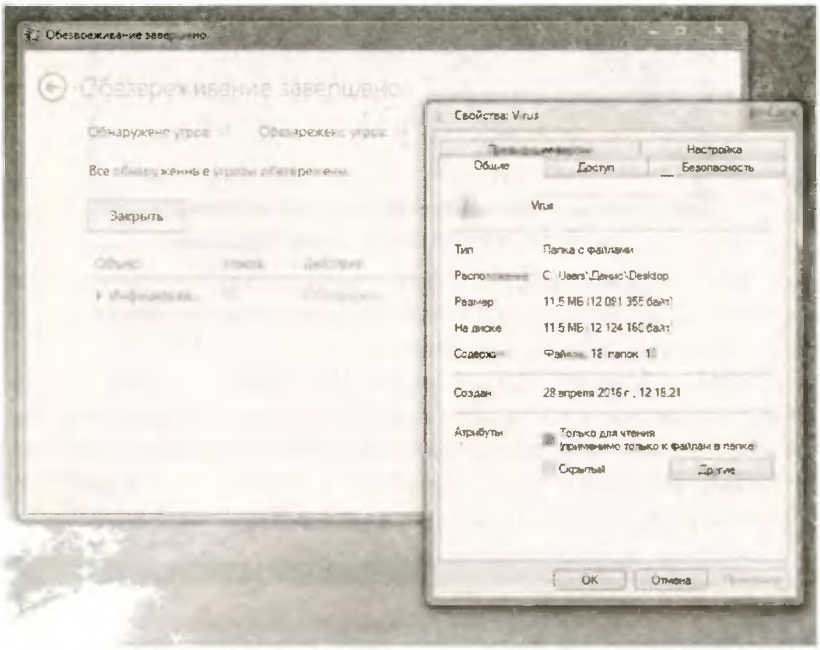


Рис. 8.22. Результат обезвреживания угроз



Рис. 8.23. Отчет сканера

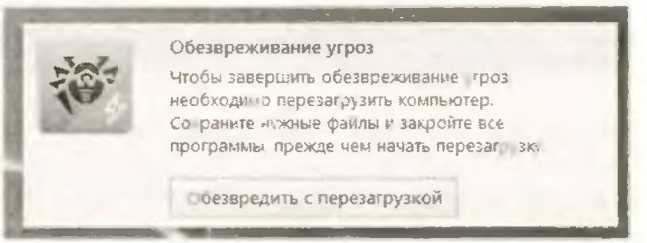


Рис. 8.24. Предложение перезагрузиться

Переходим ко второй части теста, а именно блокировке запуска вредоносной программы. Запускать буду те файлы, которые уцелели в результате проверки сканером. Защита в реальном времени (SplDel Guard) включена. Файлов осталось больше, чем в случае с Касперским. Первым делом запускаю файл с номером 1 из папки Backdoor (кстати, Касперский сразу удалил все вредоносные программы из этой папки). Реакция последовала сразу – вот только антивирус отреагировал не на сам exe-файл с номером 1, а на тот файл, который, видимо, он извлек в папку AppData (рис. 8.25).



Рис. 8.25. Реакция антивируса

Аналогичным образом отреагировал на программу Dropper из одноименной папки. А вот на вирус типа Banker от него не последовало никакой реакции. Далее переходим к моей любимой категории RansomWare. Сканер оставил все файлы из этой папки нетронутыми (рис. 8.26).

Запущено первые два файла. Вирусы размножаются по компьютеру, что видно по файлам -!RecOver*. Антивирус сразу не заблокировал запуск вируса (как и в случае с Касперским), сработала превентивная защита и отреагировала на один из файлов. Запущен третий файл, вирусы продолжают открывать различные окна, а антивирус на них никак не реагирует (рис. 8.27).

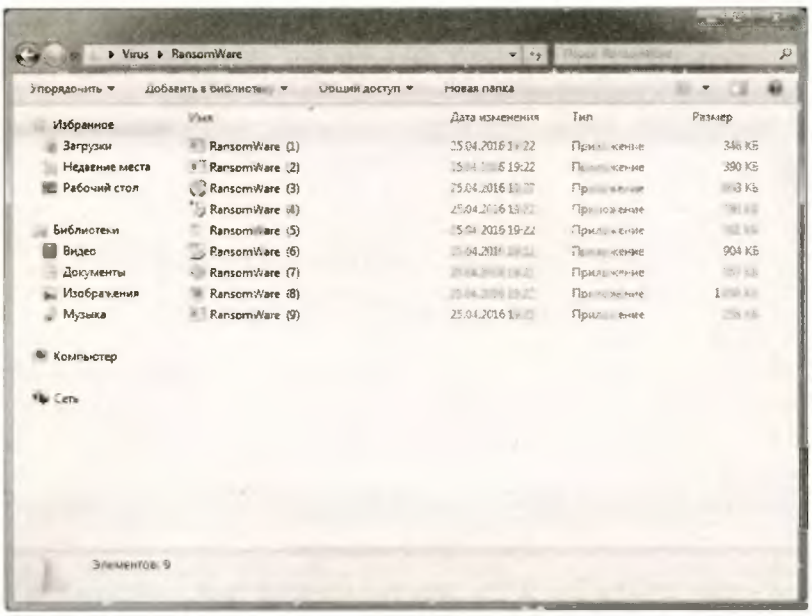


Рис. 8.26. Полный набор RansomWare

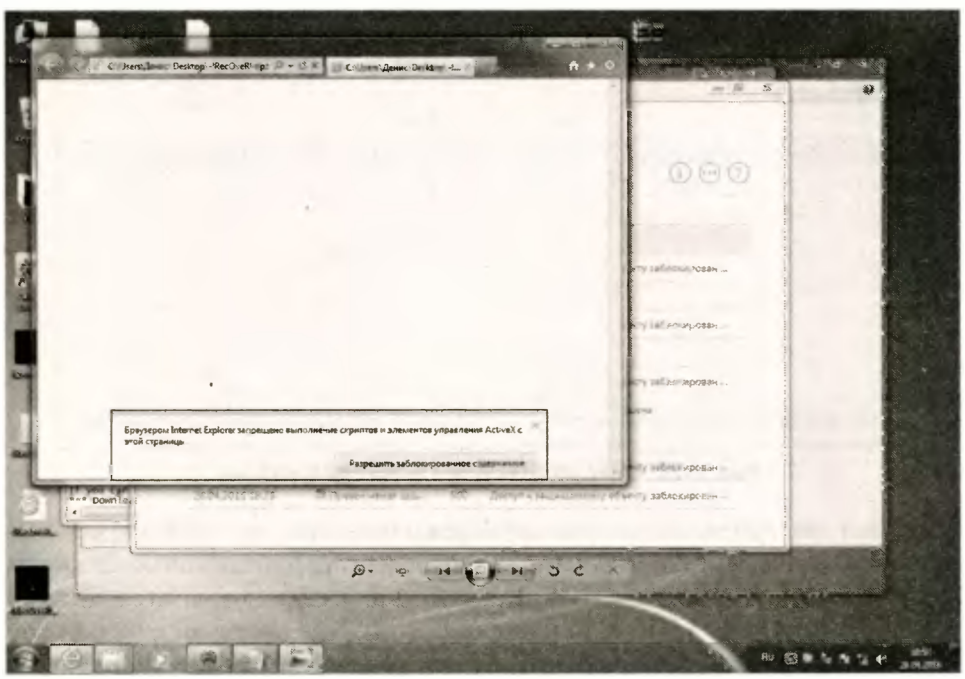


Рис. 8.27. Процесс инфицирования идет полным ходом

Запускаю файлы 4-6. Антивирус отреагировал на две из трех угроз (рис. 8.28). Но опять-таки с небольшим запозданием. Ведь работает не монитор, а именно превентивная защита.

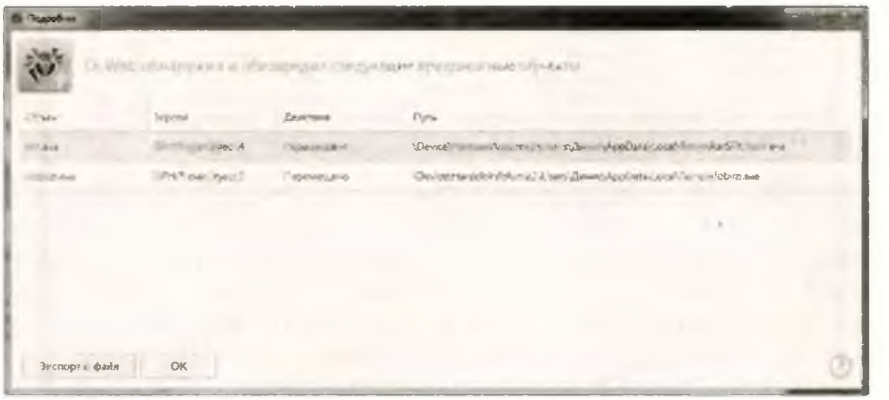


Рис. 8.28. Две из трех

Далее запускаю файлы 7 – 9. На этот раз одна из трех угроз была обезврежена.



Рис. 8.29. Одна из трех угроз была обезврежена

Если бы я тестировал все это на своей реальной машине, мне было бы уже страшно. Но ничего, идем дальше – запускаем шифровальщики. В папке TrojanCryptor есть два файла – с номерами 1 и 4 (если не считать еще трех файлов – !RecOveR*). Первый шифровальщик был запущен, а от запуска второго меня спасла древняя Win 7 – вирус оказался новее операционки, и он просто не запустился.

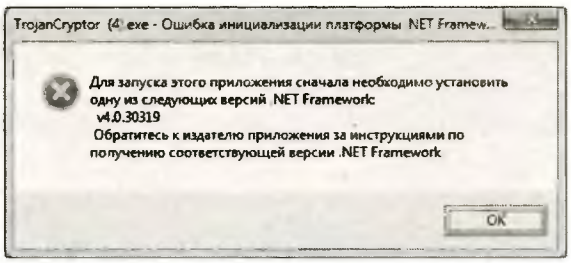


Рис. 8.30. .NET слишком старый

Из папки Virus все файлы были или удалены, или излечены, поэтому я ничего не запускал. Остался только один файл – с номером 8 из папки Worm. Запустился (рис. 8.31), реакции от антивируса не последовало.

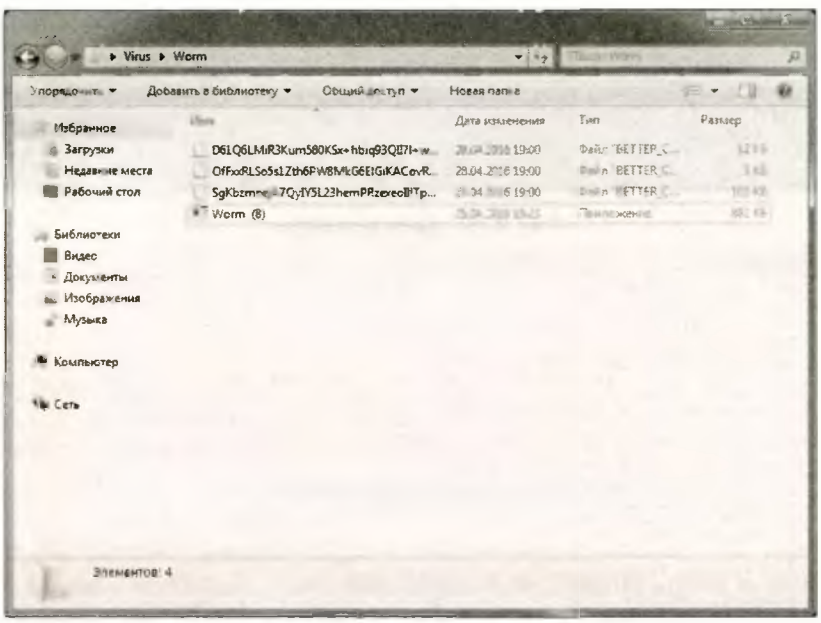


Рис. 8.31. Вирусы размножаются дальше

Компьютер тормозит, глючит все, что могло глючить, в том числе Проводник. А потом я вижу картину маслом (рис. 8.32). Антивирус не спас мой компьютер от шифровальщика. Тот самый README.TXT представлен на рис. 8.33. Теперь вы знаете, как работает вирус-шифровальщик. Можно было бы написать по упомянутому e-mail, но наверняка я бы получил инструкции по переводу денег. Лечить виртуалку я не стал, она запускается, но все файлы пользователя зашифрованы.

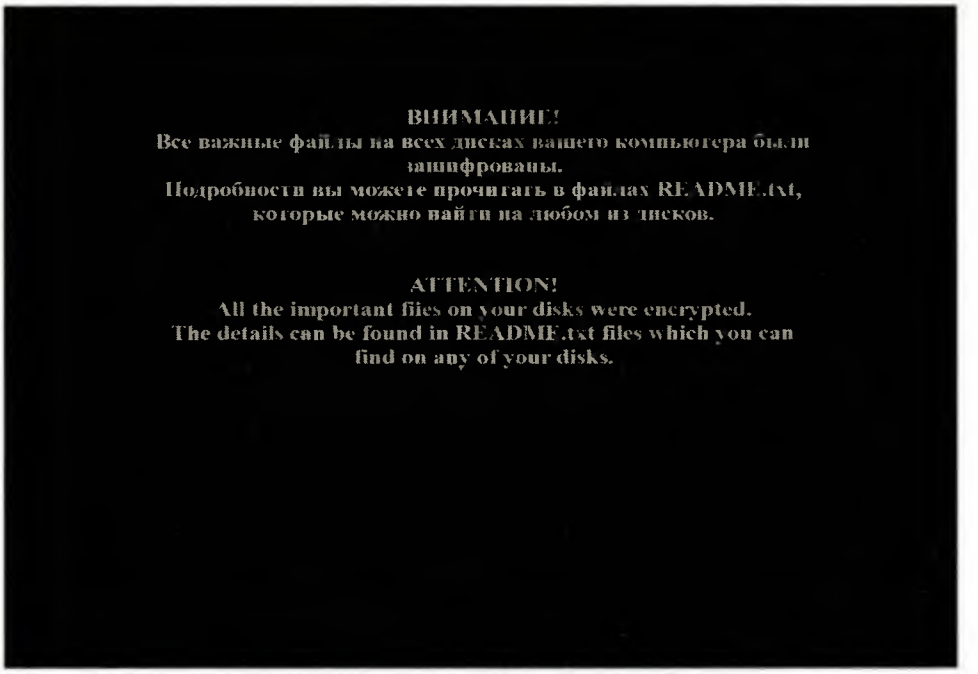


Рис. 8.32. Шифровальщик

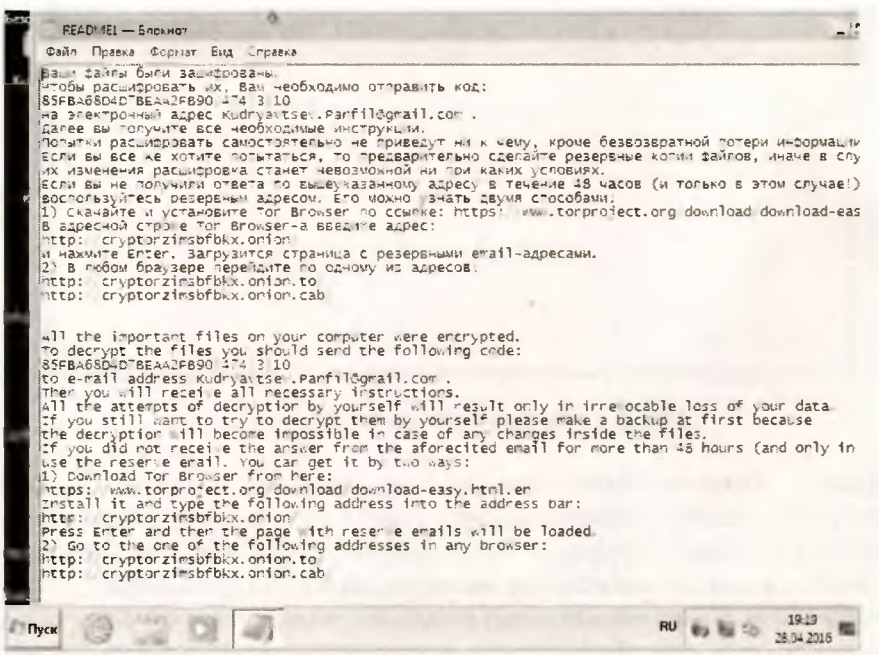


Рис. 8.33. README шифровальщика

Самое интересное, что антивирус все еще запускается, как и сама операционная система. Но, думаю всем ясно, что тест на запуск неизвестного вируса провален полностью. Клонирую чистую виртуальную машину. В нее будет заново установлен Dr.Web и будет произведен тест на детект, но уже с самыми последними базами. При установке уже решил перестраховаться и включил доступ к Dr.Web Cloud.

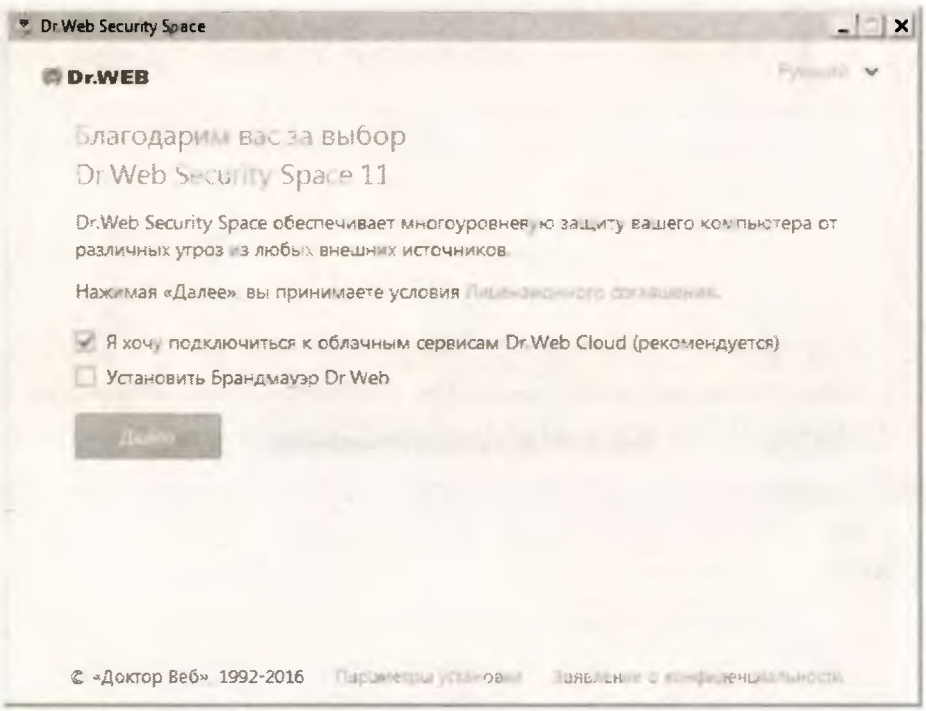


Рис. 8.34. Переустанавливаю Dr.Web

После обновления баз антивирус успешно обнаружил все 49 угроз (рис. 8.35). Больше всего мне, наверное, как и вам, хотелось узнать имя нашего «героя», который «угробил» предыдущую виртуалку, – это Trojan. DownLoader21.31460.

Ради интереса я запускаю этот же вирус, но уже после обновления антивирусных баз. Как и следовало ожидать, он запуститься не смог (рис. 8.37).

Рис. 8.37. После обновления баз зашифровать файлы не получилось

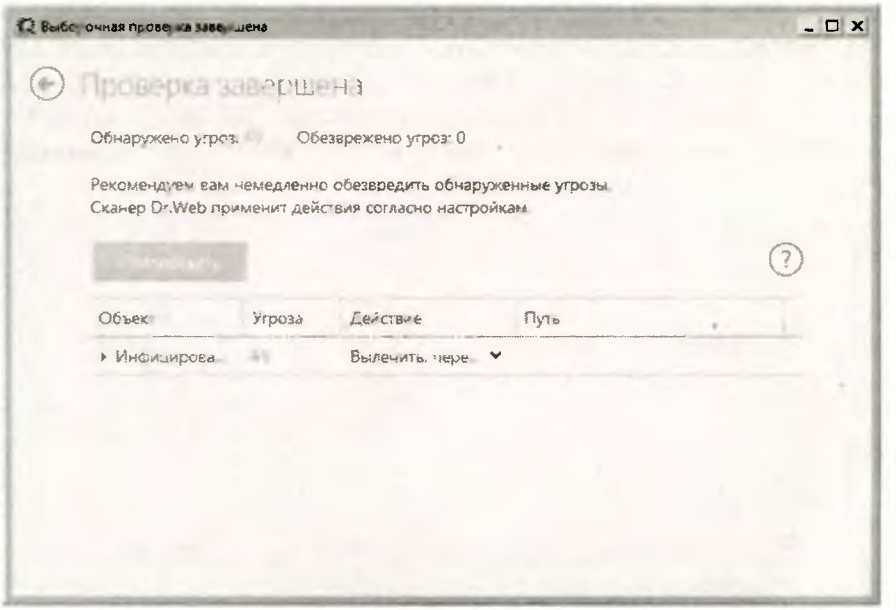


Рис. 8.35. Все угрозы обнаружены

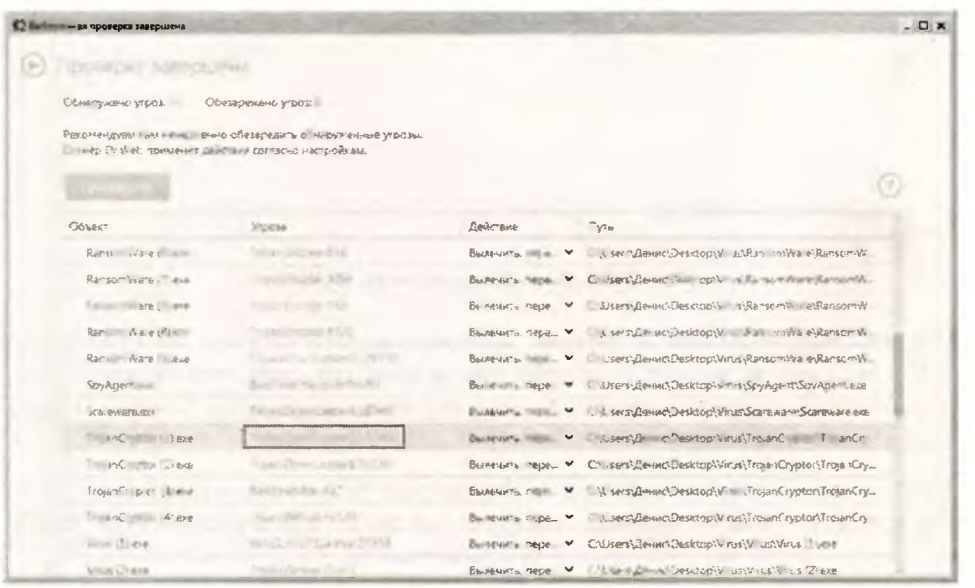


Рис. 8.36. Страна должна знать своего героя

Обновление антивирусных баз для Dr.Web играет очень важную роль. Если в случае с Касперским можно положиться на его эвристические способно-

сти, то здесь нужно следить, чтобы антивирусные базы обновлялись вовремя. Но и информация о вирусах, видимо, поступает в антивирусные базы раньше – ведь все антивирусы были установлены неделю назад, тогда же было произведено и обновление баз, после чего виртуалка «консервировалась» на неделю. Ведь в тесте на детект «Каспер» обнаружил больше вирусов.

8.4. ESET Smart Security

Как и с остальными антивирусами, ESET был установлен неделю назад, что видно по сроку действия лицензии (рис. 8.38).

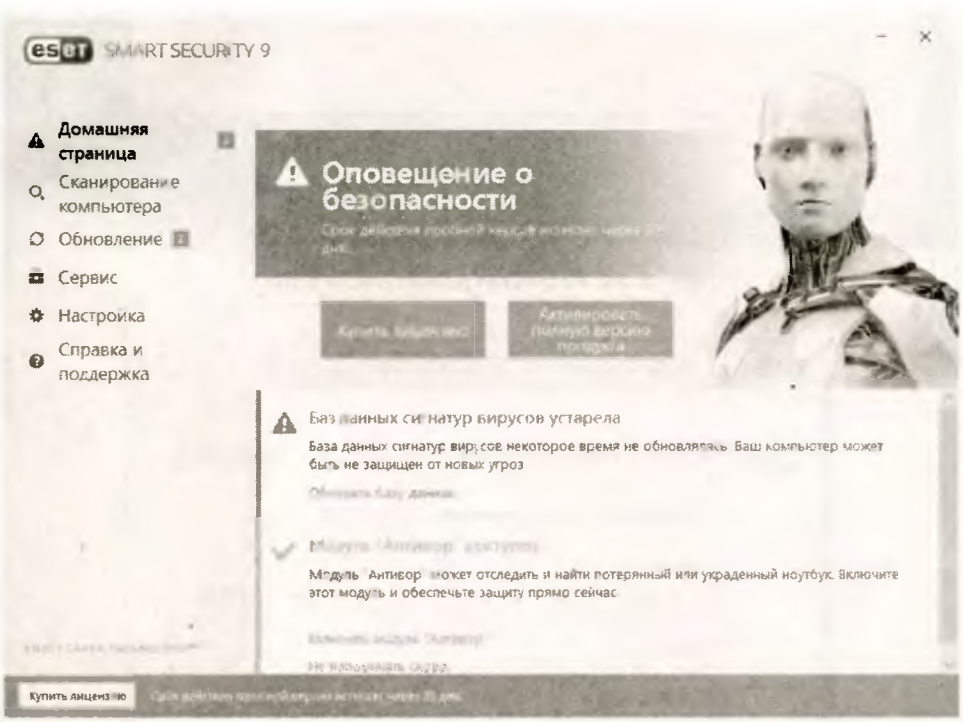


Рис. 8.38. Антивирус ESET

Тест на детект вирусов показал 36 угроз. Результат очень похожий на результат Dr.Web (рис. 8.39). В папке Virus осталось 14 файлов.

Запускаем защиту в реальном времени и запускаем оставшиеся вирусы. Первый файл – из подпапки Backdoor – вирус с номером 1 (остальные из этой папки – вычищены). Антивирус моментально справился с обнаружением вредоносной программы (рис. 8.40).

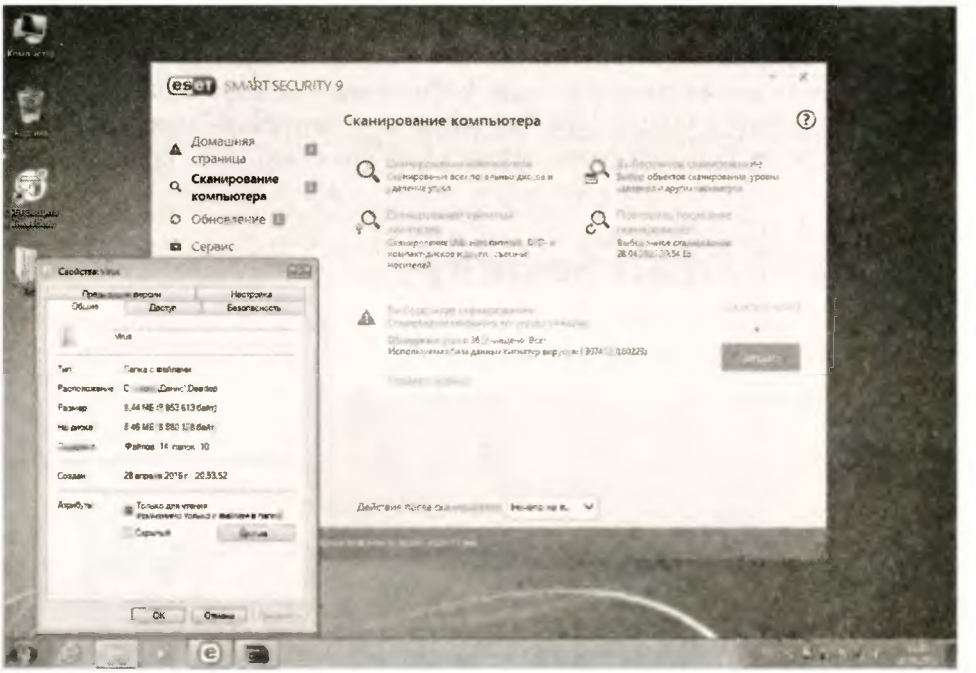


Рис. 8.39. Результат детект-теста ESET

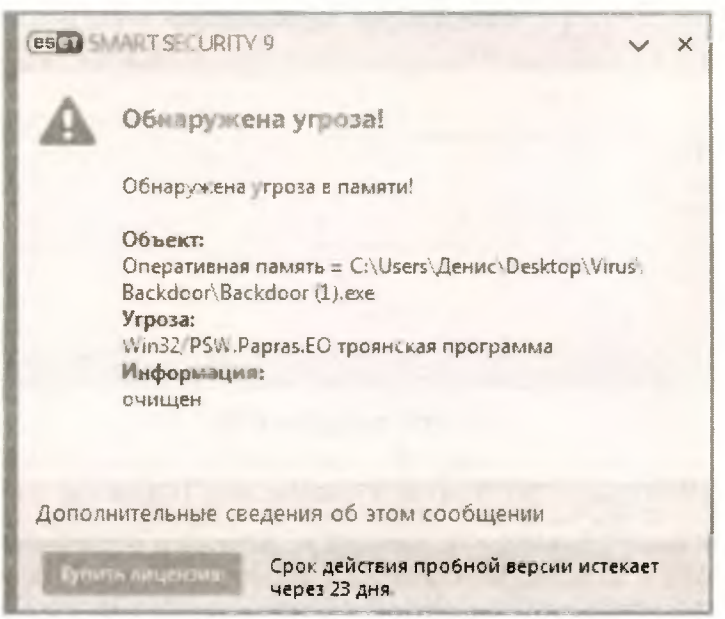


Рис. 8.40. Обнаружена угроза

Антивирус не отреагировал на единственный уцелевший в подпапке Banker вирус (файл с номером 1). Далее запускаю вирус Dropper – его сразу же «отловил» ESET.

Перехожу к многострадальной папке RansomWare. Как и Dr.Web, ESET не удалил из этого каталога ни одного файла. Со всего набора антивирус отреагировал только на файлы с номерами 3 и 8. Остальные вполне успешно были запущены (рис. 8.41). Список уцелевших файлов приведен на рис. 8.41.

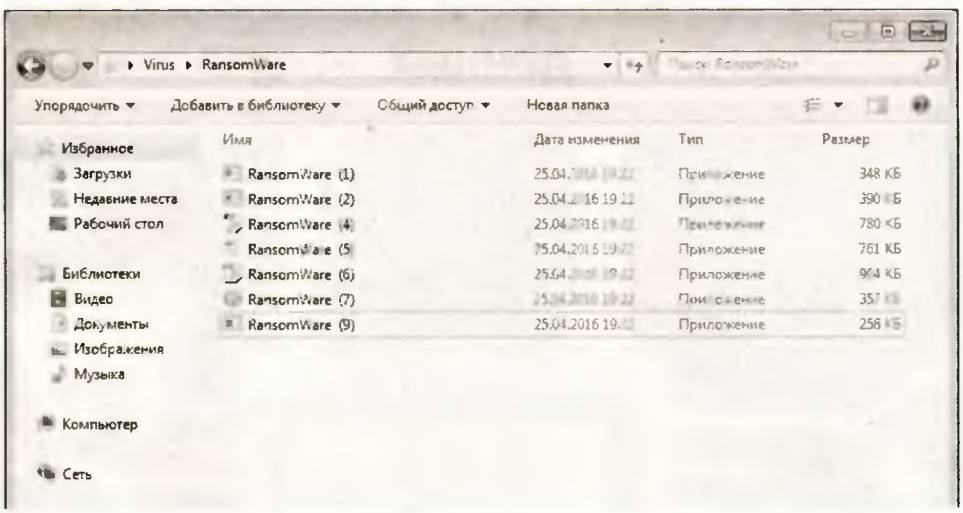
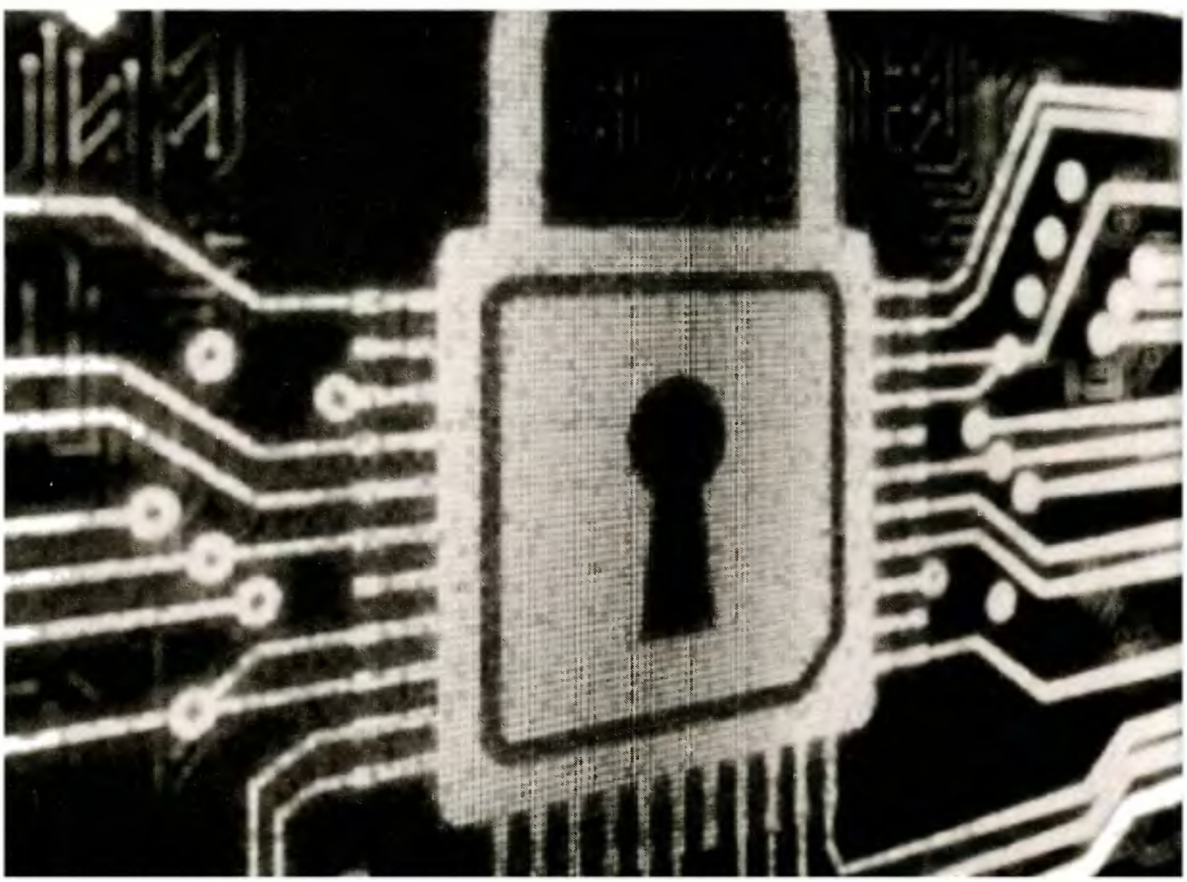


Рис. 8.41. Уцелевшие вирусы класса RansomWare

Часть 3. Защищаем файлы на Windows-компьютере

Глава 9. Выбор средства защиты данных



Существуют различные способы защиты данных на персональном компьютере. Самыми радикальными являются шифрование всего диска или шифрование одного из разделов, на котором хранятся конфиденциальные данные. Менее радикальные – криптоконтейнеры (виртуальные диски). Файл виртуального диска хранится на жестком диске, как обычный файл. Но его можно открыть в программе шифрования, и она подмонтирует содержимое виртуального диска к одной из свободных букв. После этого пользователь сможет работать с виртуальным диском как с обычным диском. Есть еще прозрачное шифрование, когда шифруется одна из папок на жестком диске. Все файлы, помещенные в эту папку, автоматически шифруются. В этой части книги будут рассмотрены все эти способы. Однако сначала нужно поговорить о выборе оптимального для вас средства защиты данных.

Глава 9. Выбор средства защиты данных

9.1. Шифрование диска

Шифрование всего диска – наиболее радикальный метод шифрования. Преимущество этого способа в том, что пока вы не введете пароль (или кто-то другой, кому в руки попал ваш компьютер), операционная система не загрузится. Если вы – агент 007 или просто страдаете паранойей, то этот способ для вас.

Но это далеко не самый оптимальный способ шифрования данных. Во-первых, вы должны понимать, что любое шифрование – это, прежде всего, преобразование, видоизменение данных. Следовательно, при записи данных на диск их нужно зашифровать, а при чтении – расшифровать. В результате снижается общая производительность работы с системой.

Во-вторых, далеко не все данные нужно шифровать. Например, зачем шифровать файлы операционной системы, исполнимые файлы программ?

Если вы – настоящий параноик, то можете возразить, мол, операционная система и приложения могут хранить конфиденциальные данные не только в пользовательских файлах, но и во временных файлах, в Cookies, в реестре, в файлах программы (каталог AppData). Когда нет времени, желания или возможности выяснить, что нужно шифровать, а что нет, часто шифруют весь жесткий диск, жертвуя производительностью.

Нужно отметить, что далеко не все программы умеют шифровать системный диск. Проверенных вариантов (чтобы вы могли не только зашифровать системный диск, но и потом расшифровать его) всего два – или стандартное средство BitLocker, или всем известная программа TrueCrypt.

Менее радикальный способ – шифрование одного из разделов. Вы можете выделить один из разделов для своих секретных документов и зашифровать его. Все ваши секретные данные (и приложения – при желании) будут храниться на этом диске. Перенести пользовательский профиль на зашифрованный диск, увы, не получится, так как далеко не все программы шифрования могут монтировать диск до входа пользователя в систему. Если вы опасаетесь, что кто-то сможет прочитать данные из вашего каталога AppData, лучше перестраховаться и зашифровать весь жесткий диск.

У шифрования раздела есть огромное преимущество перед шифрованием всего диска. Во-первых, больше выбор программ, которые могут шифровать раздел диска (просто не все программы шифрования могут зашифровать системный диск, а вот программ для шифрования обычных разделов гораздо больше). Во-вторых, все-таки файлы операционной системы не шифруются, как и файлы приложений, следовательно, с производительностью все будет в порядке.

Если у вас только один раздел, не беда. Существуют программы, которые могут «отрезать» свободное дисковое пространство и на его месте создать новый раздел. Например, пусть у вас есть один раздел (диск C) размером 500 Гб. Из этих 500 Гб пусть свободно 250 Гб. Свободное дисковое пространство можно использовать, чтобы создать новый раздел. Например, вы можете «отрезать» 50 Гб (для секретных документов, думаю, этого более

чем достаточно). После этого данный раздел можно зашифровать и использовать для хранения секретных файлов.

В качестве программы для изменения таблицы разделов я рекомендую использовать AOMEI Partition Assistant. Программа гораздо компактнее и дешевле Acronis, а работает не хуже. Изменение таблицы разделов происходит без перезагрузки компьютера (если, конечно, изменяется не системный раздел).

На рис. 9.1 изображена таблица разделов моего сервера. Для изменения размера раздела нужно щелкнуть по нему и выбрать команду меню **Partition, Resize Partition**. После этого появится окно, в котором нужно будет установить новый размер раздела. На рис. 9.2 видно, что я собираюсь «отрезать» 5.6 Гб дискового пространства от диска H.

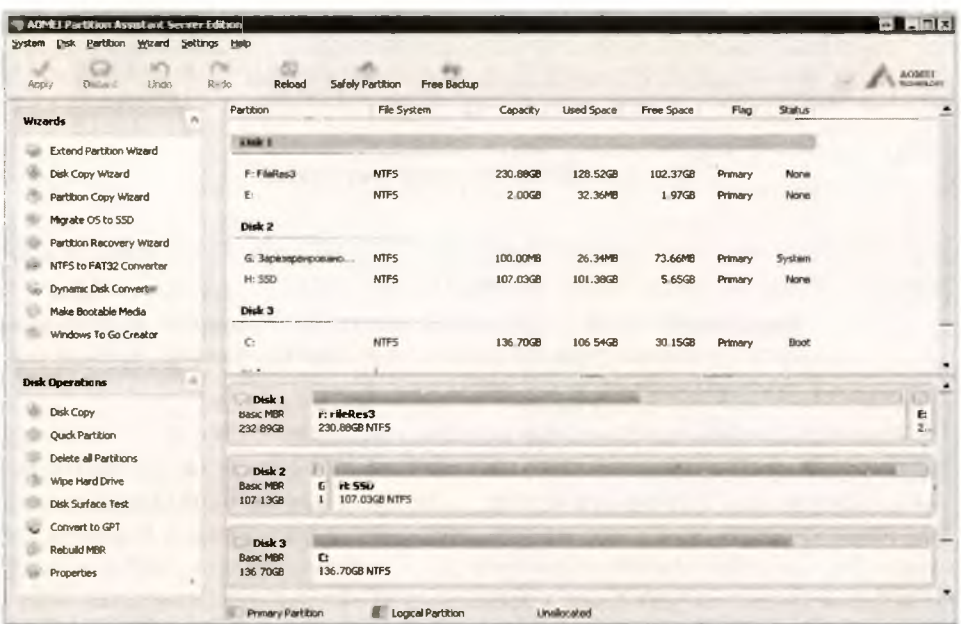


Рис. 9.1. Программа AOMEI Partition Assistant (серверная версия)

После того как программа уменьшит размер раздела, на жестком диске появится нераспределенная область. Нужно щелкнуть по ней и выбрать команду меню **Partition, Create Partition**. Далее все просто – нужно создать новый раздел (это и делает команда **Create Partition**), а потом отформатировать его как NTFS (команда **Partition, Format Partition**).

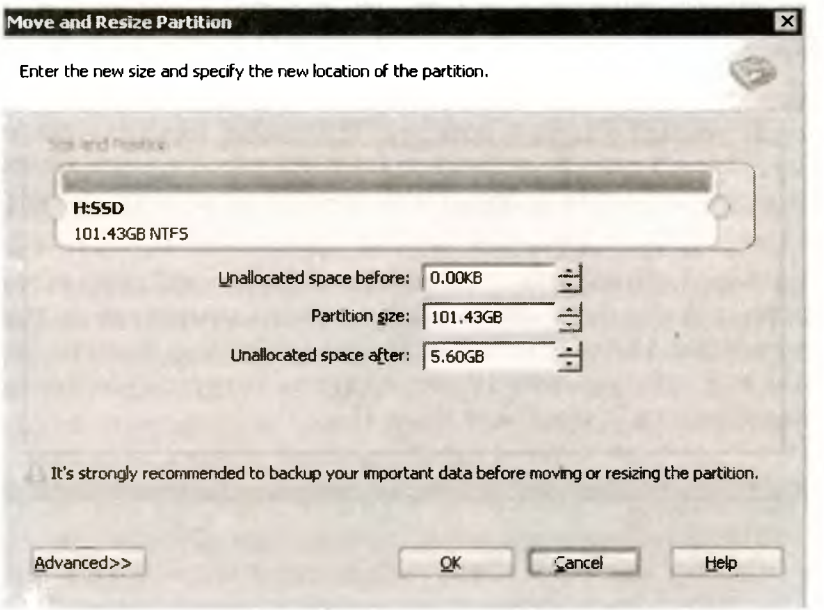


Рис. 9.2. Изменение размера раздела

Все, теперь у вас есть отдельный раздел, который можно зашифровать. О том, как это сделать, будет сказано далее в этой книге.

> **Внимание!** После шифрования нельзя будет изменять размер раздела. Поэтому сразу установите необходимый размер, возможно, с небольшим запасом (20-30%).

Типичный сценарий шифрования раздела – это совместное использование компьютера. Допустим, есть жесткий диск на 500 Гб и есть три пользователя, которые периодически работают с компьютером. Несмотря на то, что файловая система NTFS все же поддерживает права доступа и позволяет ограничить доступ одного пользователя к файлам другого пользователя, ее защиты недостаточно. Ведь у одного из этих трех пользователей будут права администратора, и он сможет получить доступ к файлам оставшихся двух пользователей.

Поэтому дисковое пространство жесткого диска можно разделить следующим образом:

- Примерно 200 Гб – общий раздел. Этот раздел также будет системным разделом. На нем будет установлена операционная система, программа и будут храниться общие файлы всех трех пользователей.

- Три раздела по ~100 Гб – думаю, 100 Гб вполне достаточно для хранения личных файлов каждого пользователя. Каждый из этих разделов будет зашифрован, а пароль доступа к зашифрованному разделу будет знать только тот пользователь, который зашифровал этот раздел. При этом администратор при всем своем желании не сможет расшифровать раздел другого пользователя и получить доступ к его файлам. Да, при желании администратор может отформатировать раздел и даже удалить его, но получить доступ он сможет только лишь в том случае, если обманом выведает у пользователя его пароль. Но, думаю, этого не произойдет, поэтому шифрование раздела – гораздо более эффективная мера, чем разграничение прав доступа с помощью NTFS.

9.2. Криптоконтейнеры, или виртуальные диски

Далеко не всегда можно зашифровать весь жесткий диск или даже раздел. Типичный пример – офисный компьютер. Вы хотите, чтобы ваши данные остались секретными, и хотите скрыть их от других коллег, которые, возможно, работают за вашим же компьютером (общее рабочее место), но в то же время у вас нет прав администратора, которые необходимы при шифровании диска или раздела.

В этом случае на помощь придут виртуальные диски, или криптоконтейнеры. Виртуальный диск представляет собой файл, внутри которого находятся ваши данные – файлы и каталоги. Можете смотреть на виртуальный диск как на архив. Только содержимое этого архива зашифровано. Также виртуальный диск можно подмонтировать к какой-то букве, например, к Z, и работать с ним как с обычным диском.

Что лучше – шифровать разделы или использовать виртуальные зашифрованные диски? Здесь каждый решает сам, поскольку у каждого способа есть свои преимущества и недостатки. Шифрование разделов так же надежно, как и шифрование виртуального диска, и наоборот.

Преимущество виртуального диска в том, что его можно легко скопировать на другой жесткий диск или флешку (если позволяет размер). Например, вы можете создать виртуальный диск на 4 Гб (ограничений на размер виртуального диска нет, если не считать естественных) и при необходимости скопировать файл виртуального диска на флешку или на внешний жесткий диск. А при правильном выборе программ шифрования можно использовать

один и тот же диск и на компьютере, и на смартфоне. Например, Android-приложение EDS использует тот же формат виртуальных дисков, что и TrueCrypt. Следовательно, перенести контейнер с компьютера на смартфон – проще простого (лишь бы на SD-карте хватило места). С зашифрованным разделом у вас такое проделать не получится.

Конечно, при необходимости можно создать образ зашифрованного диска – на тот случай, если вы хотите сделать его резервную копию или переместить на другой компьютер. Но это уже отдельная история. Если у вас возникнет подобная потребность, рекомендую программу Clonezilla – уже надежное и проверенное решение. Перенос зашифрованного раздела на другой компьютер – это более сложная затея, чем перенос виртуального диска. Если есть такая необходимость, то проще использовать виртуальные диски.

Какой способ выбрать? Если вы можете себе позволить зашифровать раздел, тогда можно выбрать этот способ. Также весь раздел лучше шифровать, если размер ваших секретных документов довольно большой.

Но есть ситуации, когда использовать весь раздел нельзя или нет смысла. Например, у вас есть только один раздел (диск C:) на жестком диске, и по тем или иным причинам (нет прав, например, поскольку компьютер не ваш) вы не можете или не хотите изменять его разметку, тогда нужно использовать виртуальные диски. Нет смысла шифровать весь раздел, если размер документов (файлов), которые вам нужно зашифровать, небольшой – несколько гигабайт.

9.3. Прозрачное шифрование

Мы уже рассмотрели два способа шифрования данных – шифрование диска/раздела и виртуальные диски. Однако не всегда такое шифрование удобно.

Во-первых, не всегда есть возможность зашифровать весь физический диск. Во-вторых, если вы используете виртуальные диски, то файлы контейнеров, как правило, занимают сотни мегабайт дискового пространства, и их весьма просто обнаружить злоумышленнику. Да, есть методы сокрытия данных, но побеждает человеческая лень. В-третьих, зашифрованная папка может постоянно расти, а размер криптодиска ограничен величиной, указанной при его создании. Конечно, есть программы, позволяющие изменять размер криптодиска после его создания, но на это нужно обращать внимание сразу при выборе программы.

Всем хочется и удобно работать с файлами, и чтобы при этом файлы были надежно защищены. Такой компромисс есть – это прозрачное шифрование файлов, когда файлы зашифровываются и расшифровываются «на лету» – в процессе работы с ними. Файлы остаются зашифрованными, а вы работаете с ними, как с обычными файлами. Например, если вы зашифровали папку C:\Documents и поместили в нее свои документы, то при открытии документа из этой папки запускается Word или Excel, и они даже не подозревают, что они являются зашифрованными. Вы работаете с зашифрованными файлами как с самыми обычными, совершенно не задумываясь о шифровании, монтировании, виртуальных дисках и т.д.

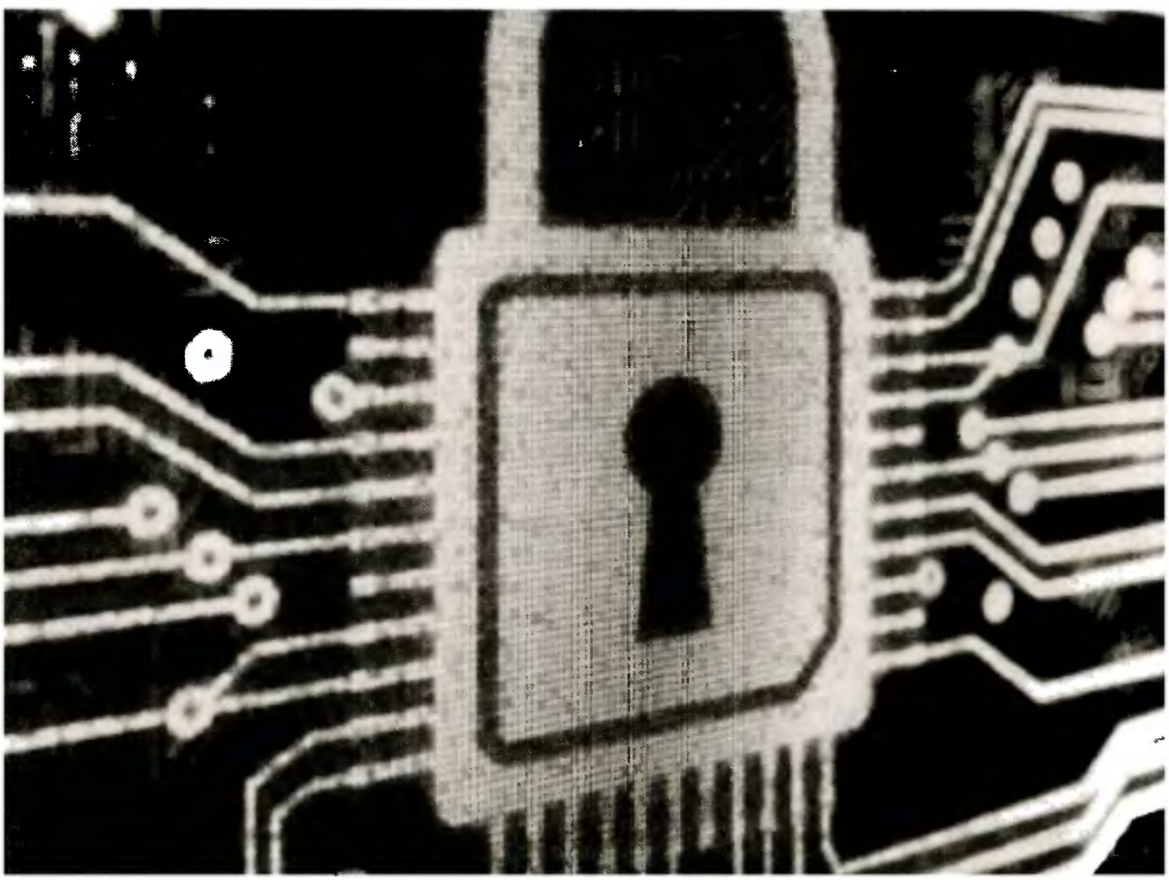
Кроме удобства использования у прозрачного шифрования есть еще одно весомое преимущество. Как правило, на виртуальных зашифрованных дисках хранится большое количество файлов. Для работы даже с одним из них вам нужно подключать весь криптодиск. В результате становятся уязвимыми все остальные файлы. Конечно, можно создать множество небольших криптодисков, присвоить каждому отдельный пароль, но это не очень удобно.

В случае с прозрачным шифрованием можно создать столько зашифрованных папок, сколько вам нужно, и поместить в каждую из них различные группы файлов – документы, личные фото и т.д. При этом расшифровываются только те файлы, к которым осуществляется доступ, а не все файлы криптодиска сразу.

Организовать прозрачное шифрование папки можно как с помощью стандартных средств Windows (Encrypted File System), так и с помощью сторонних программ. В следующей главе мы поговорим о стандартных средствах шифрования в операционных системах Windows и Linux, а именно будут рассмотрены EFS, BitLocker и eCryptFs. Также будет показано, как злоумышленник может расшифровать файлы, зашифрованные EFS.

Глава 10.

Шифрование средствами операционной системы



10.1. Прозрачное шифрование посредством EFS

10.1.1. Преимущества и недостатки EFS

В Windows (начиная с Windows 2000 и кроме Home-выпусков) традиционно для организации прозрачного шифрования используется шифрованная файловая система – EFS (Encrypting File System). Прежде чем вы примете решение, использовать EFS или нет, вам нужно знать о ее преимуществах и недостатках.

Файловая система EFS предназначена, чтобы один пользователь не мог получить доступ к файлам (зашифрованным) другого пользователя. Зачем нужно было создавать EFS, если NTFS поддерживает разграничение прав доступа? Хотя NTFS и является довольно безопасной файловой системой, но со временем появились различные утилиты (одной из первых была NTFSDOS, позволяющая читать файлы, находящиеся на NTFS-разделе, из DOS-окружения), игнорирующие права доступа NTFS. Появилась необходимость в дополнительной защите. Такой защитой должна была стать EFS.

По сути, EFS является надстройкой над NTFS. Файловая система EFS удобна тем, что входит в состав Windows и для шифрования файлов вам не нужно какое-либо дополнительное программное обеспечение – все необходимое уже есть в Windows. Для начала шифрования файлов не нужно совершать какие-либо предварительные действия, поскольку при первом шифровании файла для пользователя автоматически создается сертификат шифрования и закрытый ключ.

Также преимуществом EFS является то, что при перемещении файла из зашифрованной папки в любую другую он остается зашифрованным, а при копировании файла в зашифрованную папку он автоматически шифруется. Нет необходимости выполнять какие-либо дополнительные действия.

Такой подход, конечно же, очень удобен, и пользователю кажется, что от EFS одна только польза. Но это не так. С одной стороны, при неблагоприятном стечении обстоятельств пользователь может вообще потерять доступ к зашифрованным файлам. Это может произойти в следующих случаях:

- Аппаратные проблемы, например, вышла из строя материнская плата, испорчен загрузчик, повреждены системные файлы из-за сбоя жесткого диска (bad sectors). В итоге жесткий диск можно подключить к другому компьютеру, чтобы скопировать с него файлы, но если они зашифрованы EFS, у вас ничего не выйдет.
- Система переустановлена. Windows может быть переустановлена по самым разнообразным причинам. В этом случае доступ к зашифрованным данным, понятно, будет потерян.
- Удален профиль пользователя. Даже если создать пользователя с таким же именем, ему будет присвоен другой ID, и расшифровать данные все равно не получится.
- Системный администратор или сам пользователь сбросил пароль. После этого доступ к EFS-данным также будет потерян.
- Некорректный перенос пользователя в другой домен. Если перенос пользователя выполнен неграмотно, он не сможет получить доступ к своим зашифрованным файлам.

Когда пользователи (особенно начинающие) начинают использовать EFS, об этом мало кто задумывается. Но, с другой стороны, существует специальное программное обеспечение (и далее оно будет продемонстрировано в работе), позволяющее получить доступ к данным, даже если система была переустановлена и были потеряны некоторые ключи. И я даже не знаю, к преимуществам или недостаткам отнести сей факт: данное ПО позволяет восстановить доступ к данным, но в то же время оно может использоваться злоумышленником для получения несанкционированного доступа к зашифрованным файлам.

Казалось бы, данные с помощью EFS зашифрованы очень надежно. Ведь файлы на диске шифруются с помощью ключа FEK (File Encryption Key), который хранится в атрибутах файлов. Сам FEK зашифрован master-ключом, который, в свою очередь, зашифрован ключами пользователей системы, имеющих доступ к этому файлу. Ключи пользователей зашифрованы хэшами паролей этих пользователей, а хэши паролей – зашифрованы еще и SYSKEY.

Казалось бы, такая цепочка шифрования должна была обеспечить надежную защиту данных, но все банально сводится к логину и паролю. Стоит пользователю сбросить пароль или переустановить систему, получить доступ к зашифрованным данным уже не получится.

Разработчики EFS перестраховались и реализовали агентов восстановления (EFS Recovery Agent), то есть пользователей, которые могут расшифровать данные, зашифрованные другими пользователями. Однако использовать концепцию EFS RA не очень удобно и даже сложно, особенно для начинающих пользователей. В итоге, эти самые начинающие пользователи знают, как зашифровать с помощью EFS файлы, но не знают, что делать в нештатной ситуации. Хорошо, что есть специальное ПО, которое может помочь в этой ситуации, но это же ПО может использоваться и для несанкционированного доступа к данным, как уже отмечалось.

К недостаткам EFS можно также отнести невозможность сетевого шифрования (если оно вам нужно, то необходимо использовать другие протоколы шифрования передаваемых по сети данных, например, IPSec) и отсутствие поддержки других файловых систем. Если вы скопируете зашифрованный файл на файловую систему, которая не поддерживает шифрование, например, на FAT/FAT32, файл будет дешифрован, и его можно будет просмотреть всем желающим. Ничего удивительного в этом нет, EFS – всего лишь надстройка над NTFS.

Получается, что от EFS вреда больше, чем пользы. Но чтобы не быть голословным, далее будет приведен пример использования программы Advanced EFS Data Recovery[1] для получения доступа к зашифрованным данным. Сценарий будет самый простой: сначала я войду в систему под другим пользователем и попытаюсь получить доступ к зашифрованному файлу, который зашифровал другой пользователь. Затем я смоделирую реальную ситуацию, когда сертификат пользователя, зашифровавшего файл, был удален (это может произойти, например, в случае переустановки Windows). Как вы увидите, программа без особых проблем справится и с этой ситуацией. Но сначала нам нужно разобраться, как включить EFS-шифрование.

10.1.2. Активация EFS-шифрования

Теперь разберемся, как зашифровать папку (или файл, но как правило, проще зашифровать папку и в нее добавлять файлы, которые должны храниться зашифрованными).

[1] http://www.elcomsoft.ru/aefsdr.html

Щелкните правой кнопкой мыши по папке в Проводнике и выберите команду **Свойства**. В области **Атрибуты** нажмите кнопку **Другие** (рис. 10.1). Включите атрибут **Шифровать содержимое для защиты данных**. Нажмите кнопку **OK**, а затем еще раз **OK** – в окне свойств папки.

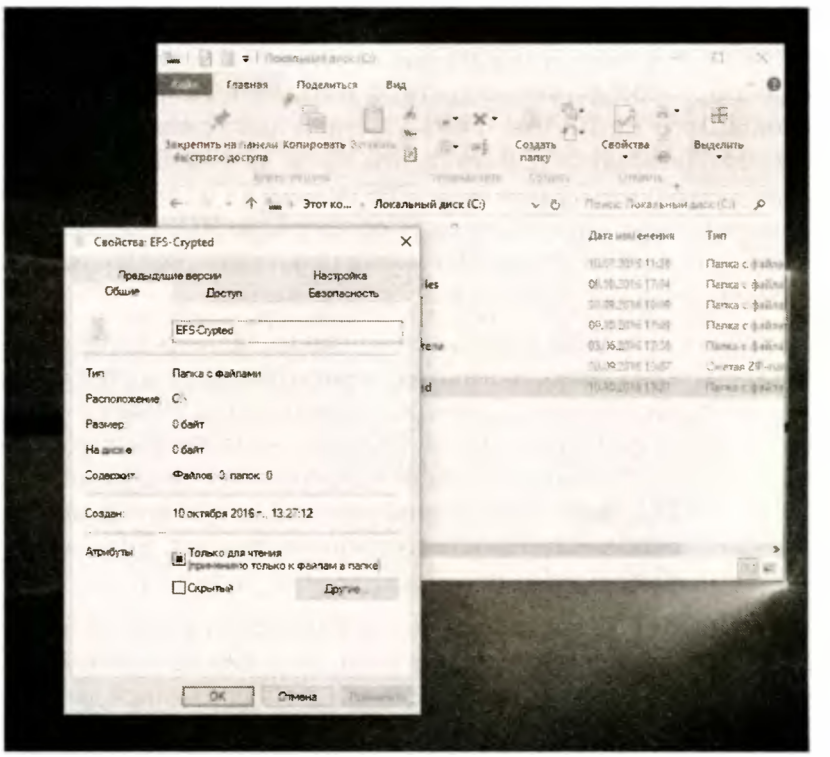


Рис. 10.1. Свойства папки

Если вы шифруете непустой каталог, система спросит, нужно шифровать только эту папку или все вложенные папки и файлы. Лучше выбрать второй вариант.

Все, осталось только подождать, пока файлы будут зашифрованы. Система предложит выполнить резервное копирование вашего ключа шифрования – на всякий неприятный случай (рис. 10.3). Название зашифрованной папки в Проводнике будет отмечено зеленым шрифтом (рис. 10.4). Конечно, черно-белая иллюстрация плохо передает оттенки серого, поэтому предназначена эта иллюстрация в основном для того, чтобы привлечь ваше внимание.

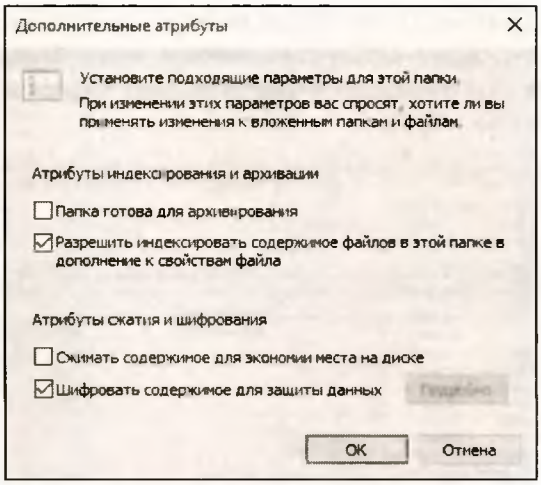


Рис. 10.2. Включение шифрования

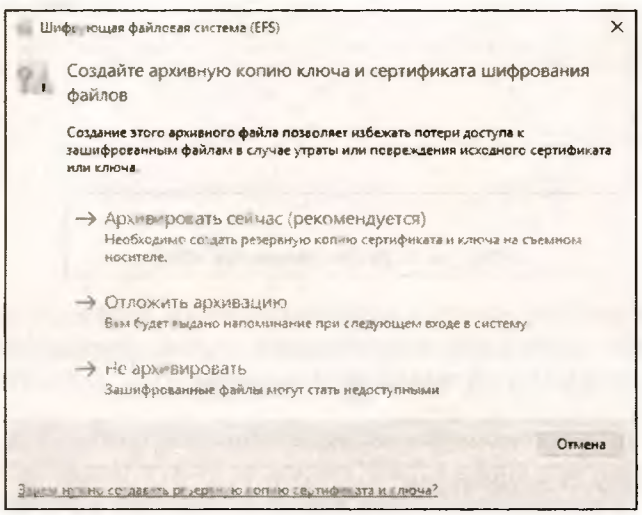


Рис. 10.3. Резервное копирование ключа шифрования

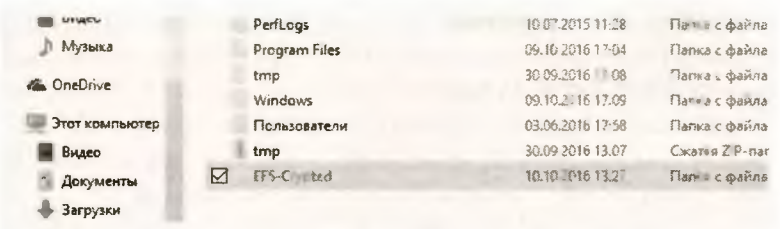


Рис. 10.4. Папка EFS-Crypted зашифрована

Просмотреть созданные сертификаты можно через консоль mmc. Выполните команду mmc, далее выберите команду меню **Файл, Добавить или удалить оснастку**. В появившемся окне выберите **Сертификаты** и нажмите кнопку **Добавить** (рис. 10.5).

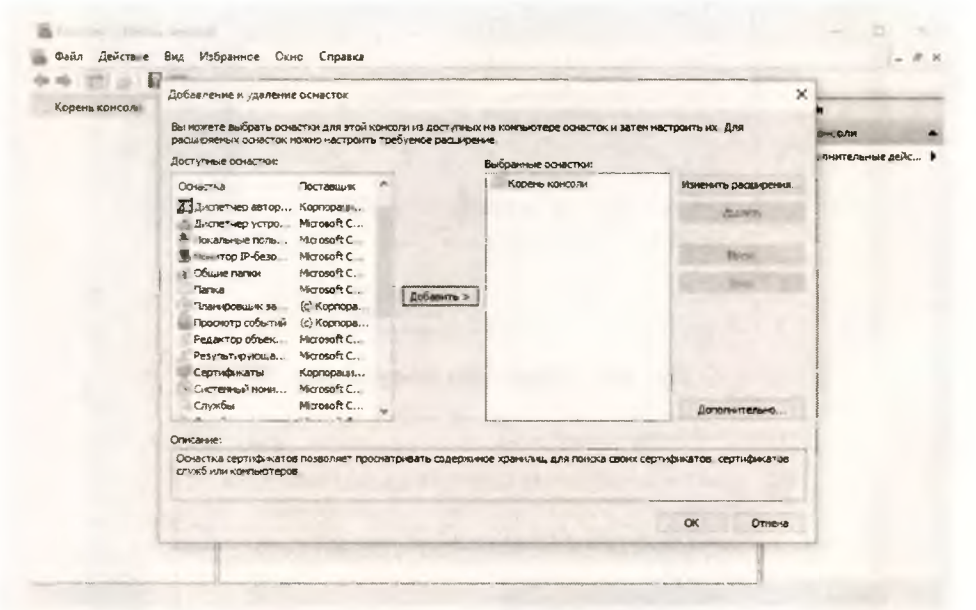


Рис. 10.5. Добавление оснастки

Далее нужно выбрать, какими сертификатами вы хотите управлять. В нашем случае мы хотим управлять личными сертификатами, поэтому выберите **Сертификат учетной записи пользователя** (рис. 10.6). Затем нажмите **ОК** в окне добавления оснастки.

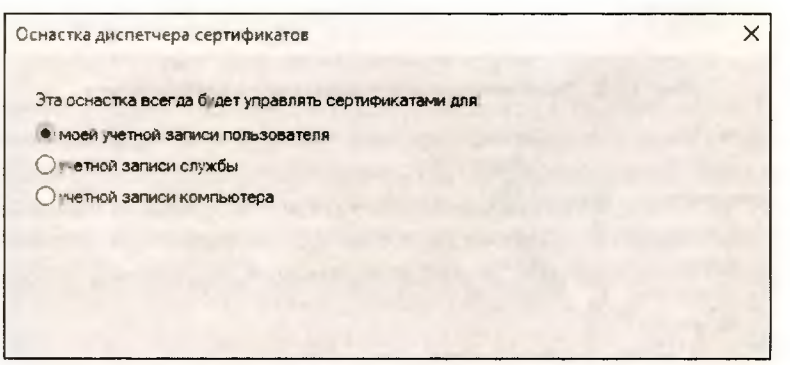


Рис. 10.6. Выбор типа сертификатов

В окне консоли mmc нужно перейти в Сертификаты – текущий пользователь, Личное, Сертификаты, и в списке сертификатов вы увидите сертификат EFS. Если его удалить, вы не сможете получить доступ к зашифрованным файлам.



Рис. 10.7. Список личных сертификатов

10.1.3. Использование программы Advanced EFS Data Recovery для расшифровки зашифрованных EFS файлов

Посмотрим, как можно расшифровать зашифрованные с помощью EFS файлы. Первым делом нужно включить шифрование для одной из папок. Для демонстрации я специально создал папку EFS-Crypted в предыдущем разделе.

Напомню, что названия зашифрованной папки и всех помещенных в нее файлов (которые автоматически будут зашифрованы) в Проводнике отображаются зеленым цветом. В зашифрованную папку я добавил текстовый файл file.txt (рис. 10.8), содержимое которого мы попытаемся просмотреть, войдя в систему под другим пользователем. Для теста был создан другой пользователь с правами администратора (такие права нужны программе Advanced EFS Data Recovery (AEFSDR) компании ElcomSoft), см рис. 10.9.



Рис. 10.9. Создан новый пользователь

Естественно, если зайти под другим пользователем и попытаться прочитать файл file.txt, у вас ничего не выйдет (рис. 10.10).

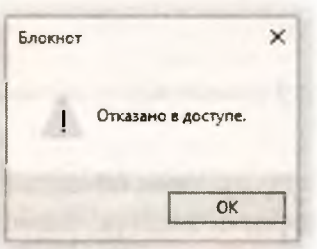


Рис. 10.10. Отказано в доступе

Но не беда – запускаем программу Advanced EFS Data Recovery и переходим сразу в Expert mode (можно, конечно, воспользоваться мастером, который открывается при первом запуске (рис. 10.11), но мне больше нравится экспертный режим). Не забудьте после переключения в экспертный режим выбрать русский язык (Options, Language, Russian).

Итак, перейдите на вкладку Зашифрованные файлы и нажмите кнопку Искать зашифрованные файлы. На рис. 10.13а уже изображен результат сканирования – найден наш единственный зашифрованный файл C:\EFS-Crypted\config.txt. Выделите его и нажмите кнопку Decrypt. Программа предложит вам выбрать каталог, в который нужно дешифровать файлы (рис. 10.13б).



Рис. 10.11. Мастер при запуске Advanced EFS Data Recovery

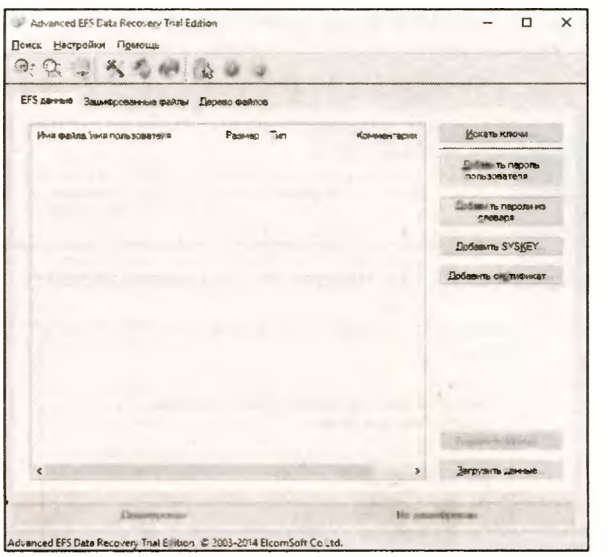


Рис. 10.12. Экспертный режим Advanced EFS Data Recovery

Поскольку у меня пробная версия программы, то для продолжения нужно нажать Продолжить (рис. 10.14). Расшифрованные файлы помещаются в подпапку AEFS_<имя_диска>_DECRYPTED (рис. 10.15). Обратите внимание – наш файл config.txt уже не выделен зеленым, и мы можем просмотреть его содержимое (рис. 10.15).

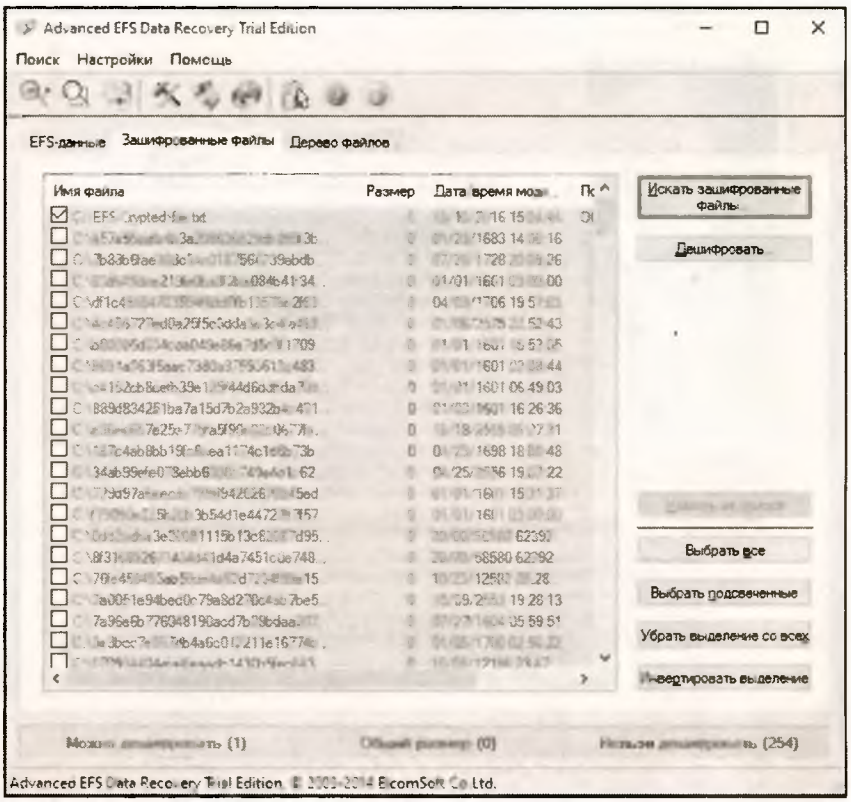


Рис. 10.13а. Найден зашифрованный файл

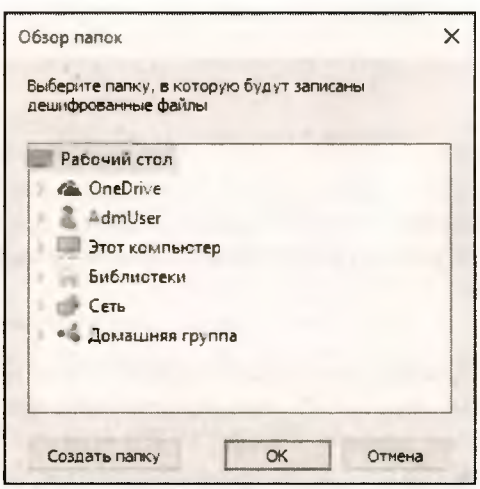


Рис. 10.13б. Выберите каталог, в который будут дешифрованы файлы

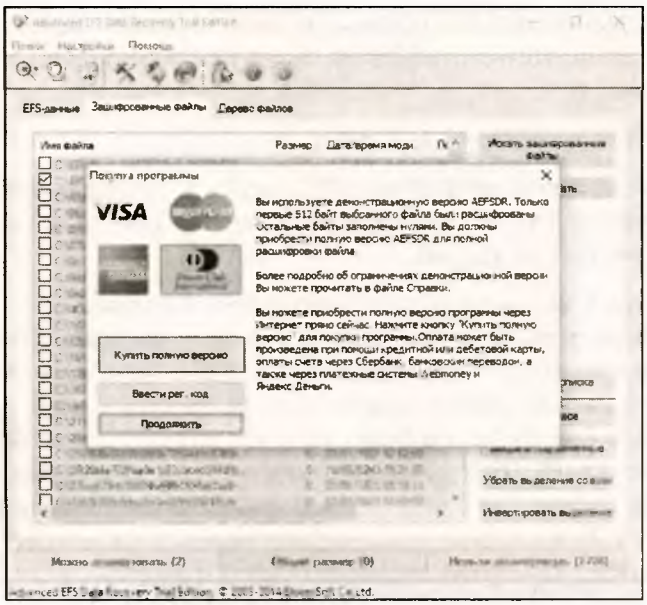


Рис. 10.14. Нажмите кнопку Continue

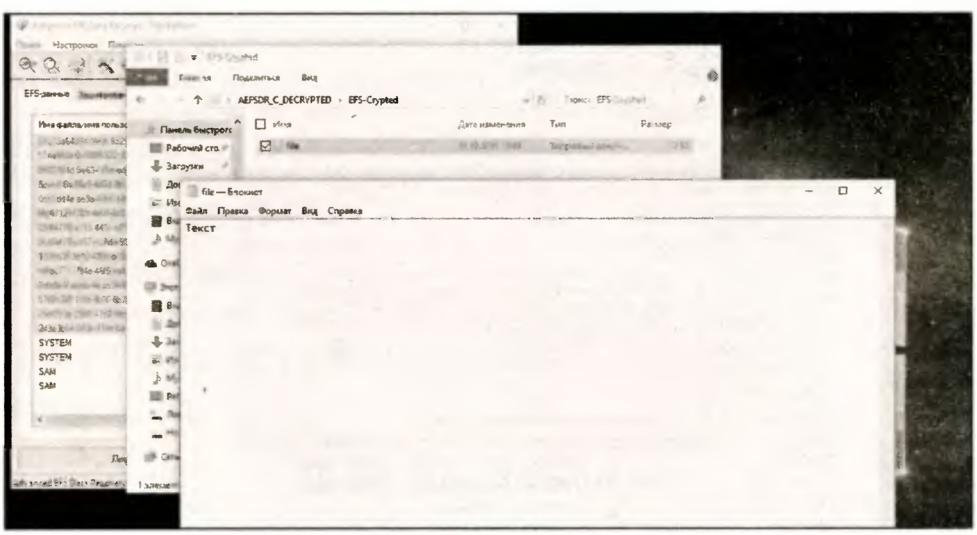


Рис. 10.15. Расшифрованный файл и содержимое файла config.txt

Теперь усложним задачу программе Advanced EFS Data Recovery, а именно – удалим личный сертификат. Войдите как пользователь, создавший зашифрованную папку, запустите консоль mmc и откройте список личных сертификатов (как было показано ранее). Удалите ваш личный сертификат.

Вы увидите предупреждение о том, что расшифровать данные, зашифрованные с помощью этого сертификата, будет уже невозможно. Что ж, скоро мы это проверим.

Далее выполните следующие действия:

- Закройте оснастку и попробуйте обратиться к зашифрованному файлу. У вас ничего не выйдет, несмотря на то, что вы зашифровали этот файл. Ведь сертификат-то удален.
- Смените пользователя, запустите программу Advanced EFS Data Recovery. Попробуйте расшифровать файл, как было показано ранее. Сначала программа сообщит, что сертификат не найден. Поэтому нужно перейти на вкладку **EFS-данные** и нажать кнопку **Искать ключи**. Через некоторое время программа сообщит вам, что нашла ключи, но, вероятно, не все (рис. 10.16). Программа рекомендует вам просканировать ключи еще раз, но на этот раз с включенной опцией **Сканировать посекторно** (рис. 10.17), но я этого не делал и сразу перешел на вкладку **Зашифрованные файлы**. Программа успешно нашла и дешифровала файл.

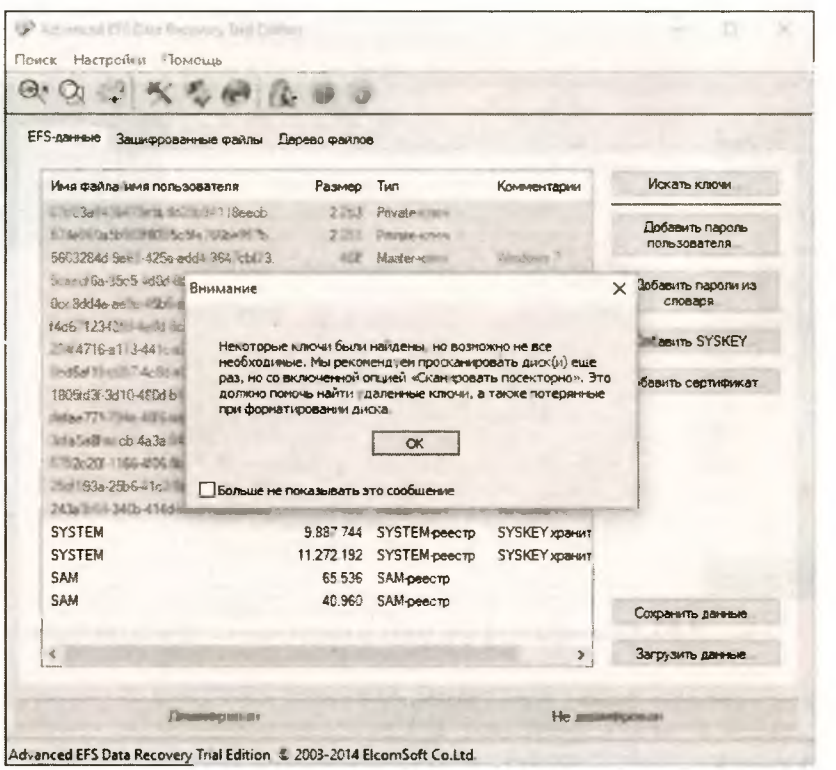


Рис. 10.16. Найдены не все ключи

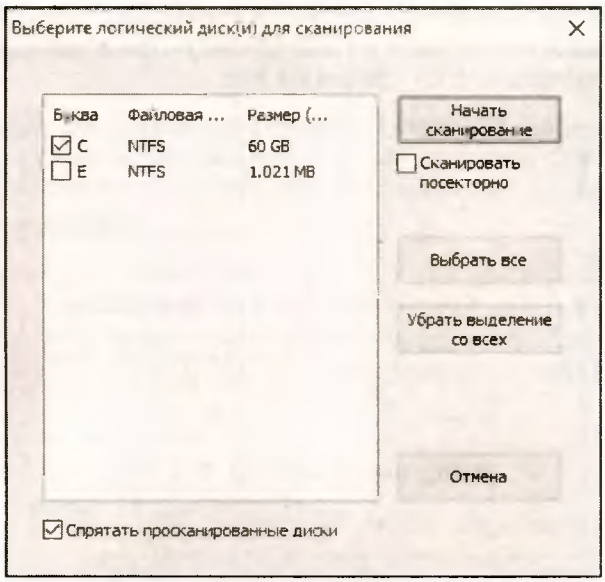


Рис. 10.17. Включите режим Сканировать посекторно

К стыду EFS или к чести Advanced EFS Data Recovery, в обоих случаях файл был расшифрован. При этом, как видите, мне не понадобились какие-то специальные знания или навыки. Достаточно запустить программу, которая сделает за вас всю работу. О том, как работает программа, можно прочитать на сайте разработчиков[2]. Единственное, что может усложнить работу программы, – наличие сложного пароля для учетной записи. Только он может спасти ваши данные. Если вы собираетесь использовать EFS, тогда прямо сейчас установите сложный пароль. В этом случае у программы, возможно, ничего не получится.

10.2. Средство шифрования диска BitLocker

10.2.1. Что такое BitLocker

BitLocker (полное название BitLocker Drive Encryption) – это технология шифрования диска, встроенная в операционные системы Windows Vista Ultimate/Enterprise, Windows 7 Ultimate, Windows Server 2008 R2, Windows Server 2012/R2, Windows 8 и Windows 10.

2 http://www.elcomsoft.ru/

Используя BitLocker, можно зашифровать полностью весь носитель данных (логический диск, SD-карту, USB-брелок). При этом поддерживаются алгоритмы шифрования AES 128 и AES 256.

Если быть предельно точным, то можно зашифровать следующие типы устройств:

- USB;
- Firewire;
- SATA;
- SAS;
- ATA;
- IDE;
- SCSI;
- eSATA;
- iSCSI;
- Fiber Channel.

При этом ключ шифрования хранится в компьютере, TPM или USB-брелке. Доступны следующие варианты ограничения доступа к диску: TPM, TPM + PIN + USB, TPM + USB, TPM + PIN.

BitLocker, в отличие от некоторых других программ шифрования, может зашифровать системный диск – диск, с которого происходит загрузка Windows. Однако это не рекомендуется делать по причине снижения производительности работы системы – зачем шифровать системные файлы, программы и т.д.? Гораздо рациональнее зашифровать только тот диск, на котором вы храните свои данные. В Microsoft сообщают, что производительность при включении шифрования системного диска станет ниже на 10%.

Поэтому лучше всего зашифровать отдельный том – отдельный логический диск, внешний USB-диск и т.д. Затем на этот зашифрованный диск поместить все ваши секретные файлы. Также можно установить на этот диск программы, требующие защиты, например, клиент-банк. Такой диск вы будете подключать только при необходимости. Дважды щелкнул на значке диска, ввел пароль и получил доступ к данным – будет именно такой принцип работы с зашифрованным диском.

Иногда, конечно, есть смысл шифровать и системный диск, например, когда нужна полная секретность. Ведь многие программы, например, те же брау-

зеры, собирают очень много информации, которую можно использовать в случае чего против вас. Зашифровав эту информацию, вы тем самым обезопасите себя.

Конечно, у BitLocker есть и ограничения. Например, нельзя зашифровать том, подключенный по Bluetooth. Нельзя зашифровать файловые системы CDFS, NFS, DFS, LFS, программные RAID-массивы (аппаратные RAID-массивы поддерживаются).

Огромным преимуществом BitLocker является поддержка шифрования GPT-дисков. Из проверенных средств шифрования поддержку GPT обеспечивают продукты от Symantec (например, Symantec Endpoint Encryption), но за них нужно платить, а стоимость BitLocker уже включена в состав Windows.

10.2.2. Шифрование диска

Запустите Проводник и щелкните правой кнопкой мыши по диску, который вы хотите зашифровать. Из появившегося меню выберите команду **Включить BitLocker** (рис. 10.18).

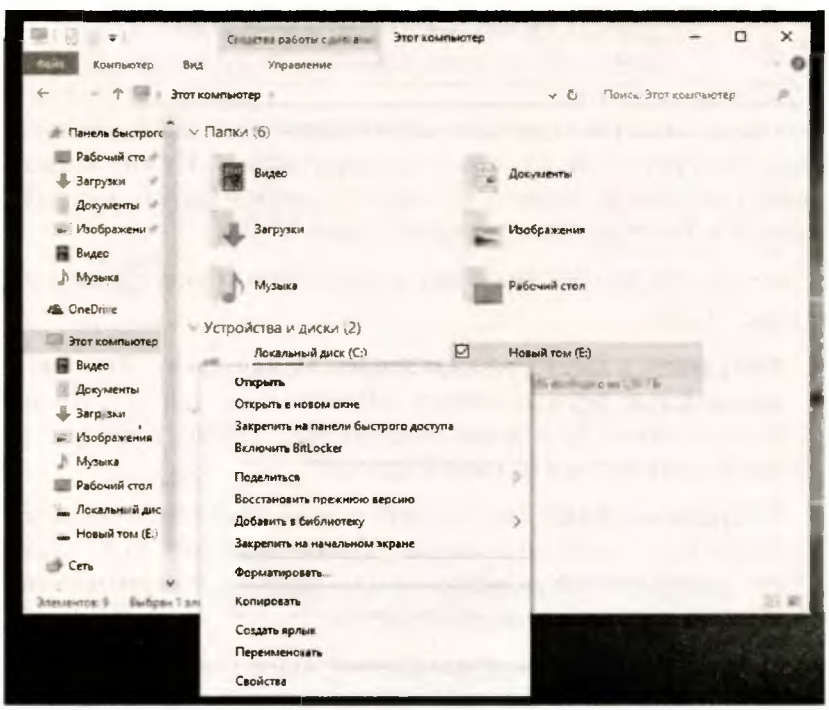


Рис. 10.18. Команда включения BitLocker

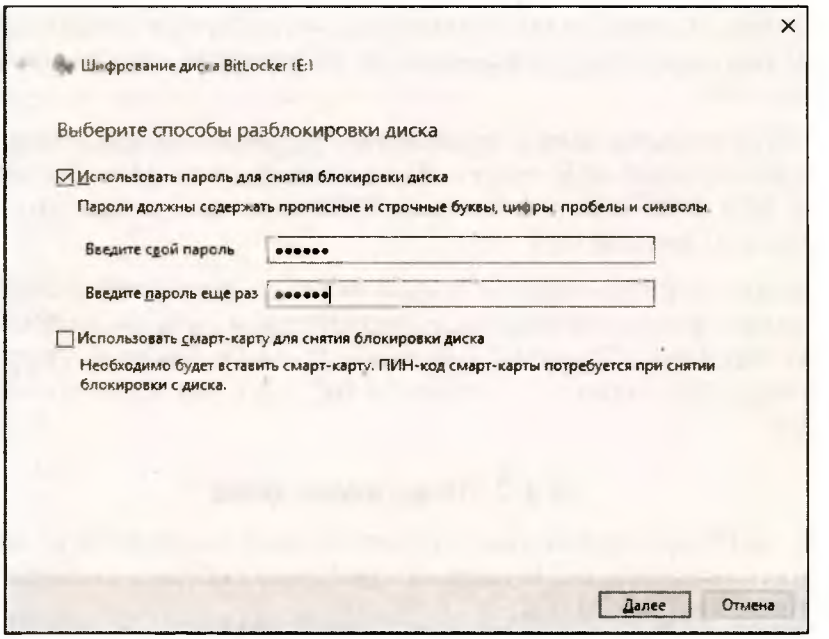


Рис. 10.19. Как будем снимать блокировку?

Нужно указать, как вы будете снимать блокировку с зашифрованного диска: с помощью пароля или с помощью смарт-карты. Нужно выбрать один из вариантов (или оба: тогда будут задействованы и пароль, и смарт-карта), иначе кнопка **Далее** не станет активной (рис. 10.19).

Далее система предложит вам создать резервную копию ключа восстановления (рис. 10.20):

- **Сохранить в вашу учетную запись Майкрософт**. Этот способ я не рекомендую: нет соединения с Интернетом – получить свой ключ не получится. Да и зачем Майкрософт хранить ключ восстановления ваших данных на своем сервере?
- **Сохранить в файл.** Это лучший способ. Файл с ключом восстановления будет записан в каталог **Документы** (рис. 10.21). После этого нужно будет переместить его на флешку, переименовать, а саму флешку спрятать в надежное место.
- **Напечатать ключ восстановления**. Идея очень странная, но если хочется, то почему бы нет?

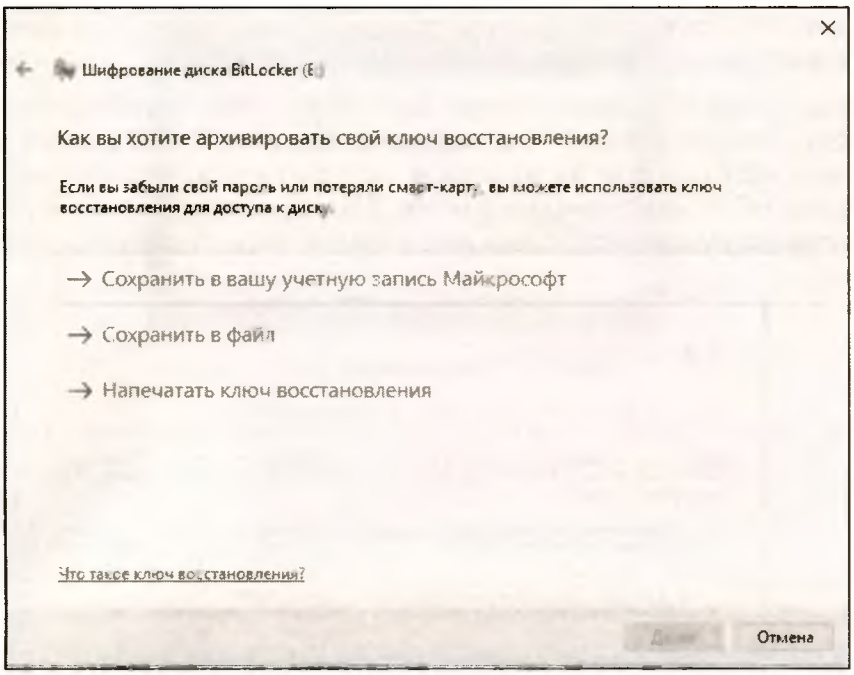


Рис. 10.20. Архивация ключа восстановления

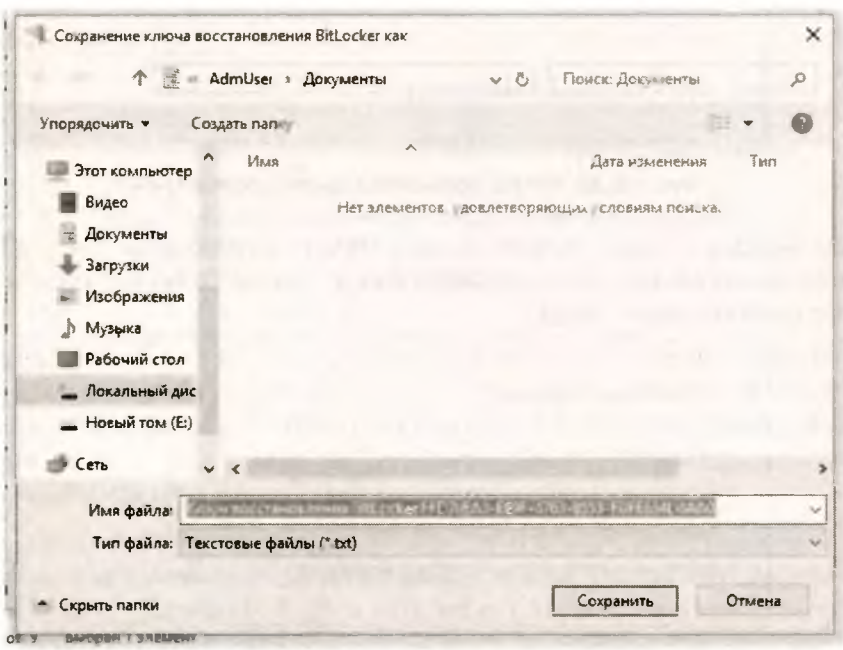


Рис. 10.21. Сохранение ключа восстановления в документах

После сохранения ключа вы вернетесь в окно с выбором метода сохранения. Нажмите кнопку **Далее** для перехода к следующему этапу.

Теперь нужно определить, какую часть диска требуется шифровать (рис. 10.22). Есть два варианта – зашифровать весь диск и зашифровать только занятое место на диске. Если на диске мало данных, то лучше выбрать шифрование только занятого пространства. Но если вы боитесь, чтобы никто не восстановил удаленные ранее с диска файлы, тогда лучше шифровать весь диск.

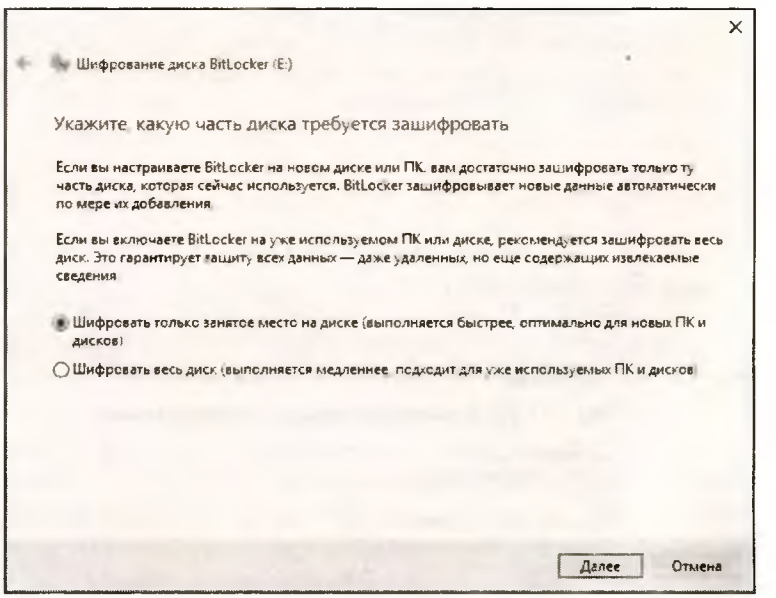


Рис. 10.22. Какую часть диска нужно зашифровать?

Итак, осталось только нажать кнопку **Начать шифрование** (рис. 10.23) и подождать, пока диск будет зашифрован, о чем вы получите уведомление, изображенное на рис. 10.24.

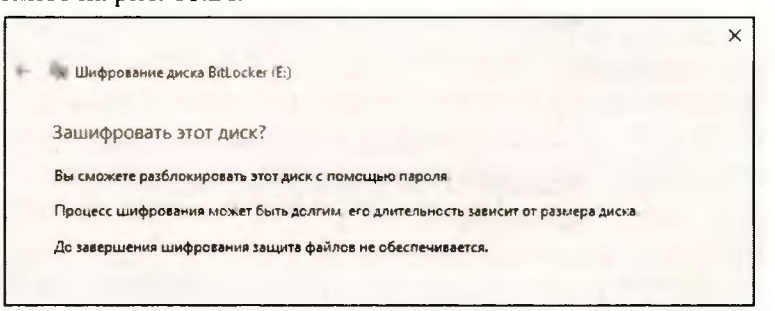


Рис. 10.23. Нажмите кнопку Start encrypting

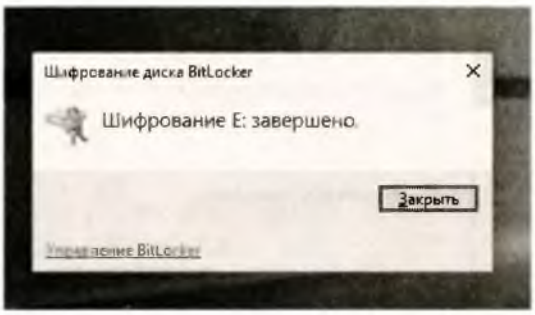


Рис. 10.24. Шифрование завершено

Важно не выключать питание компьютера и не перезагружать его, пока шифрование не будет завершено. В принципе, ничего страшного, если произойдет сбой питания – тогда шифрование будет продолжено с момента остановки, но так ли это на самом деле, я проверять не стал.

10.2.3. Работа с зашифрованным диском

В проводнике Windows зашифрованный диск помечен значком замка: у заблокированного диска замок закрыт, у разблокированного – открыт. Незашифрованный диск выводится без замка (рис. 10.25).



Рис. 10.25. Зашифрованный и незашифрованный диски

Наш зашифрованный диск заблокирован, и чтобы его разблокировать, следует щелкнуть по нему двойным щелчком. Если вы выбрали только защиту паролем, понадобится ввести этот пароль (рис. 10.26), а если была выбрана и смарт-карта, то для успешной аутентификации и разблокировки диска нужно еще вставить и ее.

После разблокировки с зашифрованным диском вы можете работать как с обычным. Для изменения пароля щелкните правой кнопкой по диску и выберите команду **Изменить пароль BitLocker** (она появится после того, как вы ввели уже текущий пароль).

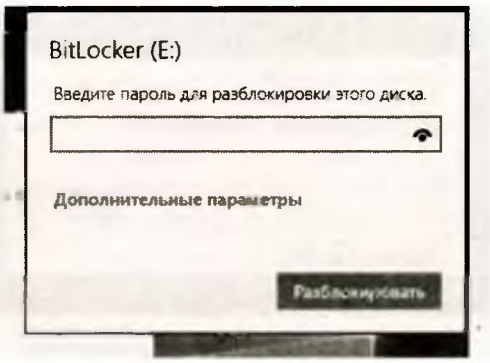


Рис. 10.26. Разблокировка диска

10.2.4. Забыт пароль. Что делать?

Теперь рассмотрим ситуацию, когда вы забыли пароль или утеряли смарт-карту. Откройте файл, содержащий ключ восстановления, и скопируйте содержащийся там ключ в буфер обмена. Нажмите в окне ввода пароля (см. рис. 10.26) кнопку **Дополнительные параметры**. Выберите в открывшемся окне команду **Введите ключ восстановления**. Вам останется только вставить в соответствующее поле ключ восстановления из буфера обмена (рис. 10.27).

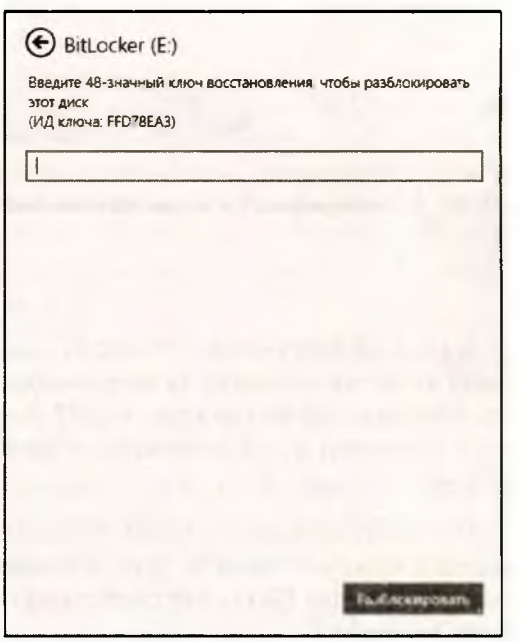


Рис. 10.27. Ввод ключа восстановления

10.3. Файловая система eCryptfs в Linux

В Linux также есть средства шифрования, а именно криптографическая файловая система eCryptfs. Использовать ее довольно просто, в чем вы сейчас и убедитесь.

Первым делом нужно установить утилиты eCryptfs. В Ubuntu/Debian для их установки используется apt-get:

```
sudo apt-get install ecryptfs-utils
```

Перед шифрованием домашнего каталога на всякий случай сделаем резервную копию – мало ли чего:

```
sudo cp -pfr ~ /tmp
```

Теперь приступим к шифрованию домашнего каталога. Чтобы его зашифровать, нужно его подмонтировать, указав тип файловой системы ecryptfs:

```
sudo mount -t ecryptfs /home/user /home/user
```

В процессе выполнения этой команды нужно ввести секретную фразу (она будет использоваться для расшифровки каталога), а на остальные вопросы программы (алгоритм, длина ключа) можно отвечать нажатием Enter.

На данный момент /home/user зашифрован. Восстановим наш бэкап и удалим его (чтобы никто не смог его прочитать):

```
sudo cp -pfr /tmp/user /home/
sudo rm -fr /tmp/user
```

Осталось самое главное – проверить, а зашифрован ли на самом деле каталог? Попробуем скопировать в него любой файл из незашифрованной файловой системы:

```
cp /etc/motd /home/user
```

Размонтируем зашифрованный каталог:

```
sudo umount /home/user
```

Теперь пробуем прочитать /home/user/motd:

```
cat /home/user/motd
```

Если вы увидите всякого рода иероглифы и абракадабру, значит, шифрование работает.

10.4. Можно ли доверять стандартному шифрованию?

В этой главе были рассмотрены три стандартных способа шифрования данных: EFS, BitLocker и eCryptfs (Linux). Все три способа довольно надежны. Нарекание вызывает лишь EFS. Как было показано в этой книге, если пароль учетной записи не очень надежный (или его вообще нет), расшифровать данные не составит никакого труда. Но если пароль надежный, придется попотеть, чтобы получить доступ к EFS. Также нужно помнить о непригодности EFS к шифрованию сетевых папок – ведь по сети данные будут передаваться в расшифрованном виде, следовательно, их могут перехватить.

Что же касается BitLocker, то, насколько я знаю, нет утилит, способных взломать его защиту. Останавливает одно – проприетарность его кода. Код BitLocker закрыт, и о наличии/отсутствии «черных ходов» в нем знает лишь Microsoft и, возможно, всем известные АНБ и ЦРУ.

Если вы не агент МИ6, то беспокоиться вам нечего. Ваши коллеги и родственники при всем своем желании не смогут получить доступ к вашим данным.

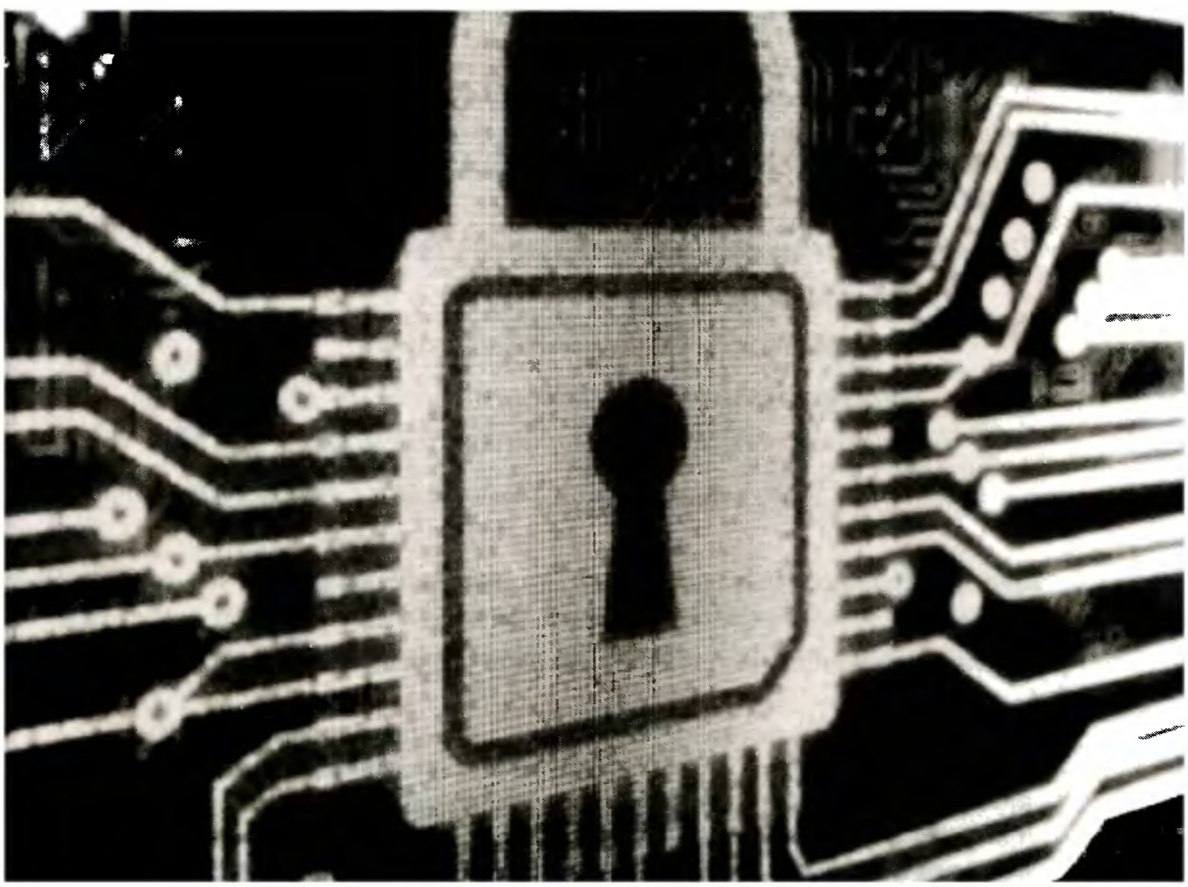
Файловая система eCryptfs обладает открытым исходным кодом, поэтому беспокоиться нечего – ваши данные точно в безопасности.

По сути, стандартные средства весьма надежны, особенно BitLocker. Только не забывайте выполнять резервное копирование ключей, иначе ваши данные уже никто и никогда не восстановит. Впрочем, это касается не только стандартных, но и сторонних средств шифрования.

Однако если у вас легкая степень паранойи или вы все-таки секретный агент, тогда вам стоит обратить свое внимание на сторонние средства шифрования, которые будут описаны в последующих главах.

Глава 11.

Шифрование жесткого диска сторонними программами. TrueCrypt и ее производные



11.1. Выбор сторонней программы для шифрования

В мире существует очень много различных программ для шифрования данных. Намного больше, чем вы можете себе представить. Первым делом нужно определиться с функциями, необходимыми вам, а потом уже искать подходящую программу.

Составьте список необходимых вам функций, например:

- Шифрование разделов
- Шифрование всего диска (системного диска)
- Двухфакторная аутентификация
- Поддержка виртуальных дисков (криптоконтейнеров)
- Формат виртуальных дисков, совместимый с мобильными приложениями

Далее для подбора программы, соответствующей вашим требованиям, посетите страничку сравнения программ для шифрования данных:

https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

В книге подобную табличку приводить не хочется по двум причинам. Во-первых, список программ обновляется, и со временем появляются новые приложения. Например, на момент написания книги просто может не быть приложения, которое соответствует всем вашим пожеланиями. Но оно может появиться месяц спустя. Велика вероятность, что оно появится на страничке в википедии.

Во-вторых, функционал существующих программ может быть расширен. Если сегодня нет нужной вам функции, завтра она может появиться.

Теперь вернемся к нашему списку. Если просмотреть таблицу функций, то TrueCrypt соответствует всем требованиям, кроме последнего. Да, нет версии программы TrueCrypt для Android, но есть приложение EDS Lite, которое поддерживает формат дисков TrueCrypt.

11.2. Программа TrueCrypt

11.2.1. История TrueCrypt и что случилось с проектом

Первая версия TrueCrypt появилась 2 февраля 2004 года. Изначально программа была основана на проекте E4M (Encryption for the Masses). Проект E4M появился в 1997 году и был очень популярен среди пользователей – еще бы: бесплатная программа открытым кодом для шифрования «на лету». Но в 2000 году работа над проектом была приостановлена, поскольку создатель E4M переключился на коммерческие разработки.

Разработчики TrueCrypt взяли за основу код программы E4M. В 2004 году TrueCrypt была единственной программой с открытым исходным кодом для шифрования на лету и с полной поддержкой Windows XP, чем не могли похвастаться другие бесплатные программы.

Настоящий прорыв в развитии программ произошел с выходом четвертой версии в 2005 году: тогда программа стала кроссплатформенной – появилась ее Linux-версия. Но кроме этого была добавлена поддержка x86-64, хэш-алгоритм Whirlpool и многое другое. В том же 2005 году (в версии 4.1) была существенно увеличена стабильность работы благодаря использованию нового режима работы (LRW).

В 2006 году программа «научилась» создавать тома, изменять пароли и ключевые файлы, генерировать ключевые файлы и создавать резервные копии заголовков томов. А для Windows NT появилась поддержка динамических томов.

В 2007 году появилась полная поддержка 32- и 64-разрядных версий Windows Vista, а также были исправлены некоторые ошибки. Что же касается Linux, то пока для этой операционной системы даже не был разработан графический интерфейс. Он появился только лишь в пятой версии, которая вышла в 2008 году. В этой же версии появилась поддержка шифрования всей файловой системы Windows, в том числе и системного раздела.

В версии 5.1 (тоже 2008 год) реализация алгоритма AES была переписана на язык Ассемблер. Ранее она была написана на языке C. В результате производительность шифрования диска существенно выросла.

В шестой версии тоже появились довольно интересные возможности:

- Параллельное шифрование/дешифрование, что повышает производительность на многоядерных и многопроцессорных системах.
- Возможность создания скрытых разделов при работе с Linux и Mac OS.
- Возможность установки скрытых операционных систем, существование которых невозможно доказать (интересная возможность для пиратов).

Поддержка Windows 7 появилась только в версии 6.3. Так что если по какой-то причине придется использовать не последнюю версию (на момент написания этих строк – 7.1), то не устанавливайте версию ниже 6.3.

В версии 7.0 еще больше ускорили алгоритм AES, появилась возможность автоматического монтирования томов, поддержка больших томов с размером сектора 1024, 2048 и 4096 байт, а также теперь TrueCrypt умеет шифровать файл подкачки Windows, который может содержать конфиденциальную информацию.

28 мая 2014 года проект был закрыт, разработка свернута. Все старые версии удалены, репозиторий очищен. Обстоятельства закрытия проекта вызвали бурную общественную реакцию. За всю свою историю TrueCrypt ни разу не была скомпрометирована. Даже был проведен независимый аудит, который не нашел каких-либо слабых сторон, закладок и прочих не очень хороших моментов в этой программе. И вот внезапно разработчики заявили о закрытии проекта.

Проанализировав многочисленные форумы с догадками о том, что же все-таки произошло, пришел к выводу, что без вмешательства третьей стороны не обошлось. Но вот кто был этой третьей стороной и какие условия были предложены разработчикам проекта, того никто не знает (кроме, понятное дело, самих разработчиков).

Тогда же, 28 мая 2014 года, вышла финальная версия 7.2. Данная версия не может шифровать данные, ее можно использовать только для расшифровки. Последняя полноценная версия – 7.1a. Специально для читателей этой книги ее можно скачать с моего сайта:

http://dkws.org.ua/files/truecrypt.zip

В этом архиве не только Windows-версия, но и версии для MacOS и Linux. Если вас смущает то, что версия будет старовата и давно не обновлялась (хотя даже в 2016 году не было найдено никаких уязвимостей в TrueCrypt), вы можете использовать VeraCrypt или CipherShed. Обе программы являются форками (человеческим языком – потомками) программы TrueCrypt. Их возможности примерно такие же, как у TrueCrypt. Далее мы рассмотрим эти программы подробнее.

> **Важно!** К сожалению, разработчики TrueCrypt не успели реализовать поддержку UEFI/GPT в последней версии программы. А это означает, что зашифровать системный GPT-диск этой программой невозможно. Более того, поддержка GPT не реализована ни в одном из форков этой программы (VeraCrypt, CipherShed, DiskCryptor и т.д.). Поэтому если вам нужно зашифровать системный GPT-диск, то выхода два. Первый заключается в использовании BitLocker. Второй – в преобразовании диска в формат MBR. Разработчики VeraCrypt обещают реализовать поддержку GPT, но этим обещаниям уже два года (с 2014 года), а поддержки GPT как не было, так и нет.

11.2.2. Возможности программы

TrueCrypt умеет создавать зашифрованный виртуальный диск тремя способами:

- В виде файла, который легко использовать: вы можете перенести или скопировать этот файл, скажем, на флешку или USB-диск, не заботясь о файловой системе, в которой отформатирован носитель. Даже если он будет отформатирован как FAT32, это никак не повлияет на качество шифрования. Размер такого файла – динамический и увеличивается по мере добавления в него новых файлов и каталогов – вплоть до всего свободного места на разделе. Однако если предполагается работа с большим объемом зашифрованных данных, лучше сразу зашифровать весь раздел – так производительность работы с зашифрованными данными будет выше.
- С помощью полного шифрования содержимого устройства. Этот способ подходит для флешек и внешних USB-дисков. Дискеты, увы, уже не актуальны, поэтому не поддерживаются современными версиями TrueCrypt.
- С помощью шифрования одного из разделов жесткого диска. Вы можете зашифровать раздел жесткого диска и поместить на него все ваши конфиденциальные документы, в том числе и базу данных вашего почтового клиента.

Шифрование TrueCrypt очень надежно. Программа поддерживает алгоритмы шифрования AES, Serpent, Twofish и др. К тому же программа поддерживает «вложенное» шифрование различными алгоритмами, например, можно сначала зашифровать данные алгоритмом AES, затем – Serpent, а затем – Twofish. Программа позволяет выбрать одну из трех хеш-функций: HMAC-RIPEMD-160, HMAC-Whirlpool, HMAC-SHA-512 для генерации ключей шифрования, соли и ключа заголовка.

Все алгоритмы шифрования используют безопасный режим работы, что позволяет выполнять шифрование и дешифровку данных «на лету», не боясь их потерять.

Для доступа к зашифрованным данным может использоваться пароль (ключевая фраза), ключевые файлы или и пароль, и ключевые файлы. Самый надежный способ – это использование для доступа к данным и пароля, и ключевых файлов. Чуть менее надежный – только ключевых файлов. Ну и самый простой (конечно, относительно – все зависит от пароля) – только пароля.

С ключевыми файлами все не так просто. Ведь возникает необходимость их постоянно копировать, хранить где-нибудь и т.д. Нет смысла хранить ключевые файлы вместе с зашифрованным томом TrueCrypt – сами понимаете, почему. Поэтому зачастую пользователи предпочитают использовать только пароль для доступа к данным. Пароль, в конце концов, можно просто запомнить. Не нужно беспокоиться о том, что нужно скопировать его куда-нибудь, он всегда с вами.

Что же касается ключевых файлов, особенность TrueCrypt заключается в том, что в качестве таких файлов могут использоваться любые файлы на вашем жестком диске, а не специальные сертификаты, кем-то проверенные и кем-то подписанные.

Вы создаете любой файл, пусть это будет обычный документ, и с его помощью зашифровываете целый раздел. Злоумышленник никогда не догадается, какой именно файл вы выбрали.

Однако возникает небольшой нюанс: если вы потеряете этот файл (вы или кто-то еще его случайно удалит или же произойдет сбой на жестком диске и будет поврежден хотя бы один байт этого файла), вы уже не сможете получить доступ к своим данным.

Программу TrueCrypt можно запускать без установки в операционной системе – для запуска программы вам не нужны права группы администраторов. А это очень удобно – не всегда есть возможность установить программу, поскольку не хватает прав доступа. В случае с TrueCrypt для использования

программы не нужны права администратора, вы можете использовать программу с обычными правами пользователя.

Вот некоторые второстепенные особенности программы:

- Изменение пароля и ключевых файлов зашифрованного тома без потери зашифрованных данных, так что пароли менять не только можно, но и нужно.
- Возможность назначения «горячих клавиш» для различных операций, например, для монтирования или размонтирования зашифрованного тома.
- Возможность резервного сохранения заголовка тома, что полезно при восстановлении информации в случае повреждения тома и для восстановления старого пароля – который был действителен для старого заголовка.
- Шифрование системного физического или логического диска. Да, вы можете зашифровать даже системный диск, аутентификация (ввод пароля) будет дозагрузочной – очень удобно.

11.2.3. Использование программы

Установка программы

Запустите программу установки. Первым делом она предложит прочитать лицензию TrueCrypt – она чем-то напоминает GPL, но все же отличается от нее. Особо можете не вдаваться в подробности, примите лицензию и нажмите кнопку **Next**. Далее нужно будет выбрать один из режимов установки (рис. 11.1):

- **Install** – самая обычная установка, для продолжения вам нужны права администратора. В большинстве случаев (если вы сам владелец компьютера, на который устанавливается программа) нужно выбрать этот вариант.
- **Extract** – обычное извлечение файлов программы в выбранный вами каталог. Фактически происходит извлечение мобильной (Portable) версии программы. Для продолжения права root не нужны, поскольку установка не выполняется. При желании программу можно извлечь на флешку и на этой же флешке создать зашифрованный файл, в котором и будете хранить все ваши конфиденциальные данные. Для запуска программы нужно запустить исполнимый файл TrueCrypt.exe непосредственно из каталога установки (который будет находиться на флешке). У этого способа есть один

недостаток, иначе все бы только и работали с TrueCrypt в portable-режиме. Система UAC будет ругаться каждый раз при запуске TrueCrypt, что очень неудобно, когда работаешь с зашифрованным томом каждый день. С другой стороны, предупреждение UAC будет отображено всего один раз – при запуске TrueCrypt, раз в день можно и потерпеть.

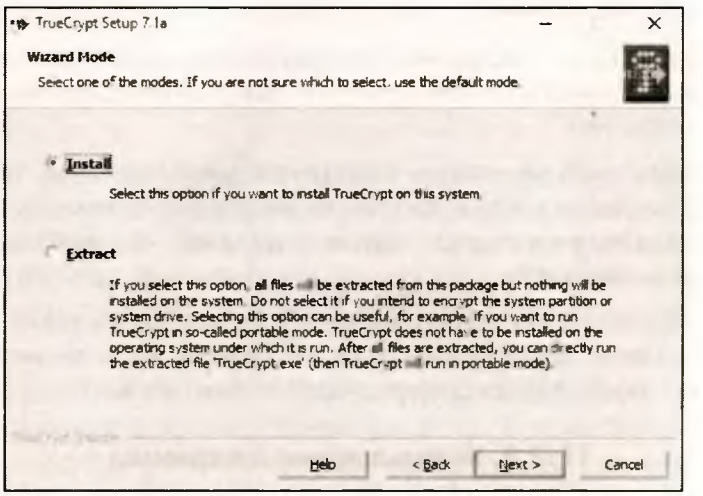


Рис. 11.1. Выбор варианта установки программы

Установка TrueCrypt похожа на установку других программ. Нажимайте **Next**, пока не увидите уведомление об успешной установке (рис. 11.2).

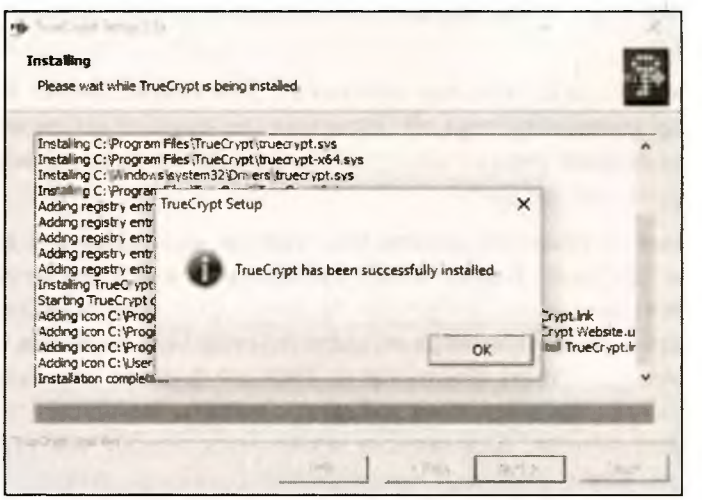


Рис. 11.2. Программа TrueCrypt успешно установлена



Рис. 11.3. Программа TrueCrypt

Запустите программу (рис. 11.3). Она отобразит список незанятых букв устройств. Содержимое списка зависит от количества разделов на вашем жестком диске (или дисках) и подключенных носителей данных.

Создание виртуального диска (контейнера)

Нажмите кнопку **Create Volume**. Не волнуйтесь, несмотря на то, что в названии этой кнопки и есть слово «Volume» (том), создавать еще один раздел на жестком диске никто не будет. Ваша таблица разделов останется в целости и сохранности. Программа предложит вам один из вариантов (рис. 11.4):

- **Create an encrypted file container** – создать виртуальный зашифрованный диск (криптоконтейнер). Он будет сохранен в файловой системе как обычный файл. В большинстве случаев рекомендуется именно этот вариант. Конечно, при условии, что у вас относительно немного данных (скажем, несколько гигабайтов), подлежащих шифрованию. Если же нужно зашифровать несколько сотен гигабайтов, то подойдет следующий вариант. Помните, что вы не сможете изменить раздел контейнера после его создания. Если в нем закончится место, то вам нужно будет или удалить ненужные файлы, или создать контейнер большего размера и скопировать в него данные со старого контейнера.

- **Encrypt a non-system partition/drive** – шифрует несистемный раздел или диск. Программа позволяет зашифровать раздел жесткого диска или полностью все устройство, например, флешку. Подходит, когда нужно зашифровать все устройство (сменный носитель) или же когда данных много и приходится шифровать весь раздел.
- **Encrypt the system partition or entire system drive** – шифрует системный раздел или весь системный диск. При выборе этого пункта нужно быть осторожным. Ведь программа вносит изменения в процесс загрузки системы – ей нужно запросить пароль до запуска Windows. Если у вас установлено несколько операционных систем, учтите, что после выбора этого пункта некоторые из них перестанут запускаться. Неопытным пользователям не рекомендуется связываться с шифрованием системного диска, так как в случае малейшего сбоя все может закончиться переформатированием жесткого диска и потерей данных.

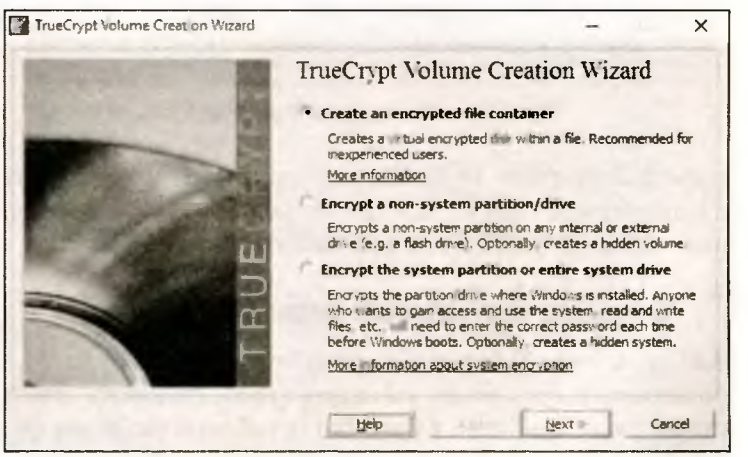


Рис. 11.4. Мастер создания зашифрованного тома

Самый удобный – первый вариант, поскольку вы можете перемещать файл виртуального зашифрованного диска в пределах всей файловой системы, как вам заблагорассудится. Можно, например, вообще скопировать его на внешний жесткий диск и спрятать в сейф.

Второй вариант менее удобен и его нужно использовать в следующих случаях:

- Когда шифруемых данных очень много и для обеспечения приемлемой производительности при работе с зашифрованным диском имеет смысл зашифровать целый раздел.
- Когда вам нужно зашифровать весь носитель, например, флешку.

Думаю, прочитав предыдущую главу, вы уже определились с оптимальным для вас способом защиты данных. Не нужно шифровать все данные подряд. Шифруйте только те, которые действительно представляют ценность для вас, и вы не хотите, чтобы кто-то их прочитал. Некоторые пользователи шифруют все подряд, в результате снижается производительность работы системы. Если разобраться, то конфиденциальных данных не так уж и много. Поэтому выбираем первый вариант. К тому же в этом случае не составит труда перенести криптоконтейнер (файл виртуального зашифрованного диска) на другой компьютер или смартфон. Шифрование раздела будет рассмотрено позже.

Далее программа предложит выбрать тип тома (рис. 11.5):

- **Standard TrueCrypt Volume** – обычный зашифрованный том. В системе он будет выглядеть как обычный диск.
- **Hidden TrueCrypt Volume** – скрытый том. Недостаток обычного тома заключается в том, что он будет виден всем, следовательно, кто-то попытается подобрать пароль к тому. Скрытый том не будет виден в списке дисков, и о его существовании будете знать только вы. Конечно, опытный пользователь сможет обнаружить, что в системе есть скрытый диск, но некоторые пользователи считают, что так надежнее.

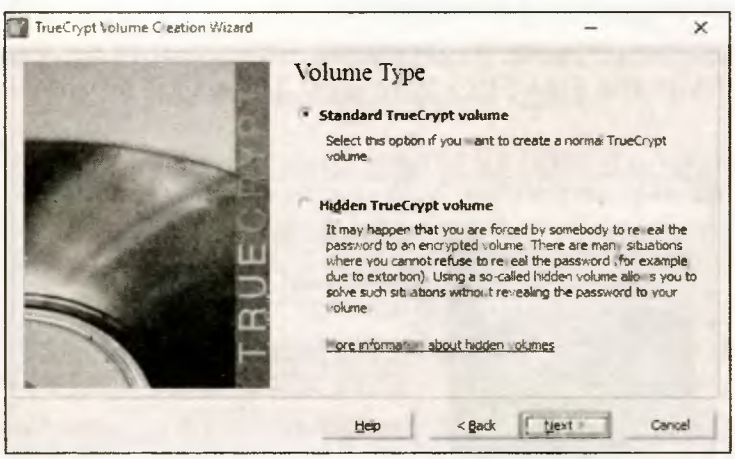


Рис. 11.5. Выбор типа тома

Пока выберите стандартный том – в большинстве случаев этого достаточно, а при надежном пароле «вскрыть» ваш том будет очень непросто.

Затем программа предложит вам выбрать местоположение для файла контейнера (рис. 11.6). Файл можно расположить в любом каталоге, к которому у вас есть доступ, а также на флешке или внешнем жестком диске. Нажмите кнопку **Select File** для выбора файла.



Рис. 11.6. Выбор местоположения для файла контейнера

Следующий шаг – выбор алгоритма шифрования и алгоритма хэширования (рис. 11.7). Можно выбрать алгоритмы AES, Serpent, Twofish или же их комбинации AES-Twofish или Seprent-Twofish-AES и т.д. При двойном или тройном шифровании помните, что у каждого алгоритма будет свой ключ и вам придется помнить не один, а три пароля. Возрастает надежность шифрования, но и вероятность забыть пароль.

Что же касается алгоритма хэширования, то возможны следующие варианты: RIPEMD-160, SHA-512 и Whirlpool. Длина хэша первого – 160 бит,



Рис. 11.7. Выбор алгоритмов шифрования и хэширования

двух последних – 512 битов. Самые надежные – последние два варианта. Какой из них выбрать? Оба алгоритма надежны. Если вы когда-нибудь имели дело с шифрованием, точнее, с хэшированием, то наверняка выберите привычный SHA-512, хотя Whirlpool (прямо как бренд моего холодильника) появился позже и должен быть надежнее SHA-512.

Следующий этап – ввод размера виртуального диска (рис. 11.8). Программа сообщит, сколько свободного места осталось на разделе, где хранится файл контейнера. Помните, что после создания изменить размер контейнера нельзя.



Рис. 11.8. Размер виртуального диска

Самый важный этап – ввод пароля (рис. 11.9). Регистр символов пароля должен быть разный, в пароле должны быть цифры и неалфавитные символы (@, ^, =, $, * и др.). Рекомендуемая разработчиком минимальная длина пароля – 20 символов, максимальная возможная длина – 64 символа.

Включив режим **Use Keyfiles**, у вас появится возможность задать ключевые файлы для доступа к тому. Указать ключевые файлы можно, нажав кнопку **Keyfiles**.

Следующий шаг – выбор файловой системы и форматирование тома (рис. 11.10). Для небольших виртуальных дисков нужно выбрать файловую систему FAT. А вот если размер диска составляет более 4 Гб и вы планируете хранить на нем большие файлы (размером тоже более 4 Гб, например, размер диска 50 Гб и размер файлов – от 4 Гб), тогда нужно выбрать файловую систему NTFS. Нажмите кнопку **Format** и подождите, пока форматирование будет завершено (рис. 11.11). Время ожидания зависит от выбранного размера диска.



Рис. 11.9. Установка пароля



Рис. 11.10. Форматирование виртуального тома, выбор файловой системы

Примечание. Что мне нравится в TrueCrypt, так это скорость ее работы. Она быстро создает виртуальные диски, она быстро шифрует разделы, а скорость обмена информацией с зашифрованными с помощью TrueCrypt дисками выше, чем с дисками, зашифрованными другими программами.

Наконец-то вы увидите сообщение, свидетельствующее об успешном создании виртуального диска (рис. 11.12).

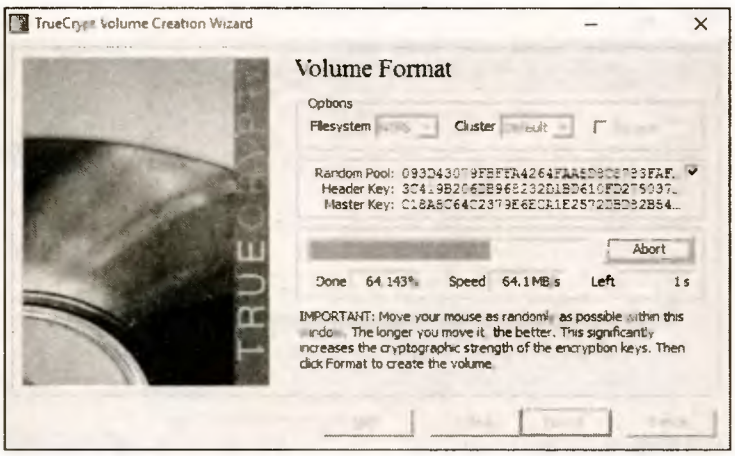


Рис. 11.11. Процесс форматирования виртуального диска



Рис. 11.12. Виртуальный диск успешно создан

Если вы желаете создать еще один контейнер, нажмите **Next**, в противном случае – нажмите **Exit**.

После создания виртуального жесткого диска его нужно смонтировать. В основном окне программы выберите букву устройства, которая будет использоваться для доступа к виртуальному диску, затем – файл виртуального диска (нажав кнопку **Select File**) и нажмите кнопку **Mount** (рис. 11.13).

Введите пароль, указанный при создании диска. Если при создании тома вы использовали ключевые файлы, тогда включите переключатель **Use keyfiles** и нажмите кнопку **Keyfiles** для выбора ключевых файлов (рис. 11.14).

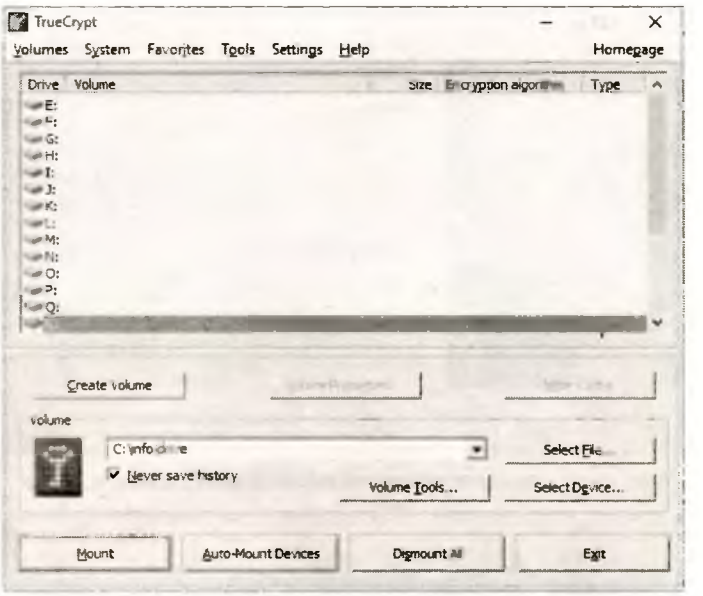


Рис. 11.13. Выбор файла виртуального диска

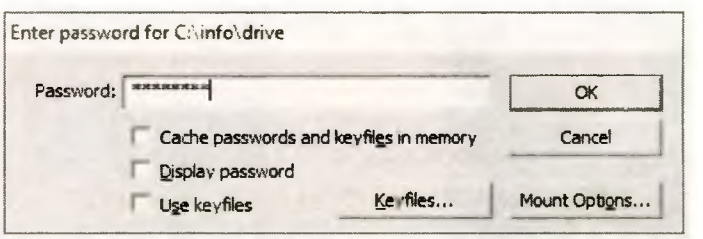


Рис. 11.14. Ввод пароля при монтировании тома

В основном окне программы вы увидите, что том смонтирован (конечно, при условии правильного ввода пароля). В нашем случае том смонтирован как диск R, размер тома – 199 Мб, алгоритм – AES (рис. 11.15).

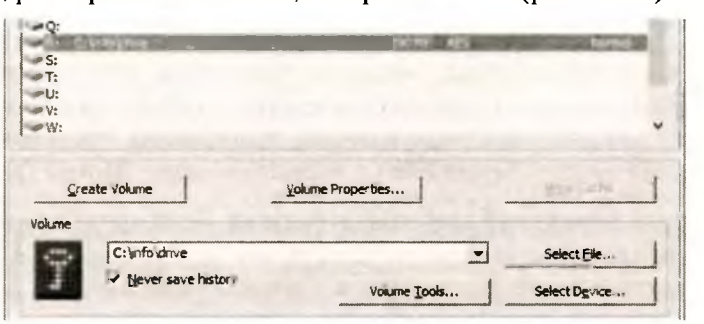


Рис. 11.15. Виртуальный диск смонтирован

После монтирования вы можете открыть окно Проводника и работать с зашифрованным диском как с самым обычным диском (рис. 11.16).

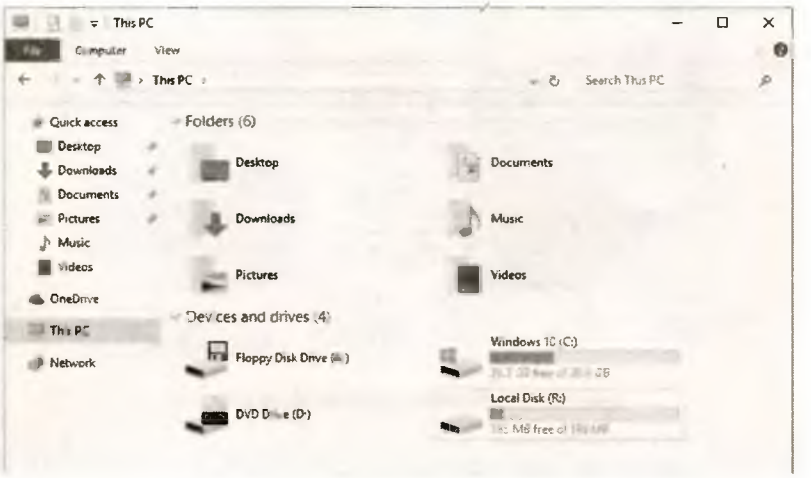


Рис. 11.16. Виртуальный диск в окне Проводника

Когда закончите работу с виртуальным диском, перейдите в окно программы TrueCrypt, выберите смонтированный диск и нажмите кнопку **Dismount**.

Шифрование всего раздела

Шифрование раздела аналогично созданию виртуального диска. Ничего сложного нет. Однако если вы не читали предыдущий раздел, самое время это сделать. Как обычно, нужно нажать кнопку **Create Volume**, только в появившемся окне нужно выбрать вариант **Encrypt a non-system partition/drive**.

После этого нужно выбрать, какой будет том – скрытый **(Hidden TrueCrypt volume)** или стандартный **(Standard TrueCrypt volume)**.

Далее необходимо выбрать том, который вы хотите зашифровать (рис. 11.17). Нажмите кнопку **Select Device**, чтобы выбрать раздел диска (рис. 11.18). Выберите раздел, нажмите кнопку **OK**, а затем – **Next**.

Программа TrueCrypt может создать зашифрованный том и отформатировать его **(Create encrypted volume and format it)** или же зашифровать раздел с сохранением имеющихся на нем данных **(Encrypt partition in place)**, см. рис. 11.19. Первый вариант предпочтительнее для пустых дисков или дисков, где нет важной информации. Второй вариант позволяет сохранить имеющиеся на диске данные.



Рис. 11.17. Нажмите кнопку Select Device

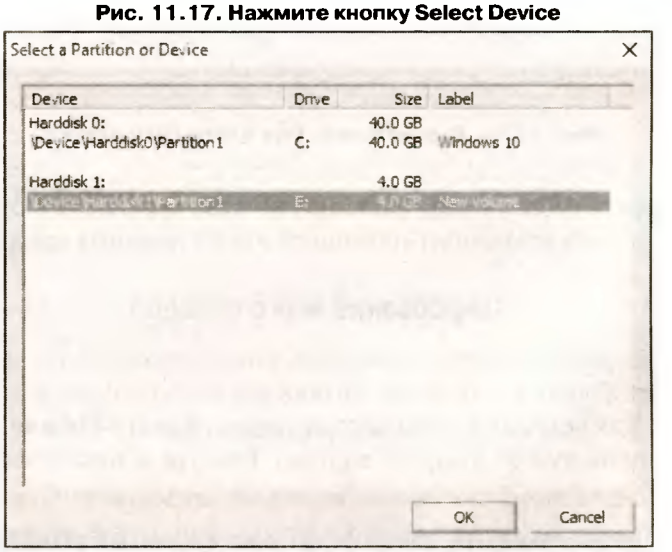


Рис. 11.18. Выберите диск (раздел) для шифрования

Внимание! Шифрование с сохранением данных занимает больше времени, но все же я рекомендую выбрать именно его, если на разделе есть данные. Если вы скопируете данные на другой раздел и выберите шифрование раздела с его форматированием (для ускорения процесса), а потом переместите данные из «резервного» раздела в зашифрованный, помните, что эти данные при удалении все еще останутся на диске и к ним может быть получен доступ с помощью специальных программ. Подробнее об этом мы поговорим в последнем разделе этой главы.

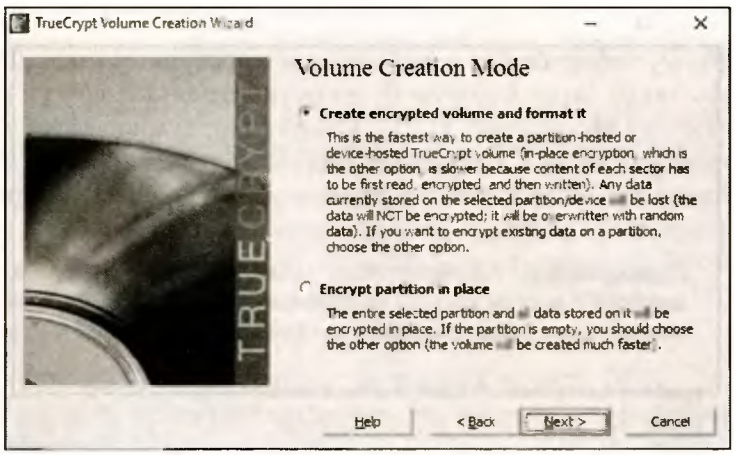


Рис. 11.19. Выбор типа шифрования

После этого процесс шифрования раздела ничем не отличается от создания виртуального диска: нужно выбрать алгоритм шифрования, ввести пароль и т.д. Важно помнить следующее: ваш диск после шифрования больше не будет доступен под прежней буквой. Например, вы зашифровали диск E. Больше вы не сможете обратиться к этому диску через букву E. При монтировании диска нужно будет выбрать другую букву и работать с данными через нее. Оригинальная буква (в моем случае – E) будет использоваться только в случае, если нужно будет удалить шифрование. Для этого нужно будет отформатировать диск, используя средства Windows (рис. 11.20).

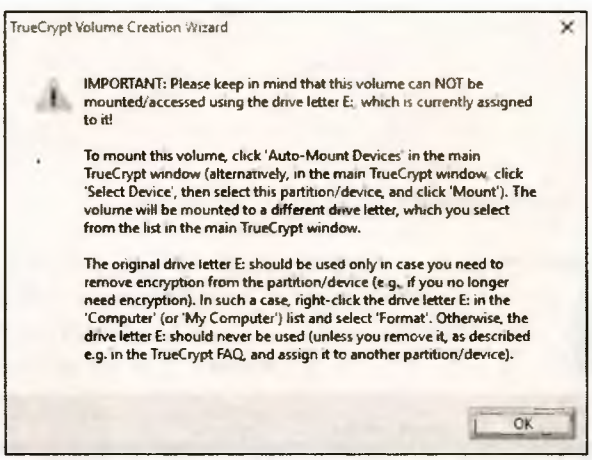


Рис. 11.20. Важное предупреждение

Как получить доступ к зашифрованному диску? В окне программы нужно нажать кнопку **Select device** и выбрать зашифрованный диск. Далее нужно выбрать букву, через которую будет осуществляться доступ к данным, и нажать кнопку **Mount** (рис. 11.21). Как обычно, нужно ввести указанный при шифровании пароль. Программа отобразит (рис. 11.22), к какой букве смонтирован диск, его физическое расположение, размер и алгоритм шифрования.

Примечание. Альтернативно можно нажать кнопку **Auto-Mount Devices** и ввести пароль, указанный при шифровании. Так зашифрованный диск будет смонтирован быстрее.

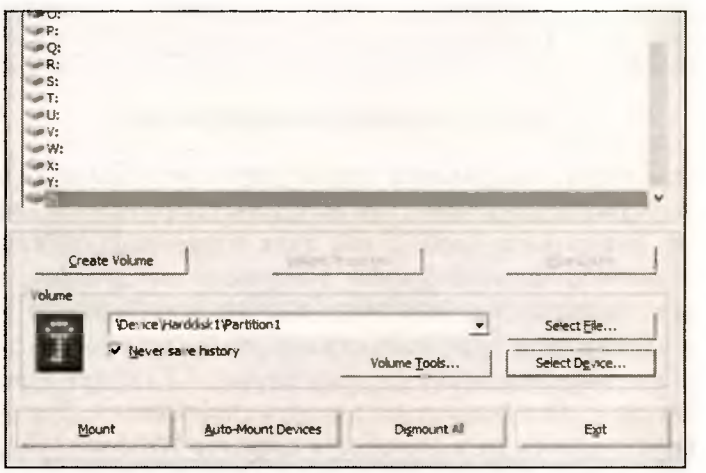


Рис. 11.21. Подготовка к монтированию диска



Рис. 11.22. Диск смонтирован

11.3. Программа VeraCrypt

VeraCrypt – это свободно распространяемое приложение, основанное на версии TrueCrypt 7.1a. Бесплатно скачать VeraCrypt можно с сайта **https://veracrypt.codeplex.com**.

Программа VeraCrypt может использовать следующие алгоритмы шифрования AES, Serpent, и Twofish. Дополнительно доступны 5 комбинаций этих алгоритмов: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES и Twofish-Serpent.

Внешне программа VeraCrypt является полным клоном TrueCrypt, поэтому подробно мы ее не будем рассматривать, так как она – точная копия своего оригинала (рис. 11.23).

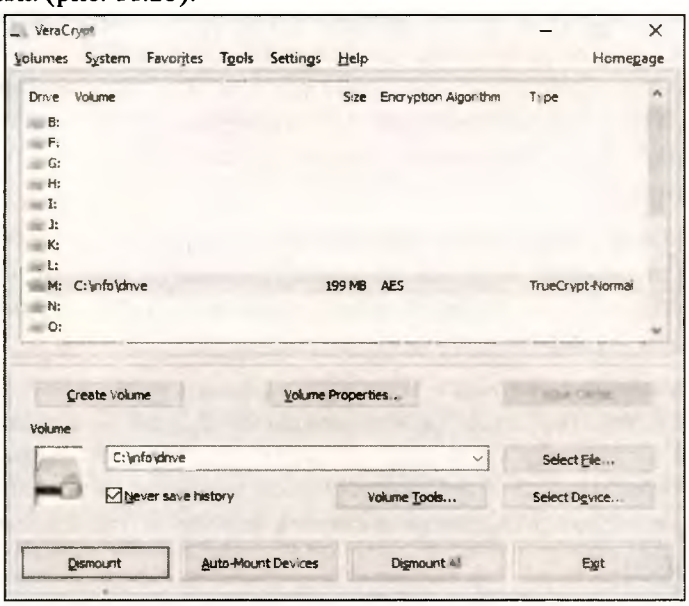


Рис. 11.23. Программа VeraCrypt

VeraCrypt совместима с TrueCrypt, но в окне монтирования нужно включать режим TrueCrypt (параметр **TrueCrypt Mode**), иначе подмонтировать диск не получится (рис. 11.24).

Что лучше – TrueCrypt или VeraCrypt? Разработчики VeraCrypt уверяют, что их продукт лучше, и приводят неоспоримые факты: TrueCrypt использует 1000 итераций при генерации ключа, которым шифруется системный раздел при использовании алгоритма PBKDF2-RIPEMD-160. VeraCrypt

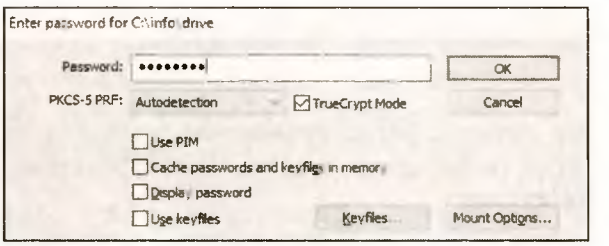


Рис. 11.24. Включаем режим TrueCrypt

использует 327 661 итераций. Для стандартных шифруемых разделов на диске и файловых контейнеров VeraCrypt использует 655 331 итераций для хэш-функции RIPEMD-160 и 500 000 итераций для SHA-2 и Whirlpool. Это существенно повышает устойчивость к атакам типа bruteforce (прямой перебор), но и существенно снижает производительность. Так написано в различных источниках, но вы будете приятно удивлены: производительность, конечно, снижается, но не существенно. Откуда я это знаю? Просто мне стало интересно, и я проверил производительность дисков, зашифрованных программами TrueCrypt и VeraCrypt. Для проверки использовал утилиту Crystal DiskMark. Если вам интересно, вы сможете произвести подобный тест самостоятельно.

Также в VeraCrypt исправлена уязвимость начального загрузчика для Windows, а для режима загрузки из зашифрованного раздела добавлена поддержка алгоритма SHA-256 и исправлены проблемы с уязвимостью ShellExecute для Windows.

Усовершенствования в формате VeraCrypt привели к несовместимости с форматом разделов TrueCrypt. Да, есть режим TrueCrypt, но «родной» формат VeraCrypt отличается от исходного формата TrueCrypt. Разработчики VeraCrypt считают формат TrueCrypt слишком уязвимым к потенциальной атаке АНБ (а не эта ли организация оказалась той самой третьей стороной?) и отказались от него.

11.4. Программа CipherShed

Программа CipherShed – еще один клон TrueCrypt. В отличие от VeraCrypt, CipherShed продолжает поддерживать старый формат (формат TrueCrypt). Программа также распространяется свободно и доступен ее исходный код. Скачать программу можно по адресу **https://www.ciphershed.org/**.

Если при установке CipherShed будет обнаружена TrueCrypt, то CipherShed предложит ее удалить. А вот VeraCrypt может спокойно жить на одном компьютере с TrueCrypt и CipherShed.

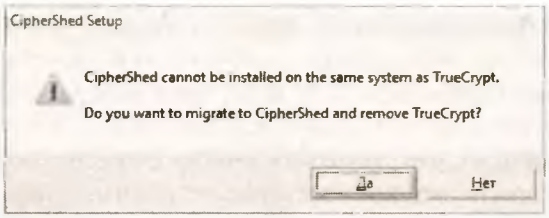


Рис. 11.25. Предложение удалить TrueCrypt

Думаю, не нужно говорить о том, что CipherShed выглядит так же, как и TrueCrypt.

Проект CipherShed появился в июне 2014 года – как раз после «смерти» TrueCrypt. Однако до сих пор проект считается экспериментальным, и версия 1.0 все еще не вышла. Как по мне, то целесообразно использовать или TrueCrypt, или VeraCrypt, в зависимости от формата, которому вы больше доверяете. Проверенный временем (TrueCrypt) или более современный и медленный (VeraCrypt). А CipherShed пусть окрепнет и наберется сил, тогда можно будет к нему вернуться, а пока он приведен в книге лишь для общего развития. А что касается производительности, то CipherShed оказался более медленным, чем даже VeraCrypt.

11.5. Программа CyberSafe и R-Studio

Программу CyberSafe мы ранее использовали для создания ключей, но это многофункциональная программа, позволяющая создавать виртуальные диски, шифровать целые разделы (кроме системного), организовывать прозрачное шифрование (гл. 12) и даже шифровать облако. Учитывая, что у вас уже огромный опыт создания контейнеров в TrueCrypt, с CyberSafe вы можете разобраться самостоятельно, тем более что ее интерфейс на русском языке, да и процедура создания контейнера гораздо проще, чем в TrueCrypt.

Программа довольно хороша, но сейчас мне бы хотелось рассмотреть один очень важный момент, а именно восстановление данных с виртуального диска, созданного этой программой. В результате системного сбоя в один не очень прекрасный момент я обнаружил, что виртуальный диск невозможно открыть. Данные инструкции по восстановлению информации подойдут и для обычных, а не только зашифрованных дисков.

Инструкция по восстановлению данных с зашифрованного раздела/виртуального диска CyberSafe Top Secret:

1. Смонтируйте зашифрованный диск или виртуальный диск в программе CyberSafe Top Secret. Будем считать, что у нас есть зашифрованный диск I, подмонтированный к X. В случае с виртуальным диском считаем, что он подмонтирован тоже к X. При попытке доступа к этому диску Windows сообщает, что прочитать данные невозможно (рис. 11.26). Данная инструкция позволяет восстановить данные с такого диска.

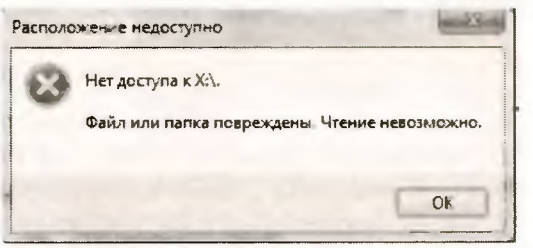


Рис. 11.26. Ошибка доступа к диску

2. Запустите инструмент R-Studio. Разрядность инструмента должна соответствовать разрядности операционной системы. На следующем рисунке мы видим наш диск X (рис. 11.27).

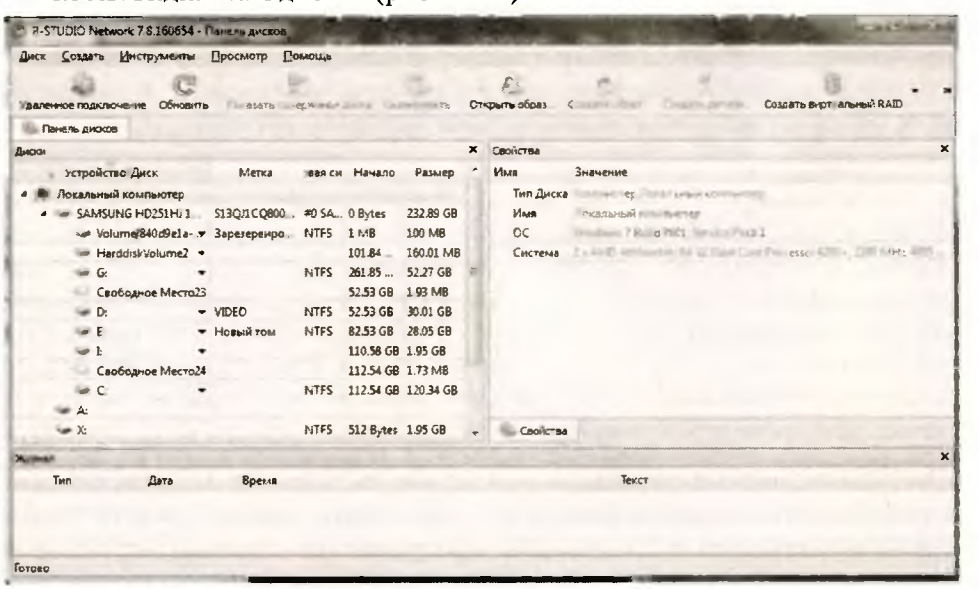


Рис. 11.27. Инструмент R-Studio

3. Щелкните по диску X правой кнопкой мыши и выберите команду **Показать содержимое диска** или просто нажмите F5.

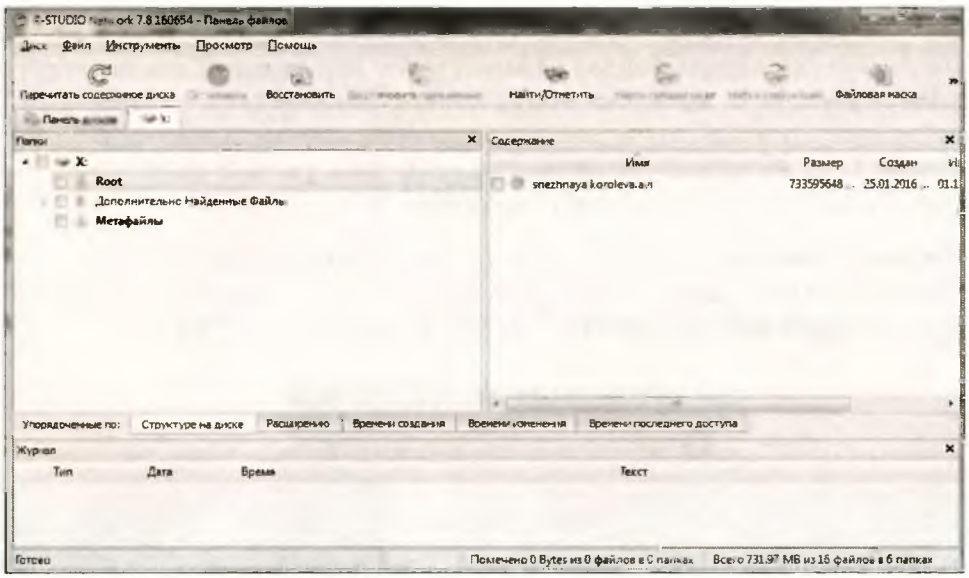


Рис. 11.28. Содержимое поврежденного диска

4. Приложение отобразит содержимое выбранного диска. На следующем рисунке видно, что на диске был всего один файл – фильм в формате AVI.

5. Выберите файлы, которые нужно восстановить, и нажмите кнопку **Восстановить** на панели инструментов.

6. В появившемся окне (рис. 11.29) выберите каталог, в который будут помещены восстановленные файлы.

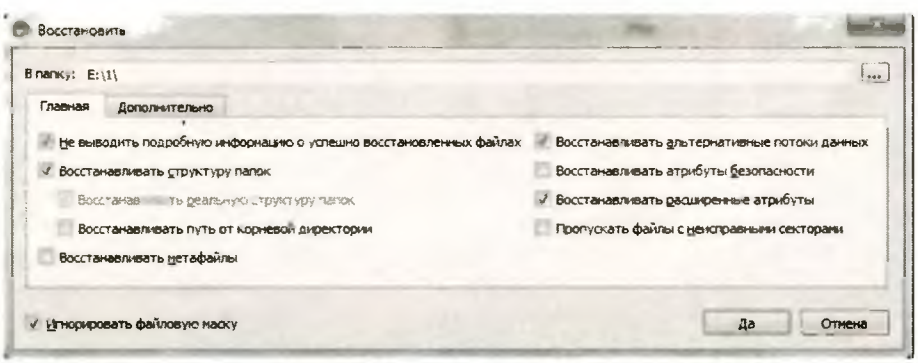


Рис. 11.29. Окно Восстановить

7. Дождитесь завершения процесса восстановления (рис. 11.30).

После восстановления файлов размонтируйте виртуальный или зашифрованный диск. Если вы использовали зашифрованный диск, то отформатируйте диск-носитель, проверьте его на наличие ошибок и зашифруйте его заново. Если вы использовали виртуальный диск, удалите файл виртуального диска с носителя и создайте его заново.

В главе 13 мы рассмотрим еще две полезных программы. Одна из них – многофункциональная FolderLock, вторая – Eraser, средство для безопасного удаления данных с диска.

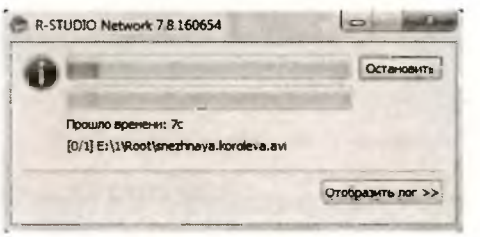
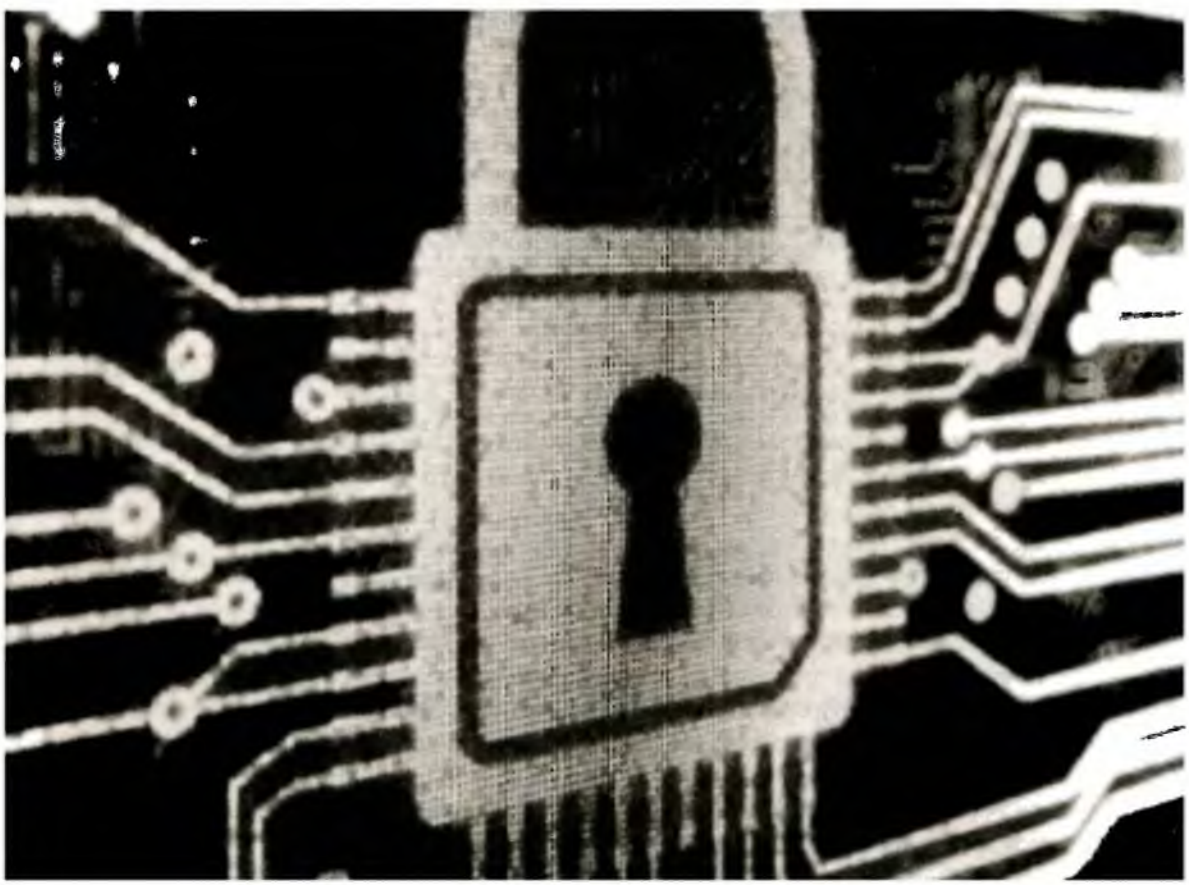


Рис. 11.30. Процесс восстановления

Глава 12.

Прозрачное шифрование по локальной сети



12.1. Сложности с сетевым шифрованием в локальной сети

Все мы знаем, как зашифровать данные, передающиеся по Интернету, – нужно использовать всякого рода VPN-сервисы. Если речь идет о защите корпоративных данных, передающихся между филиалами (часто такая передача осуществляется по Интернету: экономически не выгодно строить собственные линии передачи данных), тогда в корпоративной сети разворачивается собственный VPN-сервер.

Если нужно защитить личный трафик, то используются всевозможные VPN-сервисы с оплатой за трафик. Их услуги стоят совсем недорого. К тому же можно использовать проект TOR – он вообще бесплатный.

Об этом знают все, но что делать, если нужно зашифровать данные, передающиеся по локальной сети? Представьте, что вы зашифровали важные документы с помощью EFS или же храните их на виртуальном диске. Пока вы пользуетесь этими документами лично, проблем нет. Но проблемы возникнут, если нужно совместно работать над этими документами. Файловая система EFS не поддерживает шифрования данных, передающихся по сети. Аналогичная ситуация и с виртуальным диском: да, вы можете «расшарить» доступ к виртуальному диску, но ваши данные будут оставаться зашифрованными только на вашем компьютере. Как только они покинут его пределы, они будут передаваться по локальной сети в открытом виде. А это означает, что злоумышленник (которым может быть ваш коллега, который подключен к одной с вами локальной сети, но у которого нет доступа к зашифрованным данным) может легко их перехватить.

Что делать? Все решения шифрования трафика в основном нацелены на шифрование данных, выходящих за пределы локальной сети, то есть за-

щита осуществляется при передаче данных по Интернету. А локальная сеть считается изначально безопасной средой.

Да, есть аппаратные способы решения данной задачи – специальные сетевые адаптеры и коммутаторы с поддержкой шифрования. Но вы только подумайте: такой коммутатор нужно установить в каждой подсети, а такой сетевой адаптер – на каждый компьютер сети. Довольно затратно получается.

Я начал поиск более дешевого решения. И я его нашел. Это программа CyberSafe Top Secret. Собственно, поэтому я и познакомился с этой программой. Да, программа коммерческая. Правда, благодаря непонятной ценовой политике разработчика на сайте http://cybersafesoft.com/rus/ ее можно купить всего за 32 доллара (лицензия на 2 ПК), а не за 100 долларов (такая цена на http://cybersafesoft.com). Выходит, цена защиты одного компьютера – 16 долларов. Если количество пользователей, которые должны работать с секретными данными, больше, придется купить дополнительные лицензии. Я не думаю, что можно найти сетевой адаптер с поддержкой шифрования за эти деньги (не говоря уже о коммутаторе, который бы поддерживал такие адаптеры).

12.2. Как устроено прозрачное шифрование в CyberSafe

Разберемся, как реализовано прозрачное шифрование в программе CyberSafe. Для прозрачного шифрования используется драйвер Alfa Transparent File Encryptor[1], который шифрует файлы с помощью алгоритма AES-256.

В драйвер передается правило шифрования (маска файлов, разрешенные/запрещенные процессы и т.д.), а также ключ шифрования. Сам ключ шифрования хранится в ADS папки (Alternate Data Streams) и зашифрован с помощью OpenSSL (алгоритм RSA) – для этого используются сертификаты.

Логика следующая: добавляем папку, CyberSafe создает ключ для драйвера, шифрует его выбранными публичными сертификатами (они должны быть предварительно созданы или импортированы в CyberSafe). При попытке доступа какого-либо пользователя к папке CyberSafe открывает ADS папки и читает зашифрованный ключ. Если у этого пользователя есть приватный ключ сертификата (у него может быть один или несколько своих сертификатов), который применялся для шифрования ключа, он может открыть эту папку и прочитать файлы. Нужно отметить, что драйвер расшифровывает только то, что нужно, а не все файлы при предоставлении доступа к файлу.

[1] http://www.alfasp.com/products.html

Например, если пользователь открывает большой документ Word, то расшифровывается только та часть, которая сейчас загружается в редактор, по мере необходимости загружается остальная часть. Если файл небольшой, то он расшифровывается полностью, но остальные файлы остаются зашифрованными.

Если папка – сетевая расшаренная, то в ней файлы так и остаются зашифрованными, драйвер клиента расшифровывает только файл или часть файла в памяти, хотя это справедливо и для локальной папки. При редактировании файла драйвер шифрует изменения в памяти и записывает в файл. Другими словами, даже когда папка включена (далее будет показано, что это такое), данные на диске всегда остаются зашифрованными.

Принцип прост: на сервере (так будем условно называть компьютер, где хранится папка с зашифрованными документами) мы храним зашифрованную папку, доступ к этой папке – общий. На компьютере каждого пользователя, который должен получать доступ к секретным документам, устанавливается программа CyberSafe. Суть в том, что шифрование и расшифровка данных происходит на клиенте, а не на сервере. Поэтому по сети данные передаются в зашифрованном виде.

> **Важно!** У программы CyberSafe есть одна очень важная и непонятная мне особенность. На компьютере, на котором будут храниться зашифрованные документы, программа CyberSafe не должна быть установлена. Если ее установить, то на других компьютерах будут проблемы с доступом к зашифрованной папке. Зачем так сделано, мне не понятно. В крупных предприятиях, конечно, такое поведение очень удобно и оправдано. Как правило, общие документы хранятся на сервере (обычно под управлением Windows Server), и выделение отдельного компьютера не требуется – он уже и так выделен. Да и на сервер не нужно покупать отдельную лицензию, что, как говорится, мелочь, а приятно.

12.3. Настройка прозрачного шифрования

Поскольку с программой вы уже знакомы по предыдущим главам, опишу только общий процесс настройки:

1. Каждый пользователь должен сгенерировать и опубликовать свой ключ.
2. На сервере нужно создать пустую папку, а уже после шифрования скопировать в нее данные. Пусть это будет папка \\ACER\test\secret.
3. Нужно предоставить общий доступ к папке с секретными документами.

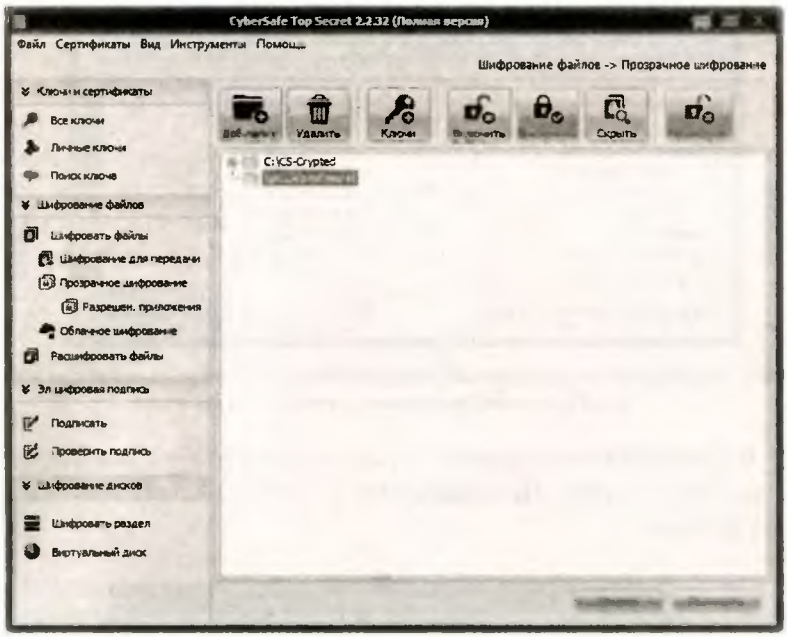


Рис. 12.1. Сетевая папка добавлена

4. На одном из компьютеров нужно импортировать сертификаты всех пользователей, которые должны получить доступ к секретным документам. Все готово к шифрованию папки.

5. Перейдите в раздел **Прозрачное шифрование**, нажмите кнопку **Доб. папку** и выберите папку, которую нужно зашифровать. Напомню, что вы должны выбрать сетевую папку \\ACER\test\secret (рис. 12.1).

6. Нажмите кнопку **Применить**. Появится запрос на добавление ключей шифрования для папки, нужно нажать кнопку **Да**. Если вы случайно ответили **Нет**, выделите папку в списке и нажмите кнопку **Ключи**.

7. Появится диалог выбора ключей пользователей (рис. 12.2). Выберите только тех, у кого должен быть доступ к папке (тех, кто сможет расшифровать файлы). Нажмите кнопку **OK**.

8. Появится запрос на добавления ключа администратора к папке (рис. 12.3). Администратор может управлять списком ключей пользователей. Если список пользователей, у которых есть доступ к папке, будет неизменным, ключ администратора можно не добавлять. Далее нужно будет выбрать администратора папки (рис. 12.4)

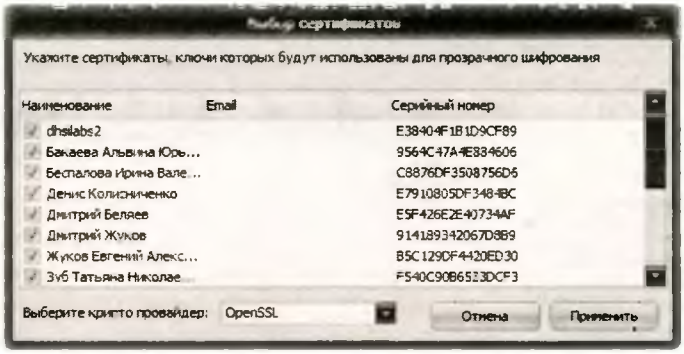


Рис. 12.2. Выберите сертификаты пользователей (e-mail пользователей стерты из соображений конфиденциальности данных)

9. Все, папка зашифрована. Чтобы начать работу с ней, выделите ее и нажмите кнопку **Включить**. После этого можно будет начать работу с папкой.

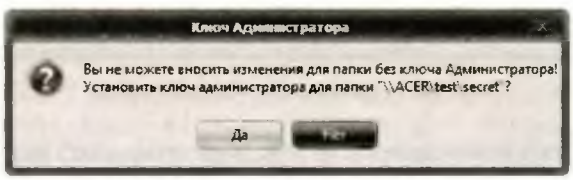


Рис. 12.3. Запрос

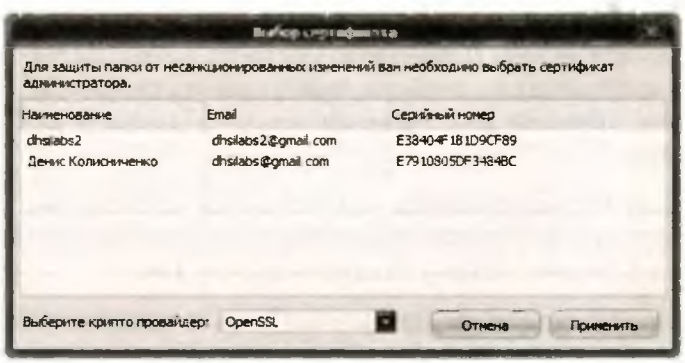


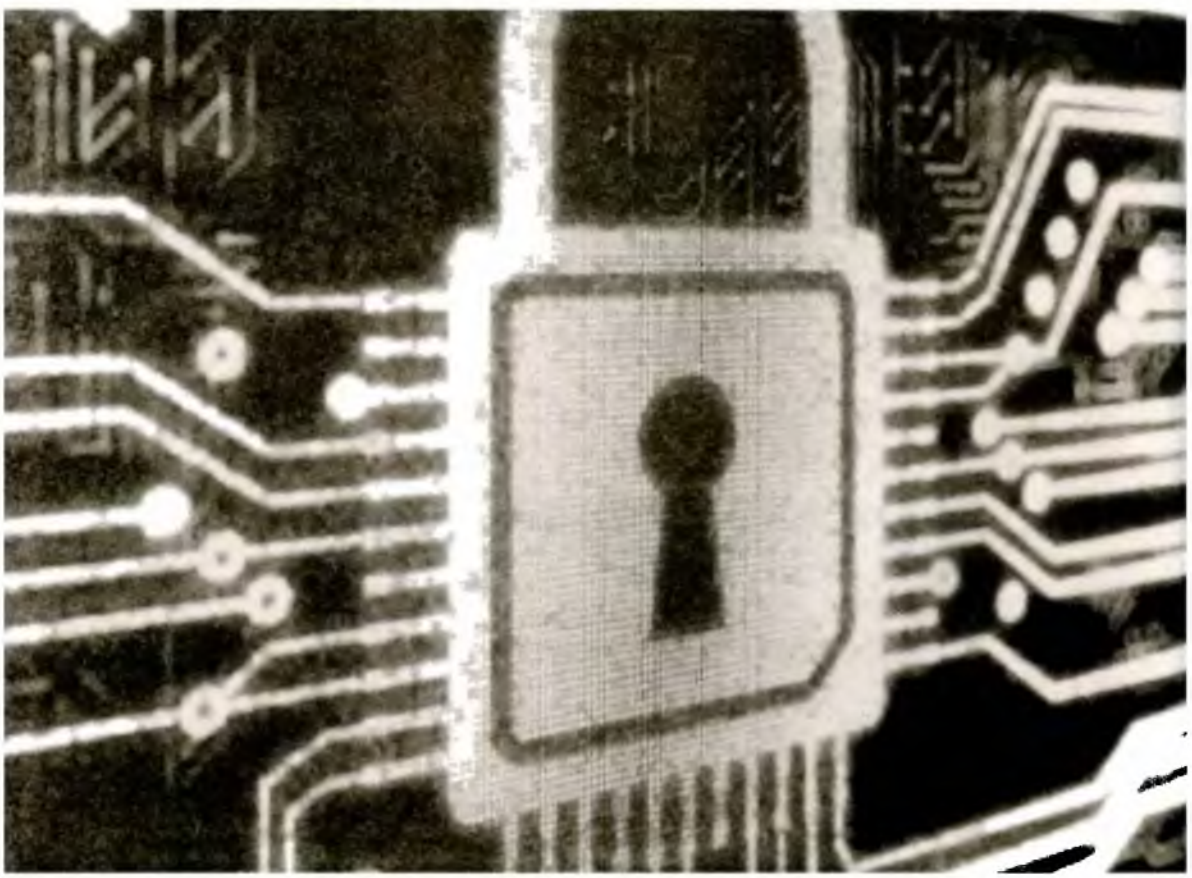
Рис. 12.4. Выбор администратора папки

Важно! Каждый раз, как вам понадобится зашифрованная папка, нужно включать ее через кнопку **Enable**. Если папка не включена и в нее добавить файлы, они будут не зашифрованы!

На этом все. Но хотелось бы еще раз обратить ваше внимание на сервер. В качестве сервера может выступать обычный компьютер под управлением Windows. Вот только не забывайте о количестве одновременно работающих с сетевой папкой пользователей. Это количество ограничивает сама Windows, и если пользователей много, вероятнее всего, придется купить Windows Server. И еще: на сервер, как уже отмечалось, не нужно устанавливать программу, иначе процесс шифрования не будет проходить корректно.

Глава 13.

Некоторые полезные программы



13.1. Программа Folder Lock

13.1.1. Возможности программы

Основные возможности программы Folder Lock следующие:

- AES-шифрование, длина ключа 256 бит.
- Сокрытие файлов и папок.
- Шифрование файлов (посредством создания виртуальных дисков – сейфов) «на лету».
- Резервное копирование онлайн.
- Создание защищенных USB/CD/DVD-дисков.
- Шифрование вложений электронной почты.
- Создание зашифрованных «бумажников», хранящих информацию о кредитных картах, счетах и т.д.

Как видите, возможностей у программы вполне достаточно, особенно для персонального использования.

13.1.2. Использование программы

Теперь посмотрим на программу в работе. При первом запуске программа просит установить мастер-пароль, который используется для аутентификации пользователя в программе (рис. 13.1). Представьте такую ситуацию:

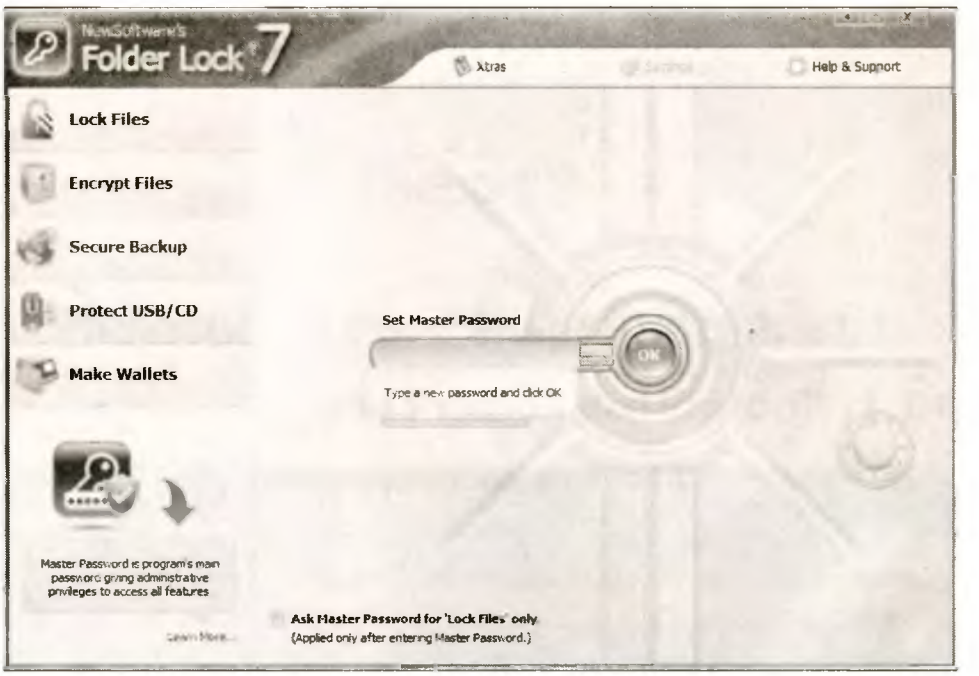


Рис. 13.1. Установка мастер-пароля при первом запуске

вы скрыли файлы, а кто-то другой запустил программу, просмотрел, какие файлы скрыты, и получил к ним доступ. Согласитесь, не очень хорошо. А вот если программа запрашивает пароль, то у этого «кого-то» уже ничего не выйдет – во всяком случае, до тех пор, пока он не подберет или не узнает ваш пароль.

Первым делом посмотрим, как программа скрывает файлы. Перейдите в раздел **Lock Files**, затем либо перетащите файлы (рис. 13.2) и папки в основную область программы, или же воспользуйтесь кнопкой **Add**. Как показано на рис. 13.3, программа позволяет скрыть файлы, папки и диски.

Посмотрим, что произойдет, когда мы нажмем кнопку **Lock**. Я попытался скрыть файл C:\Users\Denis\Desktop\cs.zip. Файл исчез из Проводника, Total Commander и остальных файловых менеджеров, даже если включено отображение скрытых файлов. Кнопка сокрытия файла называется **Lock**, а раздел – **Lock Files**. Однако лучше бы эти элементы UI было назвать **Hide** и **Hide Files** соответственно. Потому что на самом деле программа осуществляет не блокирование доступа к файлу, а просто «прячет» его. Посмотрите на рис. 13.4. Я, зная точное имя файла, скопировал его в файл cs2.zip. Файл спокойно скопировался, не было никаких ошибок доступа, файл не был зашифрован – он распаковался, как обычно.

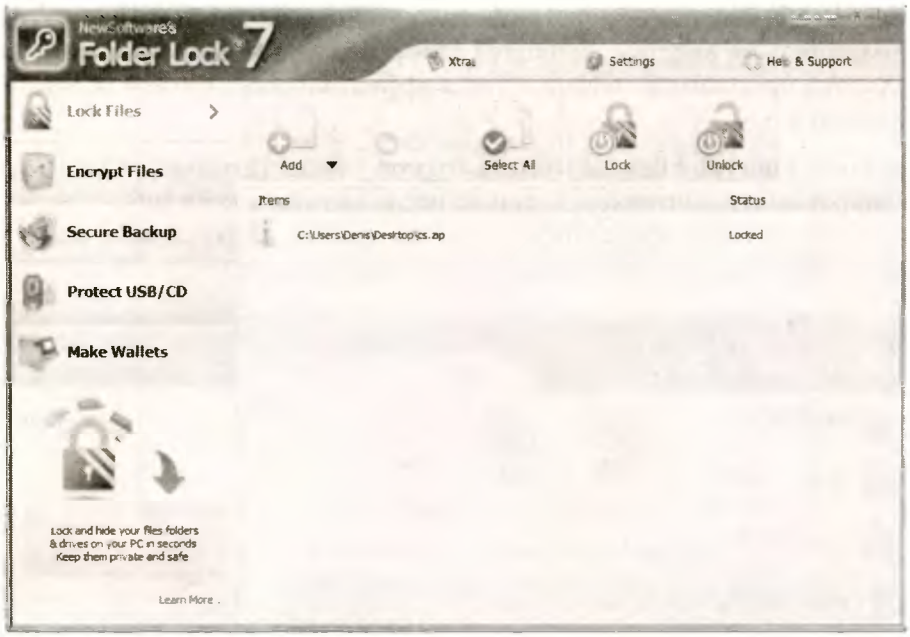


Рис. 13.2. Перетащите файл, выделите его и нажмите кнопку Lock

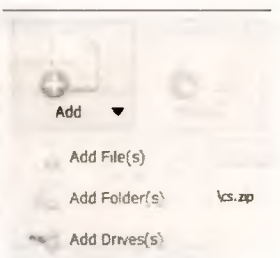


Рис. 13.3. Кнопка Add



Рис. 13.4. Копирование скрытого файла

Сама по себе функция сокрытия бестолковая и бесполезная. Однако если использовать ее вместе с функцией шифрования файлов – для сокрытия созданных программой сейфов, – тогда эффективность от ее использования увеличится.

В разделе **Encrypt Files** вы можете создать сейфы **(Lockers)**. Сейф – это зашифрованный контейнер, который после монтирования можно использовать как обычный диск: шифрование не простое, а прозрачное. Такая же техника используется многими другими программами шифрования.



Рис. 13.5. Раздел Encrypt Files

Нажмите кнопку **Create Locker**, в появившемся окне введите название и выберите расположение сейфа (рис. 13.6). Далее нужно ввести пароль для доступа к сейфу (рис. 13.7). Следующий шаг – выбор файловой системы и размера сейфа (рис. 13.8). Размер сейфа – динамический, но вы можете задать максимальный его предел. Это позволяет экономить дисковое пространство, если вы не используете сейф «под завязку».

После этого вы увидите окно UAC (если он включен), в котором нужно будет нажать **Yes,** далее будет отображено окно с информацией о созданном сейфе. В нем нужно нажать кнопку **Finish**, после чего будет открыто окно Проводника, отображающее подмонтированный контейнер (носитель).



Рис. 13.6. Название и расположение сейфа



Рис. 13.7. Пароль для доступа к сейфу

Вернитесь в раздел **Encrypt Files** и выделите созданный сейф (рис. 13.9). Кнопка **Open Locker** позволяет открыть закрытый сейф, **Close Locker** – закрыть открытый, кнопка **Edit Options** вызывает меню, в котором находятся команды удаления/копирования/ переименования/изменения пароля сейфа. Кнопка **Backup Online** позволяет выполнить резервное копирование сейфа, причем не куда-нибудь, а в облако (рис. 13.10). Но сначала вам предстоит создать учетную запись **Secure Backup Account**, после чего вы полу-

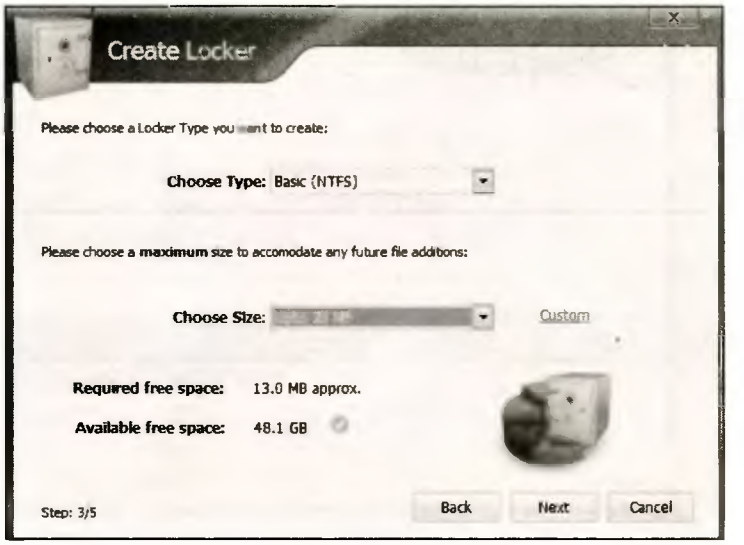


Рис. 13.8. Файловая система и размер сейфа

чите до 2 ТБ дискового пространства, а ваши сейфы будут автоматически синхронизироваться с онлайн-хранилищем, что особенно полезно, если вам нужно работать с одним и тем же сейфом на разных компьютерах.

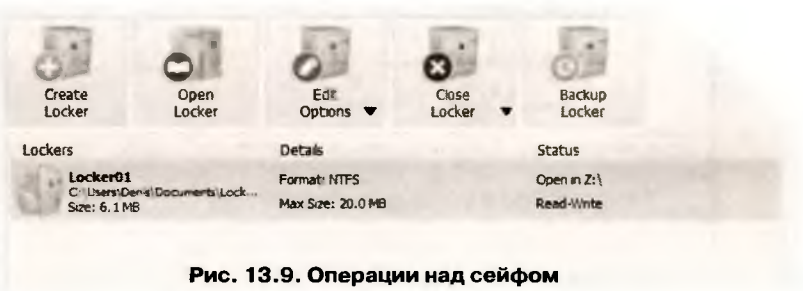


Рис. 13.9. Операции над сейфом

Ничто не бывает просто так. С расценками за хранение ваших сейфов можно ознакомиться по адресу https://secure.newsoftwares.net/signup?id=en. За 2 Тб придется выложить 400$ в месяц. 500 Гб обойдется в месяц 100$. Если честно, то это очень дорого. За 50–60$ можно арендовать целый VPS с 500 Гб «на борту», который вы сможете использовать как хранилище для ваших сейфов и даже создать на нем свой сайт.

Однако сама функция реализована довольно бредово. Допустим, вы создали сейф на 50 Гб. Сделали его резервную копию онлайн. Потом изменили в

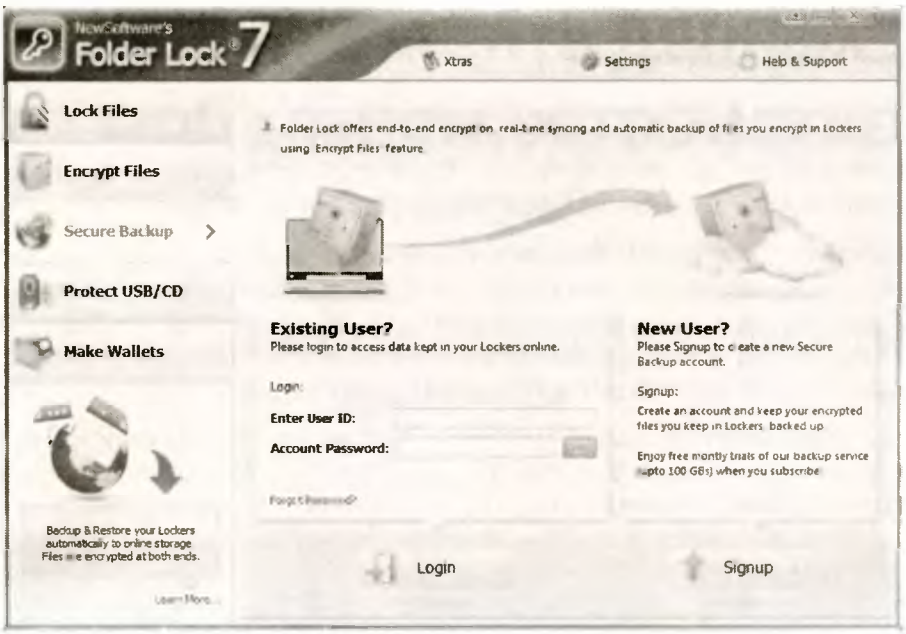


Рис. 13.10. Создание Secure Backup Account

нем один файл. И вам придется опять «заливать» в Сеть все 50 Гб. Согласитесь, не очень рационально.

13.2. Eraser: удаление информации без возможности восстановления

Когда вы удаляете файл, он на самом деле не удаляется с жесткого диска. Просто запись о файле удаляется из таблицы размещения файлов (не говоря уже о том, что есть копия этой таблицы, – по ней и производится восстановление удаленных фалов). Несмотря на то, что файл якобы удален, все данные, содержащиеся в нем, физически все еще находятся на жестком диске. Система перезапишет их только тогда, когда ей понадобится дисковое пространство, которое раньше занимал файл. Учитывая огромную емкость современных жестких дисков, может пройти несколько месяцев с момента удаления файла, а данные все еще будут на жестком диске, и их можно будет восстановить.

Вообще-то, как подмечено из моей практики, при удалении файлов работает закон Мерфи, он же закон подлости. Когда вы случайно удаляете важный файл, его зачастую нельзя восстановить или удается восстановить только частично, однако не все файлы можно прочитать при частичном восстанов-

лении. Видите ли, системе срочно понадобилось место, которое раньше занимал важный для вас файл.

Когда же вам нужно удалить компрометирующие вас файлы, физически они могут все еще находиться на жестком диске и свободно могут быть восстановлены, но вам этого не нужно. Вам нужно, чтобы они были удалены как можно быстрее и чтобы никто больше не смог их прочитать.

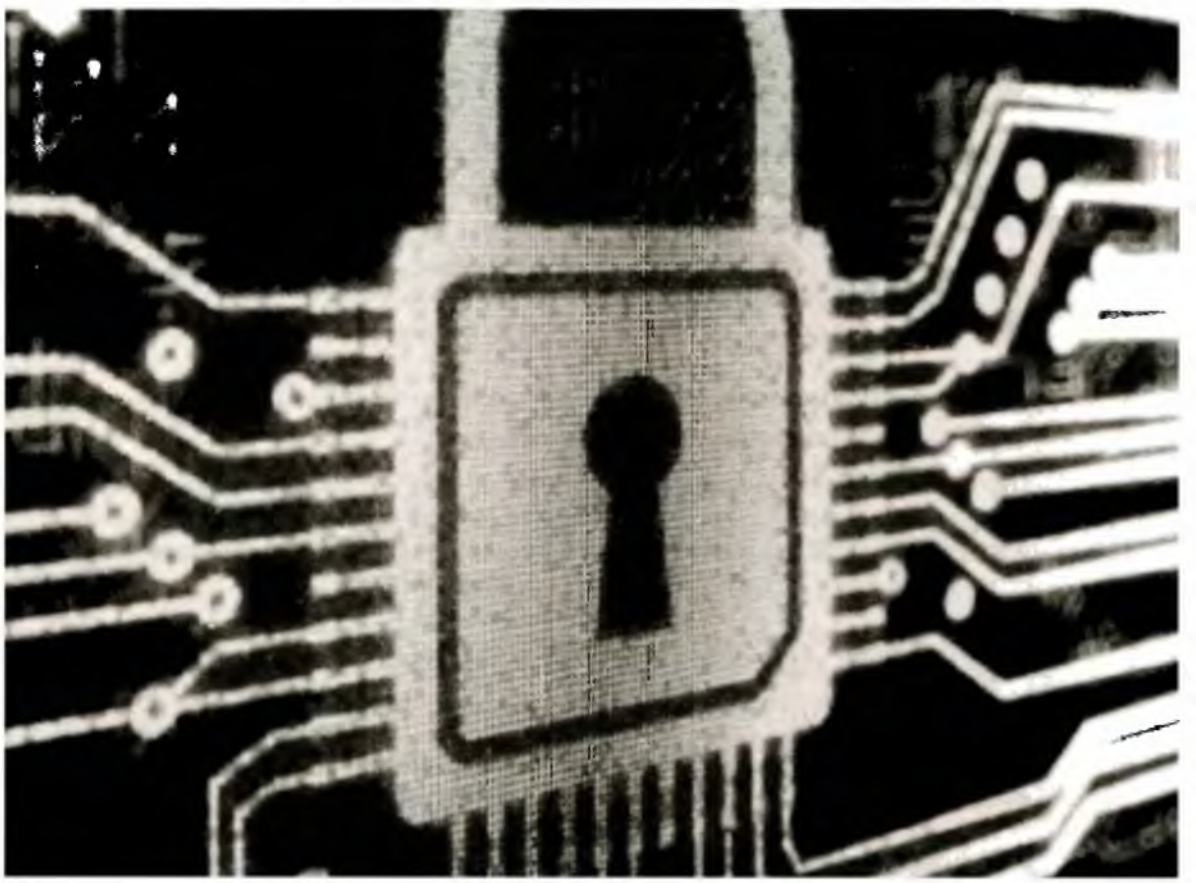
Существуют программы безопасного удаления файлов. Перед удалением файла такие программы вычисляют все блоки жесткого диска, занимаемые файлом. После удаления записи о файле из таблицы размещения все блоки данных файла перезаписываются случайной информацией или просто нулями, то есть происходит физическое удаление данных с жесткого диска.

Существует много программ подобного рода, но я остановил свой выбор на программе Eraser, скачать которую можно абсолютно бесплатно с сайта разработчика: **http://eraser.heidi.ie/.** Почему именно эта программа? Да потому что она, в отличие от некоторых других, нормально работает с Windows 10 и Windows Server 2012.

Разобраться с использованием программы очень просто – с этой программой вы справитесь и без моих комментариев. Единственное, что нужно отметить: программа требует .NET Framework, поэтому перед установкой программы нужно скачать и установить эту платформу. Благо она доступна бесплатно и ее можно скачать с сайта Microsoft.

Часть 4. Защита данных на мобильном устройстве Android

Глава 14. Защита электронной почты. MailDroid



14.1. Необходимые приложения

В главе 4 было показано, как защитить электронную почту на вашем компьютере. Теперь мы рассмотрим защиту электронной почты на смартфоне.

Стандартные почтовые клиенты, установленные по умолчанию, не поддерживают шифрование почты и электронную цифровую подпись (ЭЦП). Для работы с ЭЦП и для шифрования/расшифровки сообщений электронной почты необходимо установить следующие приложения (приложения бесплатные и устанавливаются из PlayMarket, права root для работы этих приложений не нужны):

- MailDroid – собственно, сам почтовый клиент. Ссылка на Play Market: https://play.google.com/store/apps/details?id=com.maildroid
- Crypto Plugin – плагин, поддерживающий работу с сертификатами. Ссылка: https://play.google.com/store/apps/details?id=com.flipdog.crypto.plugin

> **Примечание.** Нам не нужны Pro-версии программных продуктов, достаточно обычных (бесплатных).

Перед настройкой шифрования в Android нужно экспортировать ваши ключи и ключи всех, с кем вы планируете обмениваться корреспонденцией, и загрузить на SD-карточку (или во внутреннюю память) вашего устройства. Управление ключами было рассмотрено в главе 4.

14.2. Настройка Crypto Plugin

Первым делом нужно настроить плагин **Crypto Plugin**. Перейдите на вкладку **S/MIME** (рис. 14.1) и выберите команду **Import Certificate** (рис. 14.2).



Рис. 14.1. Вкладка S/MIME

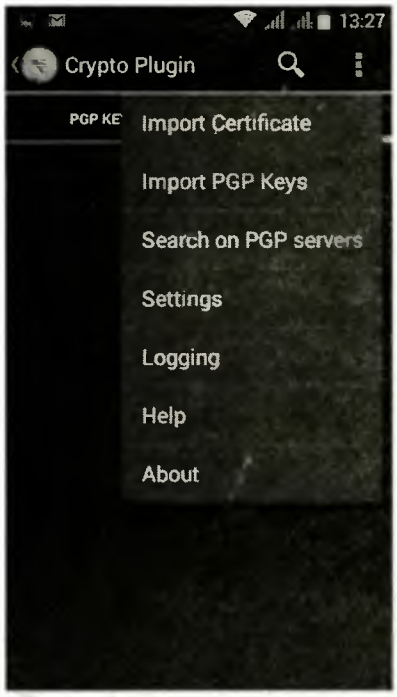


Рис. 14.2. Выберите команду Import Certificate

Первым делом нужно импортировать корневой сертификат. Его файл называется **Root Certificate** (рис. 14.3).

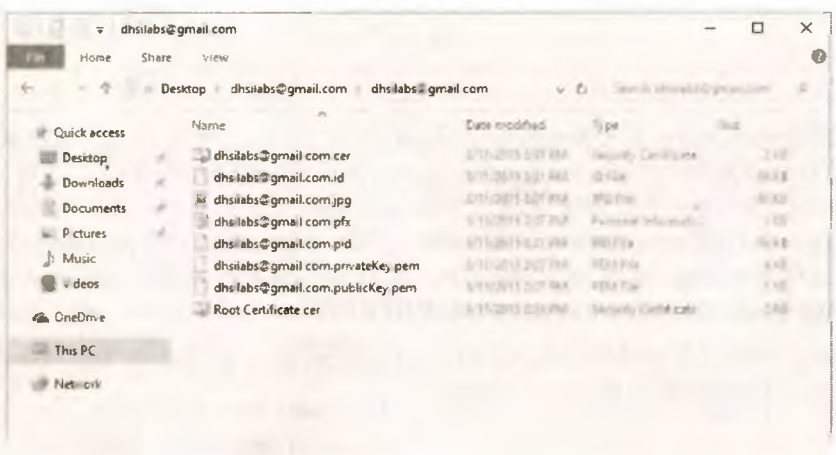


Рис. 14.3. Содержимое каталога с сертификатами

Выберите файловый менеджер, который вам удобно использовать, чтобы указать путь к сертификату. Далее нужно перейти к каталогу, в который вы поместили выбрать Root Certificate.cer (рис. 14.4). Программа спросит, как открыть файл. Нужно выбрать **«Standard»**.

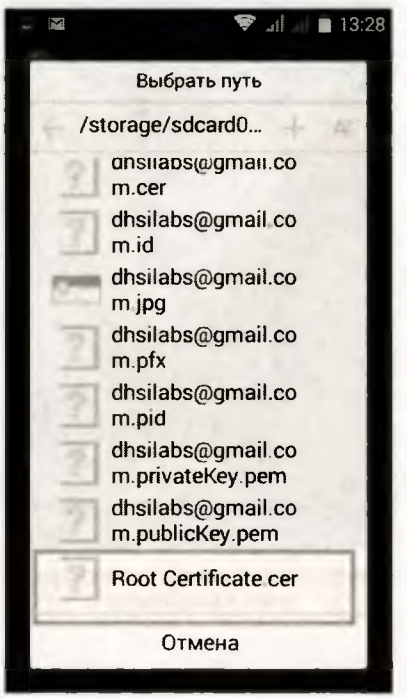


Рис. 14.4. Открытие сертификата



Рис. 14.5. Корневой сертификат импортирован

Импортированный сертификат появится в списке сертификатов (рис. 14.5). Далее операцию импорта нужно повторить для вашего личного сертификата (.pfx) и сертификатов всех, с кем вы планируете обмениваться зашифрованными сообщениями и ЭЦП (рис. 14.6). При импорте личного сертификата будет запрошен пароль (рис. 14.7). Обратите внимание: ваш личный сертификат помечен в списке как **PRIVATE**.

После импорта сертификатов можно приступить к обмену зашифрованными/подписанными сообщениями.

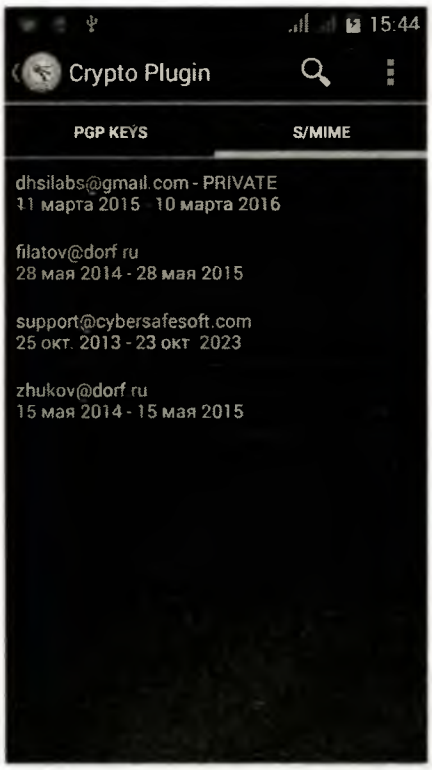


Рис. 14.6. Импортированы все сертификаты



Рис. 14.7. Пароль при импорте личного (приватного) сертификата

14.3. Настройка MailDroid

Перед тем как начать обмен зашифрованными сообщениями, необходимо проверить некоторые настройки. Откройте экран настроек. Перейдите в раздел **Encryption Plugin**. Убедитесь, что выбран режим шифрования **S/MIME** и включен переключатель **Allow MailDroid to decide** (рис. 14.8).

При создании нового сообщения в MailDroid вы можете подписать и зашифровать его. Для этого, если нужно только подписать, включите переключатель **Sign** (рис. 14.9). Если нужно не только подписать, но и зашифровать сообщение, тогда включите еще и переключатель **Encrypt**. При подписании сообщения нужно выбрать, какой сертификат будет использоваться. Выбор сертификата происходит в области **SIGNERS**. Скорее всего, у вас будет всего один сертификат (см. рис. 14.9).

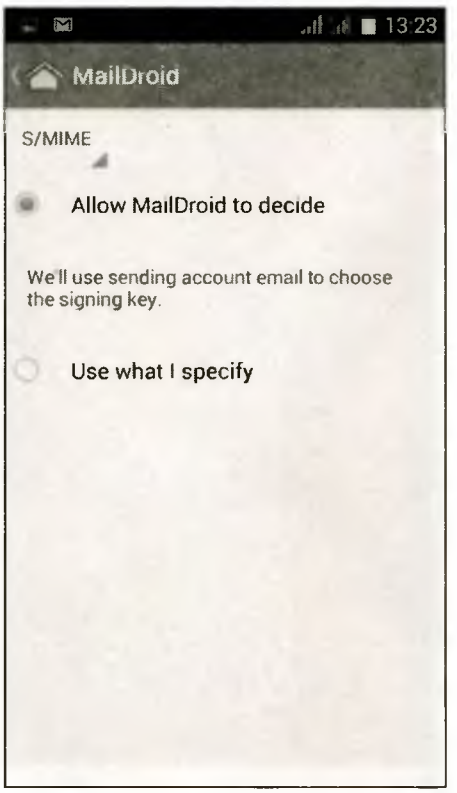


Рис. 14.8. Режим шифрования



Рис. 14.9. Электронная подпись письма и выбор сертификата

При шифровании письма сертификаты всех получателей программа добавляет автоматически (если, конечно, вы их импортировали с помощью **Crypto Plugin**). Я выбрал двух получателей. Программа автоматически добавила их сертификаты в список (рис. 14.10). Также программа выполняет проверку сертификатов получателей: обратите внимание на результат проверки сертификата – **CERTIFICATE IS OK**.

Теперь рассмотрим работу с зашифрованными и подписанными сообщениями. Когда вам придет зашифрованное сообщение, оно будет отмечено значком замка. Откройте зашифрованное сообщение. Программа сообщит, что оно зашифровано **(Encrypted)**. Нажмите ссылку **Click** для расшифровки сообщения (рис. 14.11). Введите пароль вашего сертификата (рис. 14.12).

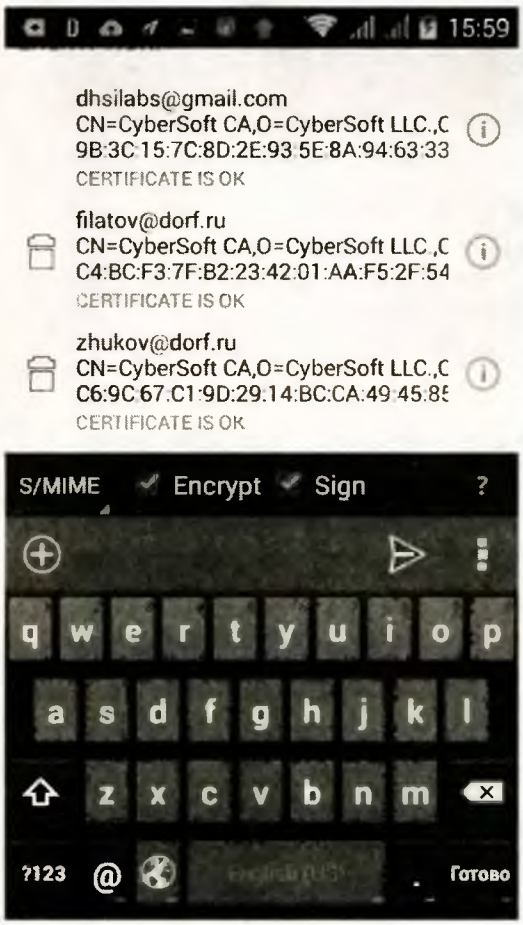


Рис. 14.10. Сертификаты получателей

Если пароль введен правильно, сообщение будет расшифровано.

14.4. После установки MailDroid

После установки и настройки MailDroid нужно отключить стандартный почтовый клиент Gmail, чтобы не получать уведомления о новой почте из двух программ. Для этого выполните следующие действия:

- Откройте окно настроек Android **(Настройки)**.
- Выберите **Приложения**.

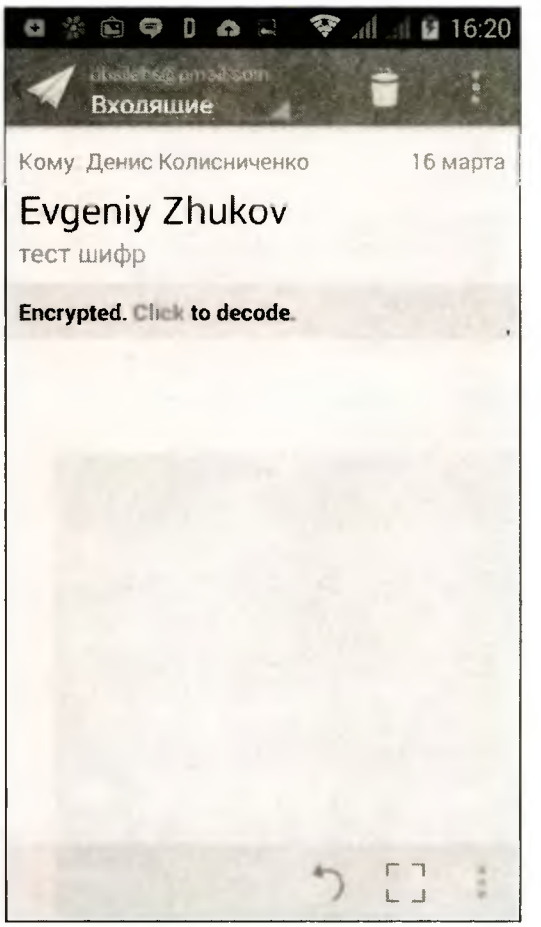


Рис. 14.11. Нажмите Click для расшифровки

- Перейдите на вкладку **Все**.
- Выберите Gmail.
- Нажмите кнопку **Остановить**.
- Нажмите кнопку **Отключить**.

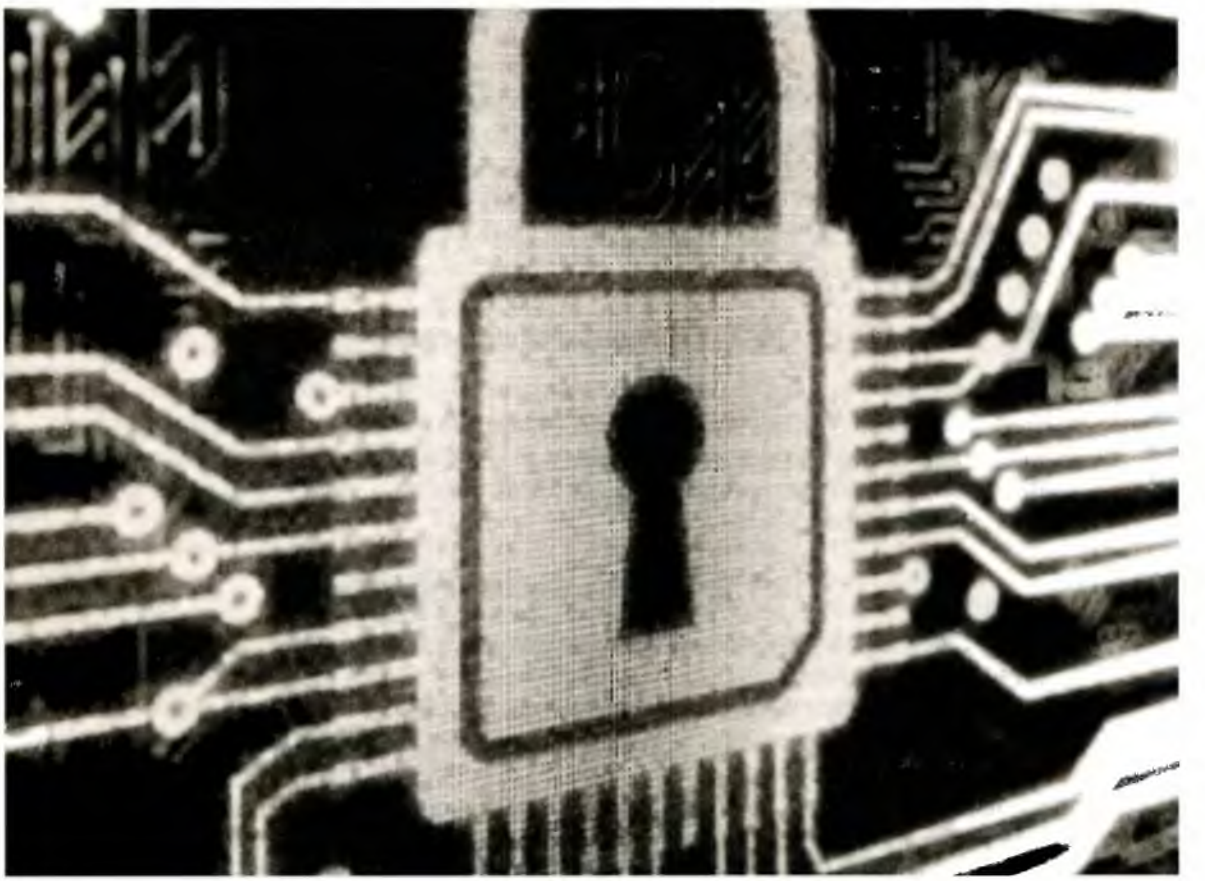


Рис. 14.12. Введите пароль сертификата



Глава 15.

Защита важных документов с помощью криптоконтейнера



15.1. Зачем нужно защищать данные на Android-устройстве

Современный мобильный телефон уже давно является небольшим персональным компьютером, и самое главное в нем – даже не возможность запуска различных приложений, а то, что на нем хранятся персональные данные пользователя. Фотографии, различные документы, номера кредитных карточек и другая платежная информация. О том, как защитить эти данные, мы и поговорим в этой главе.

15.1.1. Способы защиты данных

Как мы будем защищать их? Есть несколько возможных подходов, например, запрет запуска определенных приложений, сокрытие файлов и папок с данными, а также шифрование, причем можно зашифровать как отдельные файлы, так и все устройство. Вы же можете использовать любой из этих способов или даже все вместе.

15.1.2. От кого защищаем данные?

Также нужно разобраться, от кого или от чего мы будем защищать наши данные. Все угрозы можно разделить на две большие группы: внешние и внутренние. К внешним угрозам относятся различные недоброжелательные сайты и вредоносные программы, которые могут передать третьей стороне ваши персональные данные, изменить или уничтожить их. С внешними угрозами как-никак, но справляются антивирусы, которые вы можете установить самостоятельно. Также к внешним угрозам можно отнести возможность перехвата данных по сети, особенно когда вы подключаетесь через публичную Wi-Fi сеть (аэропорта, отеля, библиотеки, кафе и т.д.), которую вы не контролируете. Ваши пароли и финансовая информация (хотя она

часто шифруется, но все же) могут «уплыть» третьей стороне. Учитывая, что мобильные телефоны передают данные через сеть оператора, то перехват таких данных на отрезке телефон-оператор маловероятен (разве что их может перехватить сам оператор), а большинство случаев краж передаваемой информации происходит на отрезке телефон-WiFi. Помочь в этой ситуации может организация VPN и туннелирования. Кстати, перехват трафика оператором тогда вам тоже не страшен. О том, как это реализовать, мы поговорим в главе 18.

А в этой главе мы поговорим исключительно о внутренних угрозах. Например, представим, что ваш телефон попал в руки злоумышленнику. Как именно он попал в руки третьего лица - не важно. Вы могли забыть его в офисе, а ваши коллеги шутки ради или из других побуждений могли просмотреть ваши фотографии или прочитать документы. Вы могли потерять телефон, у вас могли его украсть и т.д.

Представим, что некто держит в руках ваш телефон. Первое, что становится на защите ваших данных, – это графический пароль. Если он у вас отключен, самое время его включить. Дополнительная защита никогда не помешает. Если пароль отключен, злоумышленнику достаточно провести пальцем по экрану в указанном направлении, и блокировка будет снята.

Однако графический пароль не панацея. Если у злоумышленника есть чуть больше времени или определенные навыки, такой пароль можно легко обойти. Да и никто не мешает извлечь карту памяти из телефона и прочитать ее на компьютере или своем телефоне. Чтобы извлечь карту памяти, никакой пароль не нужен.

А вот если данные на карте памяти будут зашифрованы, прочитать уже ничего не получится. Шифрование – самый надежный способ защиты ваших личных данных.

Если же шифрование вам не нужно, вам могут пригодиться и другие способы защиты, например, запрет запуска определенных приложений и сокрытие папок из галереи. Элементарно: на вашем планшете может быть установлено приложение ES Проводник или любой другой файловый менеджер. Ваш ребенок взял планшет, чтобы поиграть в какую-то игрушку, и случайно запустил файловый менеджер. Что он может наделать дальше – предсказать сложно. Играючи можно удалить все важные файлы без всякого злого умысла. Вторая ситуация – ваш не очень честный коллега попросил телефон просто позвонить. На время звонка он отошел, чтобы никто не слышал, о чем он говорит. Как скрыть папки и файлы (например, некоторые документы, фотографии), которые не должны видеть посторонние в таких ситуациях? Ведь никто ему не помешает взять и просмотреть те же фото-

графии. Даже если в них нет ничего конфиденциального, согласитесь, неприятно, когда кто-то без вашего ведома их просматривает.

15.1.3. Блокировка запуска приложения и запрет просмотра галереи

Самая надежная защита ваших личных данных – это шифрование. Однако если вам нужно только ограничить запуск определенных приложений или просто скрыть некоторые папки из галереи, вам подойдут приложения App Lock и Gallery Excluder. Первое приложение позволяет защитить паролем запуск определенных приложений (помните, что Messenger, то есть приложение, работающее с вашими SMS, – это тоже приложение), а второе – исключить из галереи папки, которые не должны просматривать посторонние люди.

Такая защита не очень надежная. При желании ее можно обойти, особенно защиту Gallery Excluder. Но если вам нужно просто запретить вашему ребенку просматривать некоторые фотографии или же запускать определенные приложения, можно воспользоваться и такой защитой.

Использовать оба приложения очень просто. В первом случае в список нужно добавить приложения, при попытке запуска которых нужно будет вводить пароль. Если пароль правильный, приложение запустится. Во втором случае в список исключений нужно добавить папки, которые не будут видны в приложении Gallery.

Но вся проблема в том, что иногда при запуске приложения, защищенного AppLock, оно успевает открыться до того, как App Lock заблокирует его запуск. Другими словами, некто может успеть прочитать ваши SMS или почту (хотя бы частично) до того, как появится окно ввода пароля. Об этой особенности приложения вы должны знать. Я с ней столкнулся лично, поэтому я не рекомендую App Lock для защиты серьезных секретных данных. К тому же никто не мешает извлечь карту памяти и прочитать эти данные напрямую без запуска приложения.

Вторая программа скрывает папки из списка в приложении Gallery. Проблема в том, что эти папки без проблем просматриваются другими файловыми менеджерами, тем же ES Проводник. То есть защиты данных не осуществляется как таковой. Я уже молчу про извлечение SD-карты. Если все-таки вы хотите воспользоваться Gallery Excluder, можете скачать APK-файл этого приложения по адресу:

http://4pda.ru/forum/index.php?showtopic=236864&st=20

На Google Play этого приложения нет.

В предыдущей главе было показано, как защитить вашу электронную почту. В этой главе мы поговорим о защите других ваших данных, например, документов, с которыми вы работаете.

Иногда нужно защитить данные определенного приложения. Не все приложения сохраняют обрабатываемые данные в виде отдельных файлов. Некоторые приложения хранят обрабатываемые данные в каталоге приложения. В этом случае вам понадобятся права root. Вы можете смонтировать криптоконтейнер к папке приложения. Тогда все попадающие в него данные будут автоматически зашифровываться. Аналогично можно зашифровать папку /DCIM, и тогда все создаваемые фотографии будут автоматически зашифровываться.

15.2. Шифрование всего устройства

Начиная с Android 4.2, вы можете зашифровать все устройство средствами самой операционной системы Android. При этом вам не нужно покупать или устанавливать какие-либо дополнительные приложения. Все осуществляется средствами самой операционной системы, причем доступ к Интернету для этого не нужен. Вы можете зашифровать данные в любой момент, когда посчитаете это целесообразным.

Работает шифрование так: после включения шифрования все данные на устройстве и на карте памяти будут зашифрованы. Конечно, если кто-то разблокирует ваше устройство, он все равно получит доступ к данным, однако это спасет ваши данные, если кто-то попытается украсть карту памяти или прочитать данные без включения смартфона с его внутренней памяти. У него ничего не выйдет, так как данные будут зашифрованы.

При включении смартфона вам нужно будет вводить пароль, позволяющий расшифровать данные. Без ввода пароля смартфон дальше не загрузится. Это не просто пин-код, это ключ, которым зашифрованы ваши данные.

О шифровании устройства вы должны знать следующие вещи:

- Шифрование возможно только в одном направлении. После шифрования расшифровать устройство уже будет нельзя. Можно только сбросить его до заводских настроек, но в этом случае вы потеряете все данные.
- Шифрование всего устройства замедляет работу смартфона. В принципе, в эру 8-ядерных процессоров и при объеме оперативной памяти от 1 Гб это не доставит вам хлопот. На более слабых устройствах «торможение» будет ощутимым.

- Шифрование устройства не спасет ваши данные от случая, если кто-то попросил ваш смартфон, чтобы просмотреть, а сам в этот момент или установит троян, или просто вручную отправит некоторые интересующие его данные на свой телефон. От таких случаев позволяет защититься только криптоконтейнер: ведь для доступа к данным внутри контейнера нужно будет ввести еще один пароль, который злоумышленник не знает.

Если вы хотите зашифровать все устройство, перейдите в **Настройки, Безопасность**, затем нажмите кнопку **Зашифровать телефон** (или **Зашифровать планшет**) в разделе **Шифрование**. Далее следуйте инструкциям.

> **Примечание.** Шифрование невозможно осуществить, пока вы не настроите PIN-код. Для этого перейдите в **Настройки, Шифрование**, выберите **Блокировка экрана**, нажмите **PIN-код** или **Пароль**.

15.3. Выбор Android-приложения для работы с криптоконтейнерами

Что такое криптоконтейнеры, вы уже знаете. В этой главе мы рассмотрим два приложения для работы с криптоконтейнерами в Android. На данный момент в Google Play доступны следующие программы для шифрования:

- LUKS Manager;
- EDS Lite;
- Cryptonite;
- CyberSafe Mobile.

Первая программа – **LUKS Manager**. Является старейшей программой шифрования файлов в Android. Программа использует алгоритм шифрования AES, а само шифрование происходит «на лету». При этом поддерживаются файловые системы EXT2/4 и FAT32. Размер зашифрованного контейнера не ограничивается (разве что только размером памяти телефона).

К преимуществам программы можно отнести шифрование «на лету» и простоту использования (работа с зашифрованными контейнерами осуществляется как с обычными папками).

К недостаткам можно отнести тот факт, что программа требует прав root для своей работы. Также программа не поддерживает контейнеры TrueCrypt, которые стали сейчас практически стандартом де-факто. Очень удобно было бы создать на компьютере зашифрованный контейнер, поместить его

на флешку, а затем при необходимости – на мобильный телефон, где можно было бы работать с ним как с обычной папкой.

Вторая программа, **EDS Lite**, хоть и молодая, но очень перспективная. Во-первых, для ее работы не нужны права root, что очень важно для многих пользователей. Во-вторых, программа поддерживает контейнеры TrueCrypt, а как мы знаем, программа TrueCrypt сейчас работает на всех основных настольных платформах.

Но программа не идеальна. Шифрование осуществляется не «на лету» и с зашифрованным контейнером нельзя работать как с обычной папкой. Однако есть встроенный файловый менеджер, который поддерживает все операции над файлами. Например, вы можете создать зашифрованный контейнер в EDS Lite или в TrueCrypt, открыть его во встроенном файловом менеджере программы и скопировать в него все файлы, которые нужно зашифровать. Не очень удобно (нельзя использовать сторонние файловые менеджеры вроде ES Проводник), но работать можно. Плохо, что остальные программы не поддерживают эти контейнеры. Например, вы создаете документ в текстовом редакторе, и чтобы он был зашифрован, вам нужно явно поместить его в контейнер. Аналогично, чтобы прочитать его, его нужно явно скопировать на карту памяти. Шифрования/дешифрования «на лету» очень не хватает этой программе. Зато поддерживаются два алгоритма шифрования – AES 256 и SHA-512.

Программа **Cryptonite** довольно молода и находится на стадии тестирования. Использовать ее на практике я бы пока не стал, зато она будет поддерживать облачные диски, что очень немаловажно сейчас, когда пошла мода на облачные технологии. Существенный недостаток этой программы – то, что она требует от ядра Android поддержки Kernel FUSE, а такая поддержка есть не в каждом телефоне.

Приложение CyberSafe Mobile существенно превосходит по функционалу EDS Lite, но обо всем по порядку. Конек приложения – это даже не сами криптоконтейнеры, а возможность их синхронизации с Google Drive, что позволяет работать с одним и тем же набором данных на разных устройствах. Подробно о шифровании облака этим приложением мы поговорим в главе 12, пока не будем на этом останавливаться.

Само приложение не требует для своей работы прав root, но до того момента, как вы не надумаете подмонтировать контейнер к какой-то папке. Помните, я говорил о возможности подмонтировать сейф к папке DCIM или папке приложения? Это возможно осуществить средствами CyberSafe Mobile, но вам понадобятся права root.

Кроме этого приложение позволяет обмениваться зашифрованными файлами с другими пользователями и позволяет шифровать произвольные папки на Google Drive. Впрочем, для каждой бочки меда можно найти ложку дегтя. Приложение платное. А его бесплатная версия ограничивает максимальную длину пароля всего в 2 символа, что, сами понимаете, очень мало. С другой стороны, приложение стоит совсем недорого (дешевле 3$) и оно ограничивает пароль не при открытии контейнера, а только при создании. То есть если вам нужно использовать приложение с одним и тем же набором данных на разных устройствах, то вы можете создать контейнер на одном устройстве и скопировать его на другое, а программу купить только на одном устройстве (на котором будете создавать контейнер).

Второй недостаток этого приложения – поддержка только собственного формата контейнера. Приложение не поддерживает формат TrueCrypt.

Какое приложение выбрать? Ответ прост. Если вы на персональном компьютере используете TrueCrypt, то выбор очевиден – EDS Lite. Если вы хотите обеспечить шифрование облака, то, судя по всему, на компьютере придется перейти на CyberSafe.

15.4. Приложение CyberSafe Mobile

При первом запуске программа попросит установить мастер-пароль (рис. 15.1). Мастер-пароль препятствует доступу к программе, если смартфон попал в чужие руки. В дальнейшем ввод мастер-пароля может потребоваться

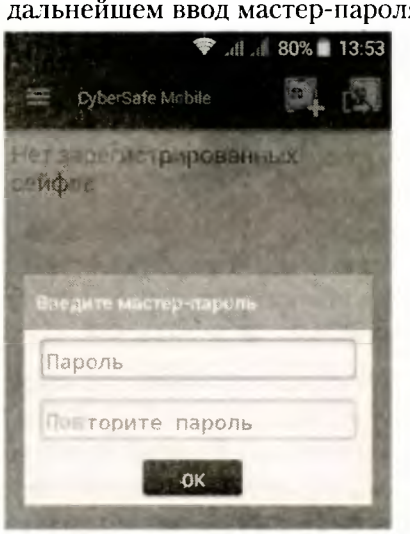


Рис. 15.1. Ввод мастер-пароля

или после перезапуска устройства (когда программа запускается впервые после перезагрузки устройства), или после долгого периода неактивности.

В верхнем правом углу находятся две кнопки: первая используется для создания нового контейнера (рис. 15.2), вторая – для открытия существующего. Рассмотрим сначала процесс создания сейфа – именно так в терминологии программы называется контейнер.

Первым делом нужно нажать кнопку **Путь к сейфу** и выбрать каталог, в котором будет храниться сейф, а также ввести имя файла сейфа (рис. 15.3). Настоятельно рекомендуется размещать сейфы на SD-карте для экономии основной памяти устройства.

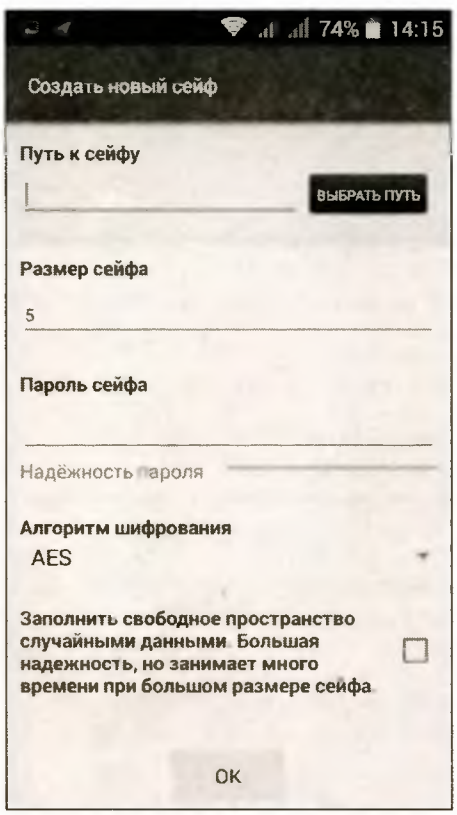


Рис. 15.2. Создание сейфа



Рис. 15.3. Выбор имени файла

Далее нужно ввести размер сейфа (параметр **Размер сейфа**). По умолчанию размер сейфа равен 5 Мб, но в большинстве случаев этого будет мало.

Программа никак не ограничивает размер сейфа и, по сути, размер сейфа ограничен только свободным пространством на вашем устройстве.

Параметр **Пароль сейфа** позволяет задать пароль контейнера. Пароль должен содержать цифры и буквы, состоять из символов разного регистра, содержать символы пунктуации, не содержать имена близких и клички животных, номера телефонов и другую всем известную о вас информацию.

Для большей секретности сейф может быть заполнен случайными данными. Для этого нужно включить параметр **Заполнить свободное пространство случайными данными**.

Для создания сейфа нажмите кнопку **OK**. Процесс создания криптоконтейнера, если отключено заполнение свободного пространства, занимает немного времени. Примерно две-три минуты для сейфа размером 1 Гб. Время создания сейфа зависит от производительности вашего устройства.



Рис. 15.4. Список сейфов



Рис. 15.5. Список файлов в контейнере

При открытии сейфа нужно всего лишь выбрать имя файла сейфа. Программа не регистрирует каких-либо расширений для файлов контейнеров из соображений секретности, поэтому только вы знаете, как называется ваш сейф. Он может называться и foto.jpg. При попытке открыть файл, отличающийся от контейнера, вы увидите сообщение об ошибке.

Все созданные и добавленные сейфы добавляются в список сейфов в разделе **Сейф** (рис. 15.4). На рис. 15.4 изображено два сейфа, оба из них закрыты. Один из сейфов мы создали, а другой – добавили в список. Обратите внимание: что в списке находятся не все сейфы, имеющиеся на устройстве, а только добавленные вами или созданные с момента последней переустановки программы. При переустановке программы список сейфов очищается, однако файлы сейфов, даже добавленные в список, не удаляются.

Чтобы открыть сейф, нужно или коснуться его названия, или вызвать контекстное меню (длинное касание) и выбрать команду **Открыть**. Появится окно ввода пароля сейфа. Нужно ввести пароль, указанный при его создании. Далее программа отобразит список файлов, хранящихся в сейфе. Для нового сейфа данный список будет пуст (рис. 15.5).

Добавить файлы в сейф можно как с помощью стороннего файлового менеджера, так и с помощью файлового менеджера, встроенного в программу. Вот как добавить файлы в сейф с использованием стандартного файлового менеджера:

- Откройте боковое меню и выберите команду **Файловый менеджер**.
- Выберите, где находятся файлы, которые нужно поместить в сейф, – на устройстве или на карте памяти (рис. 15.6). Также обратите внимание, что программа поддерживает работу с сетевыми папками (общие папки Windows).
- Перейдите в папку и выделите файлы, которые нужно добавить в файл. Выделение файлов производится путем касания миниатюры файла.
- Вызовите контекстное меню, выполнив длинное касание выделения (коснитесь пальцем выделения и ждите, пока появится меню), рис. 15.7.
- Выберите команду **Копировать** или **Вырезать** – в зависимости от того, что нужно сделать, скопировать или переместить файлы в сейф.
- Используя боковое меню, перейдите в раздел **Сейф**.

- Откройте сейф, в который нужно скопировать/переместить выделенные файлы.

- Нажмите кнопку **Вставить**, чтобы вставить в сейф выделенные файлы (рис. 15.8).

Начнется процесс копирования/перемещения файлов. Ход операции отображается в области уведомлений, когда файлы будут скопированы, вы увидите соответствующее уведомление в области уведомлений.

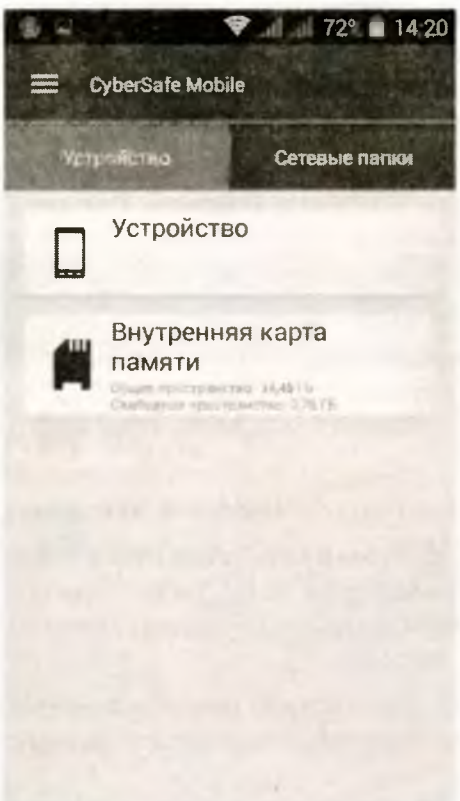


Рис. 15.6. Файловый менеджер

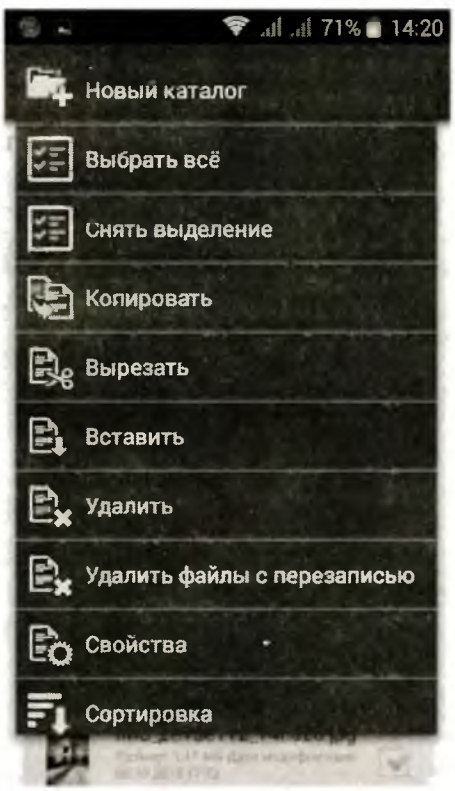


Рис. 15.7. Операции над файлами

15.5. Приложение EDS Lite

Когда вы запускаете программу впервые, список контейнеров пуст (рис. 15.9).

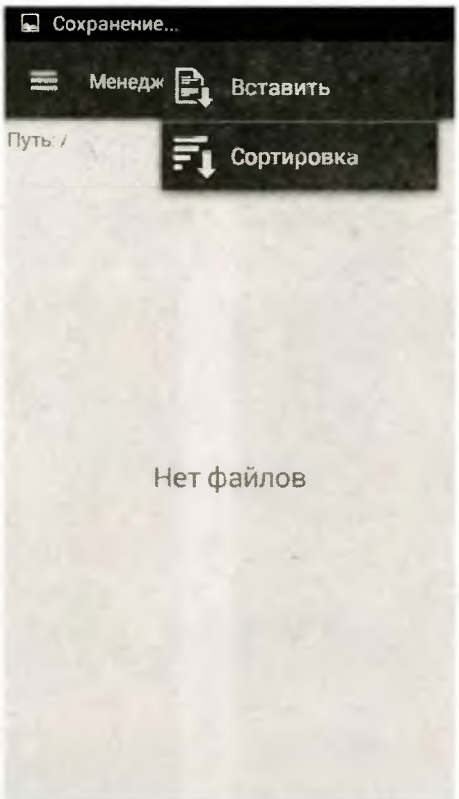


Рис. 15.8. Вставка файлов в контейнер

Для создания нового контейнера нажмите кнопку с изображением ключа и знака +. На появившейся странице вы сможете ввести параметры контейнера (рис. 15.10), а именно:

- **Укажите путь к контейнеру**. Лучше создавать контейнеры на внешней SD-карте. Даже в случае выхода устройства из строя, внешнюю SD-карту можно извлечь и прочитать данные. Да и на внешней карте, как правило, больше места.
- **Пароль контейнера**. Недостаток программы – то, что она допускает использование простых паролей. Ради интереса я ввел пароль qwerty, и программа «проглотила» его. К тому же нет поля подтверждения пароля, поэтому будьте внимательны при вводе пароля, чтобы не допустить ошибку.
- **Размер контейнера.** Определите максимальный размер, который сможет занимать файл, указанный в первом параметре. На рис. 15.10 создается контейнер размером 2 Мб. Это значение по умолчанию очень

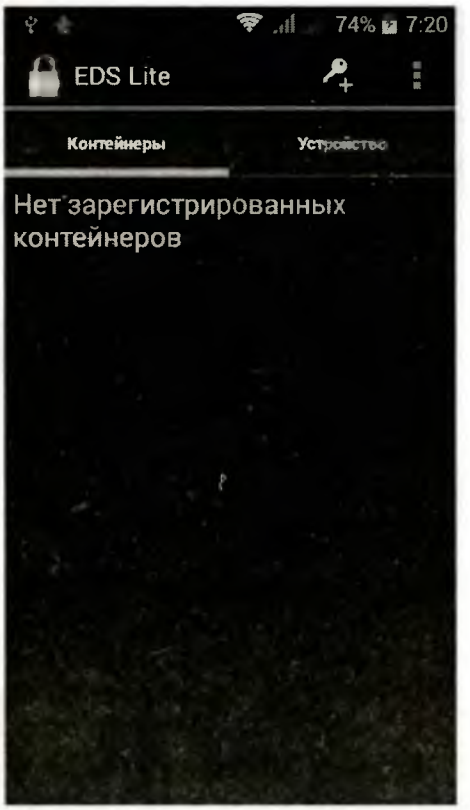


Рис. 15.9. Список контейнеров пуст

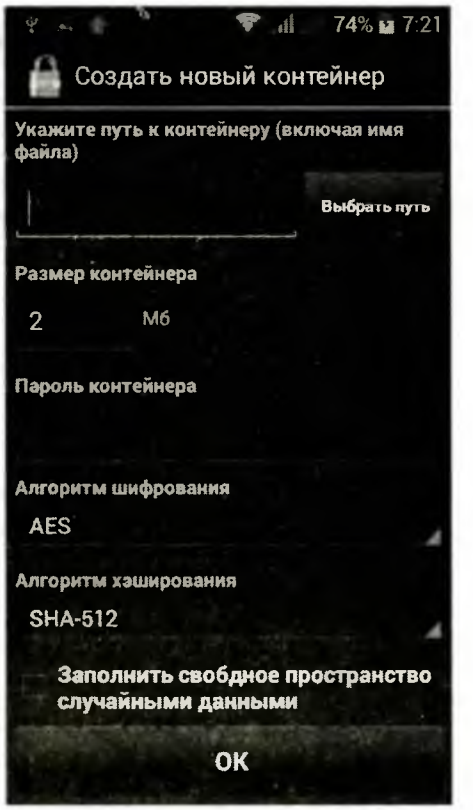


Рис. 15.10. Создание контейнера

мало. Такой маленький контейнер можно создать или чтобы научиться работать с программой, или если вам нужно хранить в контейнеры текстовые документы – они не занимают много места. Размер контейнера определяйте сами, исходя из своих потребностей. Кому-то и 20 Мб будет достаточно, а кому-то и 2 Гб – мало.

Остальные параметры можно оставить без изменения для создания контейнера. После создания контейнера вы увидите его в списке контейнеров (рис. 15.11).

Выберите контейнер. Появится окно ввода пароля. Дальше иллюстрации сделать невозможно, поскольку программа блокирует возможность создания снимков экрана – нельзя «сфотографировать» ни окно ввода пароля, ни содержимое контейнера.



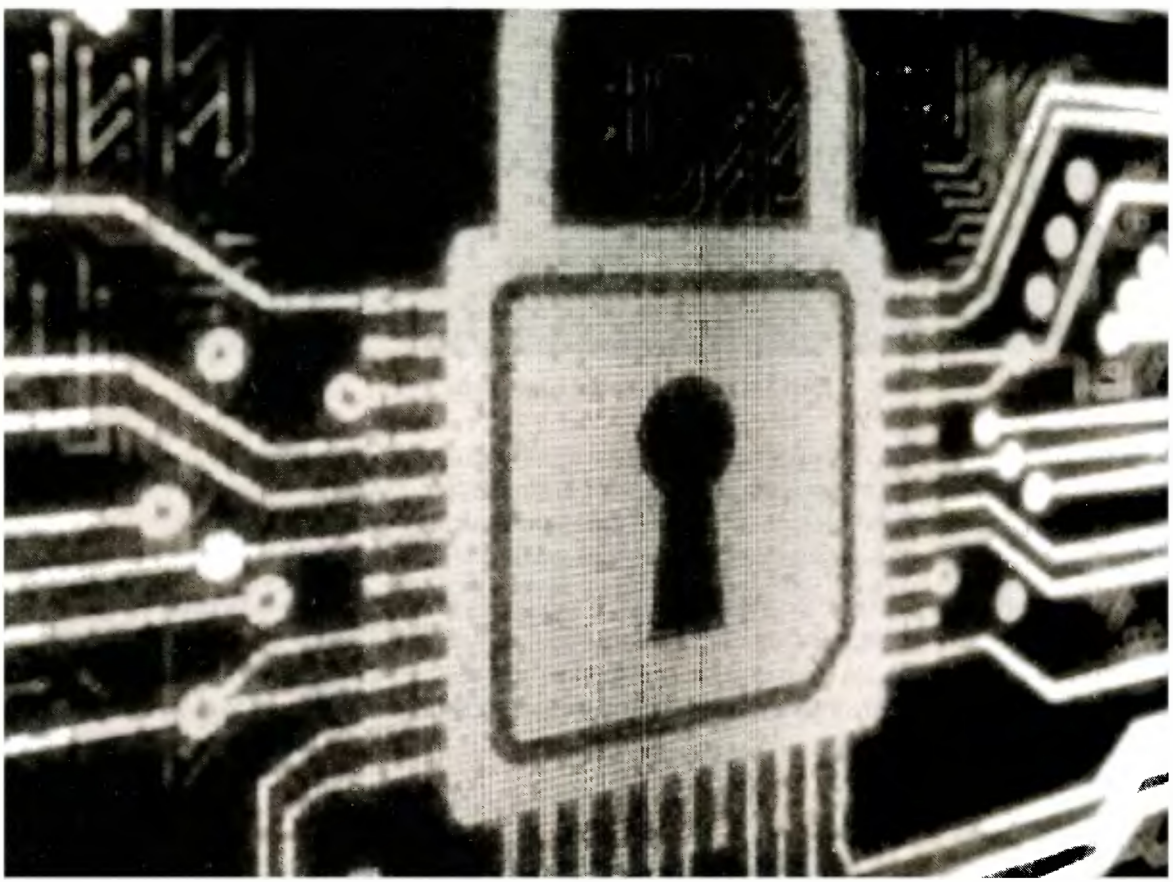
Рис. 15.11. Созданный контейнер

Когда контейнер будет открыт, вы увидите двухпанельный файловый менеджер. Используйте его для помещения в контейнер файлов. Они будут зашифрованы. Незашифрованные версии файлов на вашей SD-карте нужно удалить (иначе какой смысл в создании контейнера?).

Программа EDS Lite довольно удобная. Да, она не позволяет работать с зашифрованными файлами через сторонние файловые менеджеры, но зато не требует права root. Да и в отличие от стандартных средств шифрования, позволяет зашифровать только те файлы, которые нужны, а не все устройство или не всю SD-карту.

Глава 16.

Защита фото и видео "на лету"



16.1. Приложения для защиты фото и видео

Защищать фото и видео можно по-разному. Все зависит от того, какая вам нужна защита. Можно, например, создать криптоконтейнер и в спокойной обстановке переместить в него отснятый материал (фотографии и видеоролики). Для такой защиты подойдет любое приложение, поддерживающее криптоконтейнеры.

Совсем другое дело, когда нужно сразу защищать отснятый материал. Тогда вам пригодятся специальные приложения.

По правде говоря, защита фото и видео в Android все равно так или иначе связана с криптоконтейнерами. Просто существуют приложения, позволяющие автоматизировать рутинную работу с ними.

В этой главе мы рассмотрим два приложения – Hide Pictures & Videos (Vaulty) и CyberSafe Mobile. Первая подойдет для тех, у кого нет root-доступа к устройству, а вторая – тем, у кого этот доступ есть.

16.2. Приложение Hide Pictures & Videos

В Play Market вы можете найти много приложений для сокрытия фотографий и видео. Почему выбрано именно это приложение? Потому что, в отличие от других программ, это приложение реально работает. Но у него есть недостаток – оно на английском языке. Однако приложение просто в использовании, поэтому англоязычный интерфейс нельзя назвать серьезным недостатком.

Принцип работы этого приложения прост. Оно создает криптоконтейнер где-то на SD-карте, точный путь изменить нельзя, но при желании его мож-

но хотя бы вычислить. В этот контейнер вы можете переместить уже отснятые фото и видео. Также есть возможность снять фото и видео с записью в этот контейнер. Программа не производит каких-либо системных низкоуровневых операций, поэтому права root не нужны.

Посмотрим, как оно работает. При первом запуске приложение отображает список своих возможностей (рис. 16.1). Кроме помещения файлов в криптоконтейнер оно может выполнить их резервное копирование. Также есть встроенный просмотрщик и органайзер для фотографий.



Рис. 16.1. Список возможностей приложения



Рис. 16.2. Резервное копирование фото

Нажмите кнопку **Accept**. Далее приложение предложит настроить резервное копирование (рис. 16.2). Если оно вам не нужно, выберите **No backup**.

Далее нужно выбрать, какой способ защиты использовать – пин-код, текстовый пароль или без пароля (немного не понимаю, зачем нужен этот способ), см. рис. 16.3.

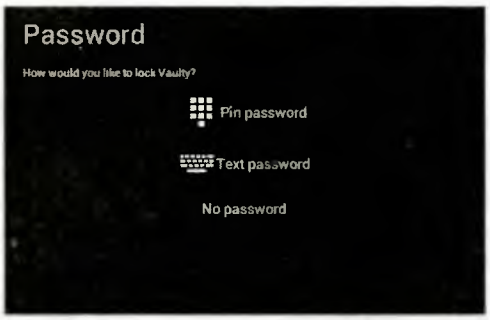


Рис. 16.3. Тип защиты

Самый безопасный тип защиты – текстовый пароль. Выберите его и введите сначала пароль (рис. 16.4), затем – его подтверждение, а потом – контрольный вопрос и ответ в случае, если забудете пароль.



Рис. 16.4. Установка пароля

Приложение сообщит, что в контейнере пока ничего нет. Нажмите кнопку **HIDE PICTURES & VIDEOS** (рис. 16.5).

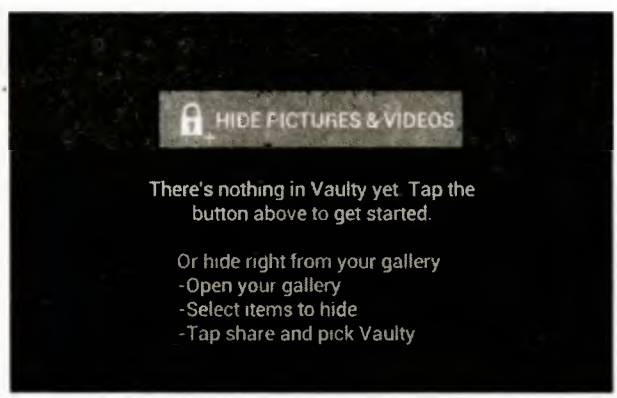


Рис. 16.5. Нажмите единственную кнопку

Далее нужно выбрать фотографии, которые вы хотите скрыть. Приложение отобразит вашу галерею (рис. 16.6).



Рис. 16.6. Галерея фото и видео

Перейдите в один из каталогов и выберите фото, которые нужно скрыть. В верхнем правом углу есть кнопка, позволяющая выбрать все фото/видео (рис. 16.7). Затем нажмите кнопку с изображением замка. Начнется перемещение выбранных объектов в контейнер (рис. 16.8). Далее вы увидите список защищенных объектов в вашем контейнере (рис. 16.9).

Обратите внимание на рис. 16.9. В верхнем правом углу есть кнопка **CAMERA**. Нажмите ее, чтобы снять фото или видео. Снятый материал сразу попадет в контейнер. При повторном входе в программу будет запрошен



Рис. 16.7. Выбор фото для защиты

пароль, установленный при ее первом запуске. Изменить пароль можно в настройках программы.



Рис. 16.8. Перемещение фото в контейн

Рис. 16.9. Список объектов в контейнере

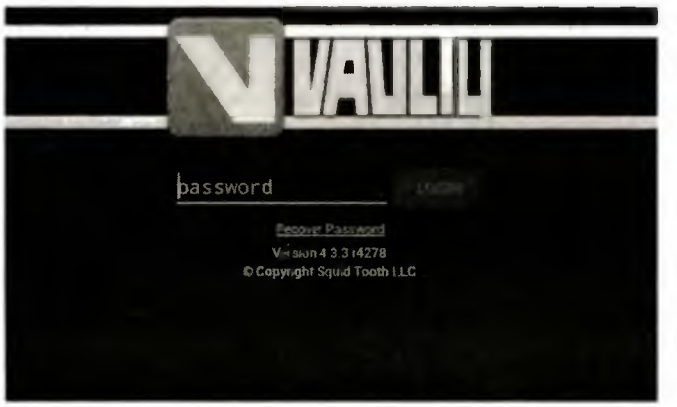


Рис. 16.10. Вход в программу

16.3. CyberSafe Mobile

Здесь защита фото и видео построена несколько другим образом. Собственно, приложению все равно, что защищать, но здесь будет показан пример, как защитить фото и видео.

Первым делом нужно создать довольно большой криптоконтейнер. Например, 4 Гб. Если вы снимаете только фото, то его хватит на более чем 2700 фото (примерно 1.5 Мб каждое фото, камера 5 Мп). Можно, конечно, создать контейнер и большего размера, если достаточно места на SD-карте. В предыдущей главе был описан процесс создания криптоконтейнера в этой программе, поэтому не будем на нем останавливаться.

Далее нужно настроить автоматическое монтирование контейнера к папке /storage/sdcard0/DCIM/Camera. Именно в эту папку помещаются все отснятые фото и видео. Конечно, в настройках камеры нужно установить, чтобы фотографии сохранялись на SD-карту, а не в память телефона.

При открытии сейф может быть подмонтирован к установленному пользователем каталогу (точка монтирования). Это означает, что после монтирования можно будет обращаться к файлам сейфа через этот каталог. Любые файлы, скопированные в этот каталог, автоматически попадут в сейф. Любые изменения в сейфе сразу же отразятся в точке монтирования. Пользователям ОС UNIX/Linux знакома операция монтирования (команда mount) – принцип тот же.

Также сейф может быть автоматически подмонтирован при запуске устройства. Автоматическое монтирование может быть полезно для шифрования данных определенного приложения.

В нашем случае таким приложением будет приложение Camera, сохраняющее свои данные в приведенный ранее каталог.

При наличии root-доступа при первом запуске программа предложит включить монтирование сейфов (рис. 16.11). Если вы откажетесь, позже можно будет включить монтирование в настройках программы

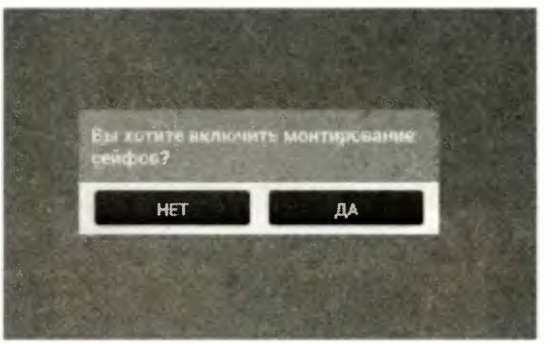


Рис. 16.11. Включение монтирования

При включенном монтировании в окне **Свойства сейфа** появятся следующие параметры (рис. 16.12):

- **Путь для монтирования** – здесь нужно указать каталог, к которому будет монтироваться контейнер. Если оставить это поле пустым, то сейф будет подмонтирован к каталогу <default>\<имя_сейфа>. Каталог по умолчанию (default) определяется в настройках программы. Здесь нужно указать каталог /storage/sdcard0/DCIM/Camera.
- **Автоматически монтировать сейф при загрузке** – контейнер будет смонтирован автоматически при загрузке Android. Параметр подходит для описанного ранее сценария использования программы.
- **Автоматически монтировать сейф на старте программы** – контейнер будет подмонтирован после запуска программы. Пока вы не введете мастер-пароль, контейнер смонтирован не будет.

Чтобы автоматическое монтирование было действительно автоматическим, нужно включить параметр **Запомнить пароль**, хотя это и не очень безопасно.

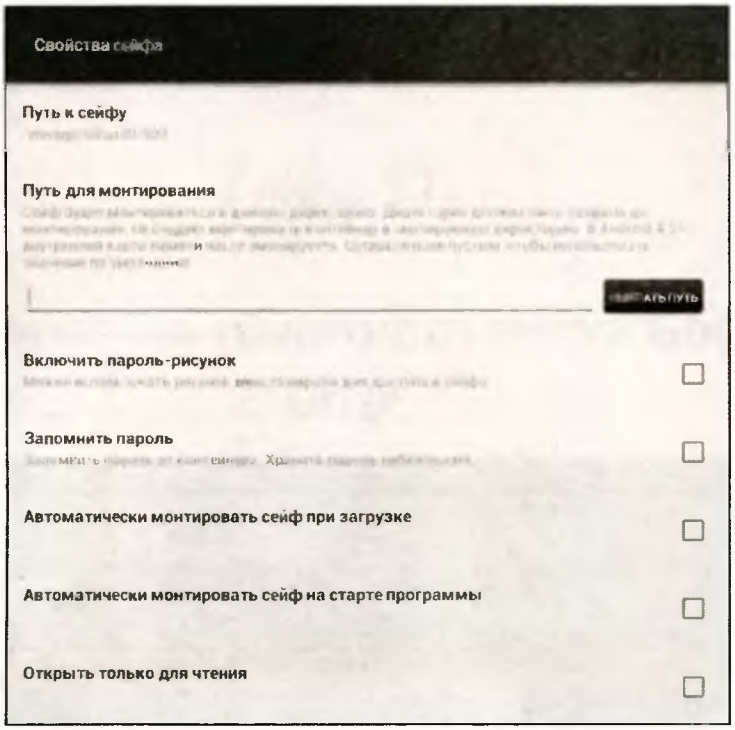
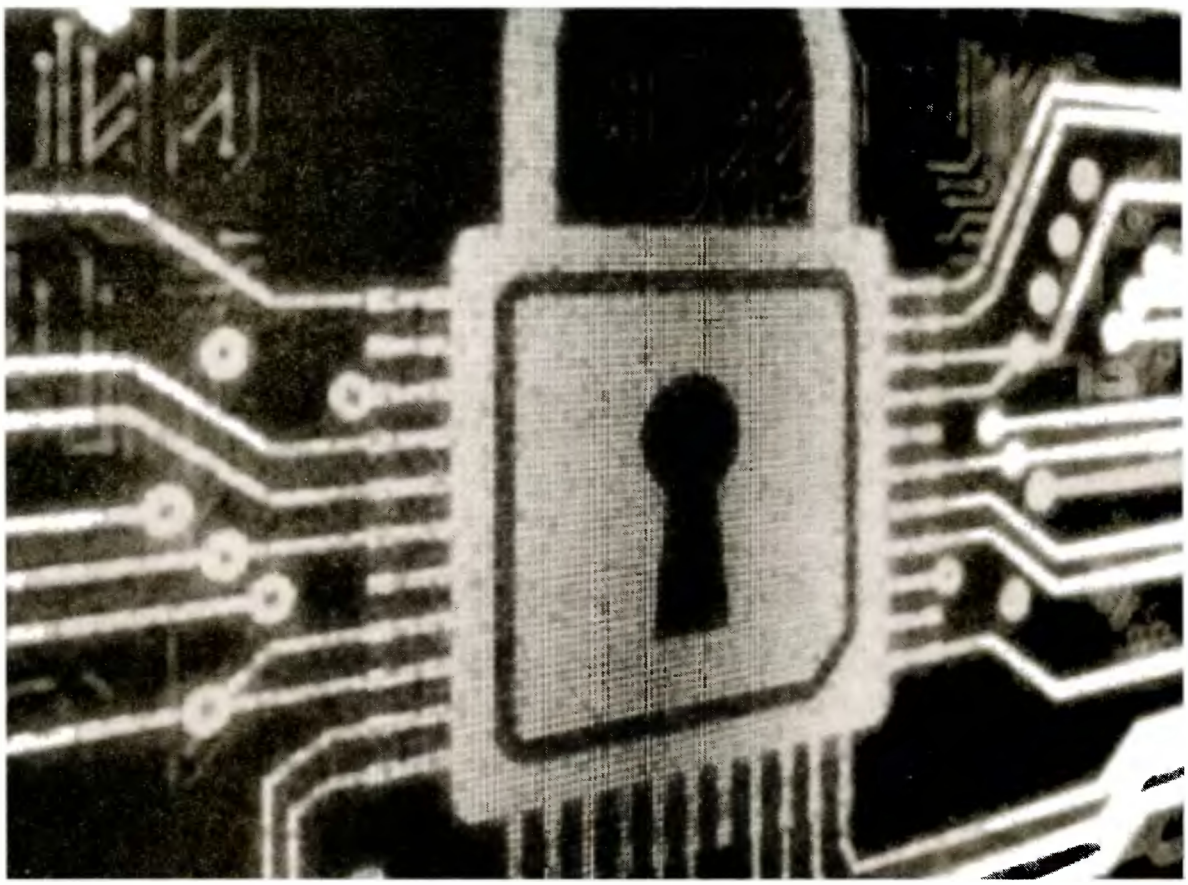
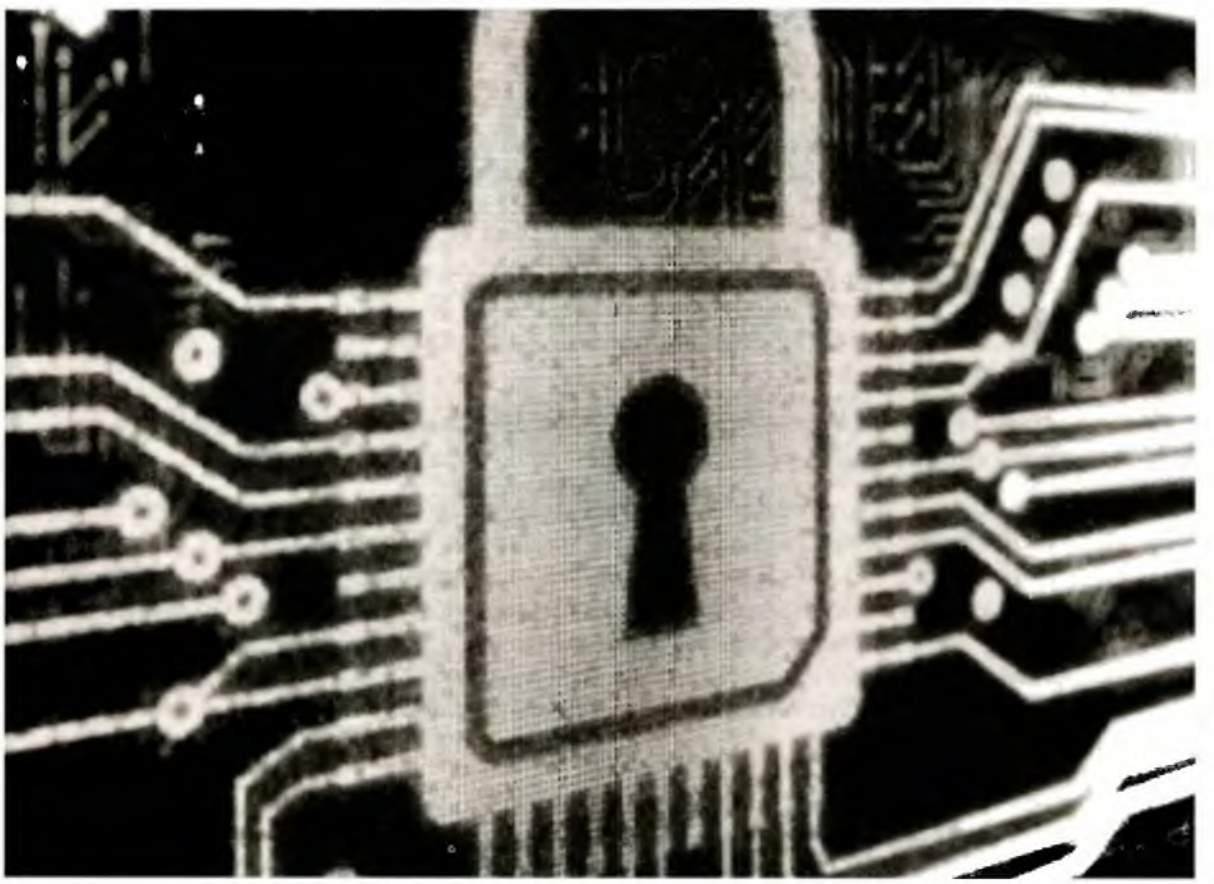


Рис. 16.12. Настройка монтирования контейнера к каталогу



Глава 17.

Шифрование облачного диска Google Drive



17.1. Шифрование и синхронизация папки облачного диска

В этой главе будет рассмотрено простое приложение для шифрования облачного диска Google Drive – CyberSafe Mobile. Это далеко не единственное приложение, и вы можете использовать тот же Boxcryptor. Преимущество Boxcryptor в том, что он может поддерживать разные облачные сервисы, а не только Google Drive, но за его использование нужно заплатить 36 евро в год, что довольно дороговато. Есть, конечно, и бесплатная версия, но она есть и у CyberSafe Mobile – CyberSafe Mobile Lite. Перед тем как сделать окончательный выбор, установите обе программы и выберите ту, которая вам больше подходит.

Итак, сейчас перед нами стоит следующая задача. Есть некий контейнер, содержимое которого нужно синхронизировать с папкой Google Drive.

При включении синхронизации содержимое контейнера синхронизируется с содержимым выбранной папки, находящейся на вашем Google Drive. А это означает, что любой файл, который вы поместили в контейнер, будет отправлен (естественно, в зашифрованном виде) в указанную папку на Google Drive. Аналогично, любой файл, добавленный в эту папку, будет автоматически скопирован в сейф. Понятно, что вручную в эту папку добавлять файлы не нужно. Синхронизацию правильно настраивать так:

- Создаются контейнеры одинакового размера на разных устройствах.
- На обоих устройствах используется один и тот же Google-аккаунт.
- В качестве папки синхронизации выбирается одна и та же папка на Google Drive. Потом, когда вы добавите в контейнер какой-то файл

на одном устройстве, он через некоторое время появится и на втором устройстве (в контейнере). Google Drive здесь играет роль буферной зоны, в которой хранятся зашифрованные файлы.

Рассмотрим процесс первоначальной настройки синхронизации с Google Drive. При первоначальной настройке вам нужно создать/импортировать личный ключ, а также добавить Google-аккаунт в программу.

Последовательность действий:

1. Вызовите контекстное меню сейфа и выберите команду **Синхронизировать содержимое сейфа с Google Диск**.
2. Первым делом программа предложит создать или загрузить ключ (рис. 17.1).



Рис. 17.1. Управление ключами

Если у вас нет ключа, нажмите кнопку **Создать ключ**, после чего введите пароль (рис. 17.2) для ключа и выберите один из Google-аккаунтов (аккаунт

должен предварительно быть настроен в вашем устройстве, см. рис. 17.3).

Далее программа сообщит, что у вас уже есть ключ (рис. 17.4). Можно нажать кнопку **Публикация ключа**, чтобы опубликовать ваш публичный ключ на нашем сервере ключей. После публикации ключа его смогут найти другие пользователи нашей программы, что облегчает обмен ключами между пользователями.



Рис. 17.2. Ввод пароля для ключа

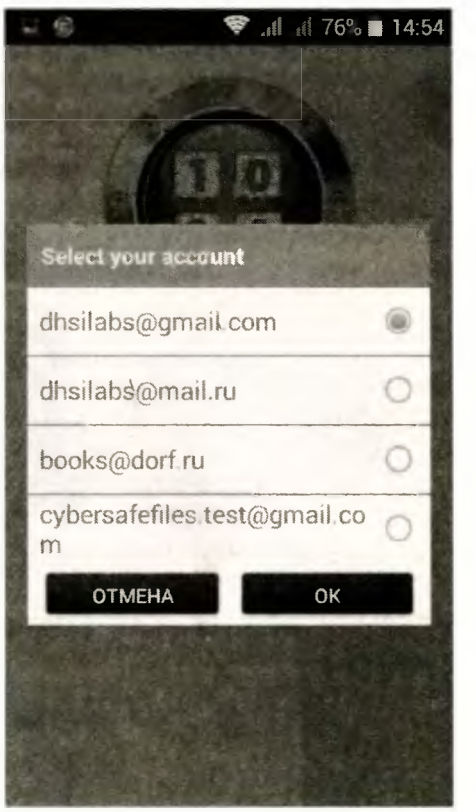


Рис. 17.3. Выбор аккаунта для ключа

Если у вас есть ключ, тогда нажмите кнопку **Загрузить ключ** и перейдите в каталог с файлами ключа. Выберите ID-файл и нажмите кнопку **Выбрать**. При импорте ключа программа попросит вас ввести соответствующий ключу пароль.

После загрузки ключа вы увидите экран, изображенный на рис. 17.4, информирующий, что ключ уже создан/загружен. Нажмите кнопку **Назад** на вашем устройстве, чтобы перейти к настройке Google Диска.



Рис. 17.4. Ключ создан/импортирован



Рис. 17.5. Google-диски не добавлены

При первоначальной настройке не будут добавлены какие-либо Google-диски (рис. 17.5). Нажмите кнопку в верхнем левом углу для добавления Google Диск.

Выберите один из зарегистрированных на устройстве аккаунтов (рис. 17.6). После этого выбранный вами аккаунт появится в списке. Вы можете добавить сразу несколько Google-аккаунтов.

Выберите нужный Google Диск, появится список папок. Выберите (или создайте) папку, которая будет использоваться в качестве папки синхронизации с вашим сейфом (рис. 17.7). Нажмите кнопку **Выбрать**. Начнется процесс синхронизации файлов. По окончанию этого процесса вы получите уведомление (в области уведомлений). Желательно, чтобы процесс синхро-

низации проходил, когда вы подключены к Интернету по Wi-Fi или 4G (чем выше скорость передачи данных, тем быстрее завершится синхронизация).

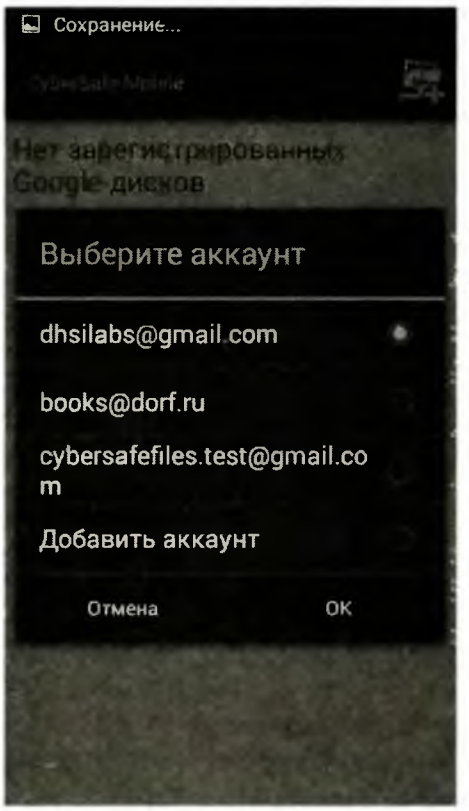


Рис. 17.6. Выбор аккаунта Google

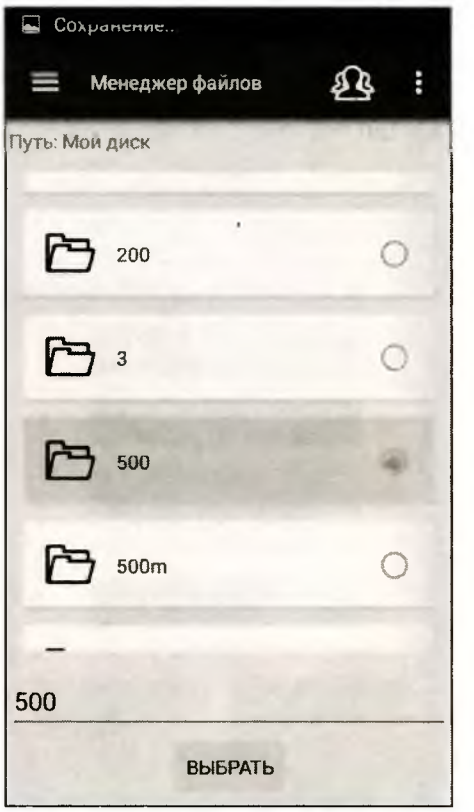


Рис. 17.7. Выбор/создание папки синхронизации

17.2. Простое шифрование облачной папки

Иногда нужно просто зашифровать облачную папку. Вам не нужна синхронизация, нужно просто чтобы в определенной папке на Google Drive файлы были зашифрованными. Первым делом нужно создать/импортировать ключ, как было показано в предыдущем разделе. После этого нужно добавить Google-аккаунт – то же было продемонстрировано в прошлом разделе. Проще всего это сделать при настройке синхронизации. Можете включить синхронизацию с папкой, а потом ее выключить, если она вам не нужна. Просто при первом включении синхронизации программа предло-

жит сделать как раз то, что нам нужно, – создать/импортировать ключ и зарегистрировать Google-аккаунт в программе. Можно это сделать и другим путем – ключи можно создать в настройках программы, а потом добавить Google-аккаунт в разделе Google Drive меню программы.

После того как вы подключите Google-аккаунт в программе, выберите папки, которые вы хотите зашифровать, и выберите команду **Зашифровать выбранные папки** из контекстного меню (рис. 17.8). Для шифрования одной папки нужно в нее зайти и выбрать команду меню **Расшифровать текущую папку**. Для расшифровки папки нужно выбрать команду **Расшифровать текущую папку**.

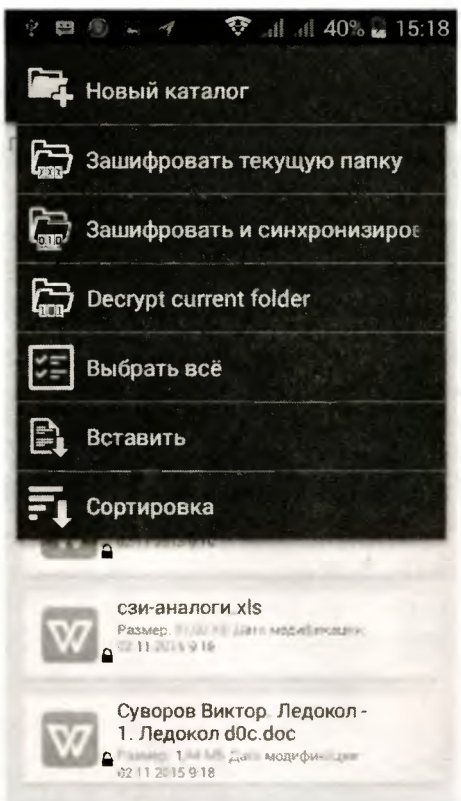


Рис. 17.8. Меню программы

17.3. Передача зашифрованных файлов другим пользователям с помощью Google Drive

Программа CyberSafe Mobile позволяет поделиться файлами (то есть предоставить общий доступ к зашифрованным файлам) с другими пользователями. При передаче файлов из сейфа другому пользователю файлы шифруются публичным ключом получателя файлов. Получатели могут расшифровать файлы, используя свои закрытые ключи. Процесс шифрования и дешифрования происходит прозрачно для пользователя, поэтому последний ничего не замечает.

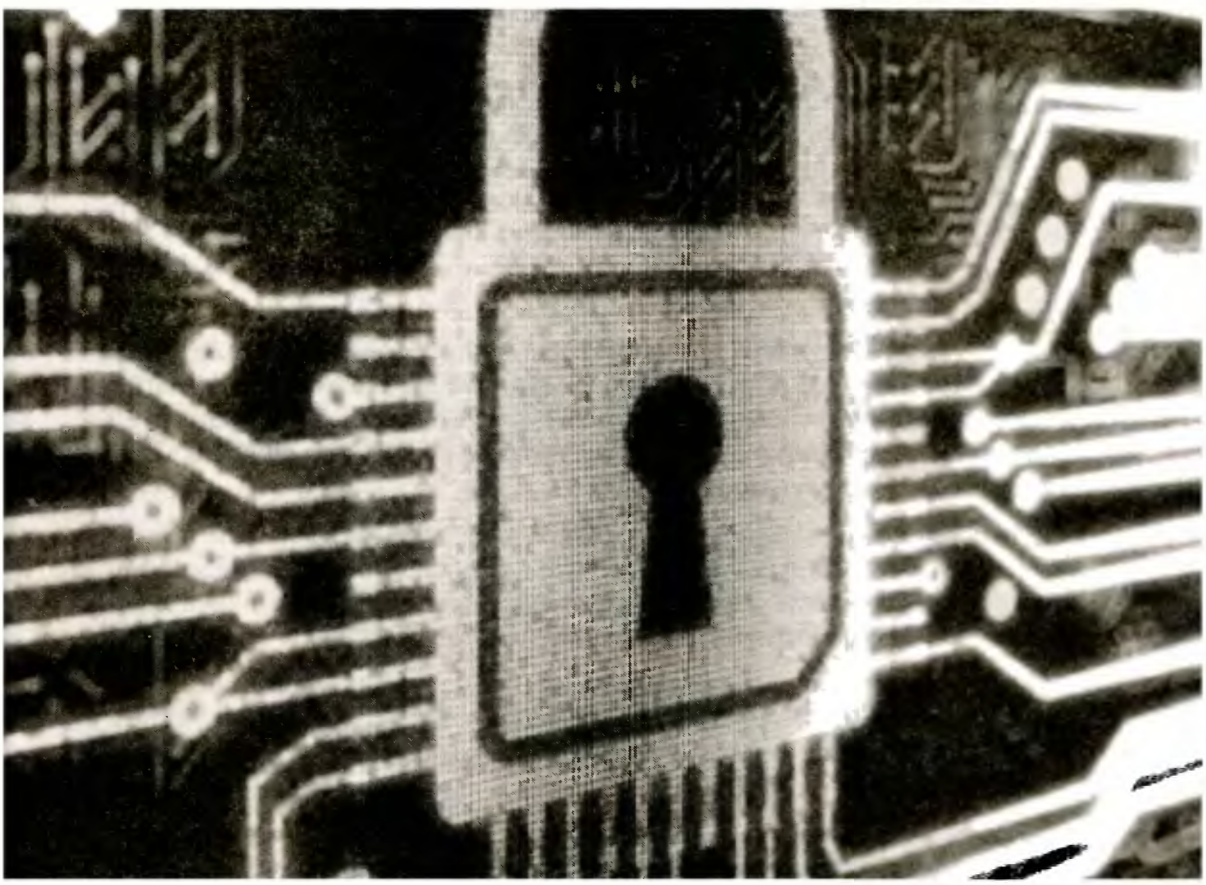
Передать файлы другому пользователю очень просто. Для этого нужно открыть контейнер, выбрать файлы и выполнить команду **Поделиться** (пиктограмма пользователя со стрелкой). Далее нужно выбрать пользователя (или пользователей), которому вы хотите отправить файлы. Если список пользователей еще пуст, нажмите кнопку поиска (с изображением лупы) и введите e-mail пользователя. Если он уже опубликовал свой публичный ключ на сервере, он будет автоматически импортирован.

> Внимание! При «расшаривании» файлов они помещаются (копируются) в папку Shared/<имя пользователя> вашего сейфа, поэтому перед тем как «поделиться» файлами, убедитесь, что сейфе есть достаточно свободного места!

Пользователь по e-mail будет уведомлен о том, что ему предоставлен доступ к файлам. Файлы, которые вы отправили пользователю, он сможет просмотреть в разделе **Доступные мне** на своем устройстве.

Глава 18.

Защита передаваемых по сети данных от прослушивания



18.1. Как защищать передаваемые по сети данные в Android?

Ранее было показано, как зашифровать данные, находящиеся на вашем смартфоне или планшете. Теперь мы поговорим о защите данных, которые передаются по сети: ведь когда вы просматриваете веб-страницы, вводите пароли к этим веб-страницам и другую важную информацию (например, сообщения в чате социальной сети) – эта информация может быть перехвачена. Далеко не все сайты используют протокол HTTPS, поэтому часть информации передается в открытом виде.

Кто может перехватить ваши данные? Как минимум, это недобросовестные владельцы бесплатных Wi-Fi-сетей, к которым вы подключаетесь. Также ваши данные может перехватить провайдер того человека, к чьей Wi-Fi-сети вы подключаетесь, и, конечно же, передаваемая информация доступна вашему сотовому оператору.

Кроме самой передаваемой информации иногда есть смысл скрыть посещаемые узлы. В этом случае, даже если злоумышленник/провайдер/оператор не увидит, какие данные вы передаете (при использовании протокола HTTPS), он сможет просмотреть, какие узлы вы посещали.

Способы защиты такие же, как и в случае с компьютером: VPN и сеть Tor. В первом случае будет защищен весь трафик, поскольку он будет проходить внутри VPN-соединения, а ваш провайдер или оператор сети увидит только соединение с VPN-сервером.

Конечно, теоретически данные может перехватить сам VPN-сервис, но поскольку он лицо незаинтересованное, да еще и находится, как правило, в другой стране, то до вас ему нет никакого дела.

С сетью Tor немного сложнее. Она хоть и бесплатна, но ее использовать смогут лишь те программы, которые можно настроить на Tor. Как правило, это браузеры и некоторые клиенты для отправки мгновенных сообщений. Сам факт подключения к сети Tor еще не означает защиты ваших данных. Нужно, чтобы сетевое приложение было настроено на Tor. Если вас интересует только защита браузера, то сети Tor будет полностью достаточно. А вот с другими приложениями нужно или их настраивать должным образом (что в случае с Android-приложениями не всегда возможно), или использовать VPN.

18.2. Выбор VPN-сервиса

Для использования VPN вам нужно найти подходящий VPN-сервис. Данные отправляются в зашифрованном виде на VPN-сервер, откуда пересылаются тому узлу, с которым вы фактически желаете работать. Провайдер не увидит, какие данные и какому узлу вы отправляете. Он увидит только зашифрованное соединение с VPN-сервером.

Хорошие VPN-сервисы платные. Платить немного, но придется. В среднем за использование VPN-сервиса нужно будет заплатить около 50 долларов в год.

Ранее вы уже познакомились с сервисом Private Internet Access (**http://privateinternetaccess.com/**). Это один из самых известных сервисов, предоставляющих услуги анонимизации в сети. Кроме привычных услуг (анонимизация, обеспечение конфиденциальности, шифрование) он предоставляет защиту от изменения DNS серверов (DNS leak protection).

Стоимость PIA не высока – примерно 40 долларов в год, при этом стоимость одного месяца использования составит всего 3.33$. Если же вы предпочитаете помесячную оплату, тогда придется платить 6.95$ в месяц, что в два раза дороже. Нужно отметить, что вы получаете за эти деньги неограниченный трафик, то есть кроме оплаченной суммы вам больше не придется платить. Это окончательная сумма.

VPN-клиент для Android 5.x/4.x можно установить с Play Market:

https://play.google.com/store/apps/details?id=com.privateinternetaccess.android

К преимуществам этого сервиса можно отнести высокую скорость работы и относительно недорогую стоимость. Но есть и недостатки. В частности,

VPN-серверы расположены всего в 10 странах мира. Другие сервисы предоставляют больше разнообразия.

Сервис http://www.vpnshieldapp.com/ отличается очень невысокими ценами. Так, месяц доступа обойдется в 3.99$, но возможна и понедельная оплата. В этом случае неделя обойдется всего в 1 доллар, а подписка на год стоит 30 долларов. Это один из самых дешевых сервисов.

VPN-клиент доступен в Play Market:

https://play.google.com/store/apps/details?id=com.vpnshieldapp&hl=ru

Данный сервис не собирает, в отличие от предыдущего, информацию о клиентах, во всяком случае, так сказано на их веб-сайте.

VPN-сервис IPVanish VPN (https://www.ipvanish.com/) обойдется вам или в 10 долларов в месяц, или в 78 долларов в год. Это самый дорогой VPN-провайдер, рассматриваемый в этой книге.

Серверы находятся в США, Канаде, Великобритании, Франции, Японии, Малайзии, Венгрии, Нидерландах, Южной Африке, Испании, Швеции и Южной Корее.

Поскольку сервер находится в США, то на него распространяется действие акта DMCA Copyright Policy, а это означает, что он следит за своими пользователями. Какая именно информация собирается, на сайте сервиса не сказано.

Как по мне, идеальным вариантом является второй рассмотренный сервис. Он самый дешевый и не находится в США (следовательно, на него не распространяется акт DCMA). Вообще в мире существует много VPN-сервисов, но я не вижу смысла рассматривать все из них в этой книге. Если вам будет мало перечисленных сервисов, вы всегда сможете найти дополнительные.

18.3. Настройка VPN-клиента

Настройка VPN-клиента, как правило, не требуется: вам нужно установить VPN-клиент вашего сервиса и нажать кнопку подключения. На этом все. Но некоторые сервисы не предоставляют Android-клиентов, поэтому вам придется использовать клиент, встроенный в сам Android:

- Откройте настройки телефона (**Настройки**).
- Перейдите в **Беспроводные сети, Еще, VPN**.
- Нажмите кнопку **+** в верхнем углу.
- Введите название VPN-соединение, адрес VPN-сервера, имя пользователя, пароль (эти данные вы получите у VPN-провайдера).
- Перейдите в **Беспроводные сети, Еще, VPN** и выберите созданное VPN-подключение для использования. После успешного подключения все данные будут передаваться в зашифрованном виде.

18.4. Tor в Android

О том, что такое Tor и как он работает, было рассказано в главе 6. Сейчас же мы рассмотрим только настройку Tor в Android.

Torrent-клиент для Android называется Orbot, и загрузить его можно по адресу:

https://play.google.com/store/apps/details?id=org.torproject.android

Напомню, что установка Orbot не означает, что теперь ваше устройство защищено, и вы можете безопасно передавать данные. Требуется дополнительная настройка.

Запустите Orbot. Вы увидите большую серую луковицу – это символ проекта Tor. Серая она потому, что вы не подключены к сети Tor в данный момент (рис. 18.1).

Нажмите на луковицу. Начнется процесс подключения к сети Tor. После подключения к сети Tor вы увидите сообщение, изображенное на рис. 18.2.

Сообщение гласит, что вы подключены к Tor, но это не означает, что ваше устройство безопасно. Нажмите кнопку **Browser** для проверки вашего соединения. Далее вам предложат установить приложения, оптимизированные для работы с сетью Tor, см. рис. 18.3. Выберите приложение Orfox – это аналог Firefox, уже настроенный на работу с Tor. Установите это приложение.



Рис. 18.1. Приложение Orbot



Рис. 18.2. Вы подключены к сети Tor

После установки Orfox порядок работы будет следующий. Первым делом вам нужно запустить Orbot и убедиться, что соединение с Tor установлено. Далее запустить Orfox и открыть нужный вам сайт.



Рис. 18.3. Какой браузер использовать?

Глава 19.

Обзор Android-приложений для шифрования данных



19.1. Многообразие выбора

В этой главе будет приведен обзор приложений, которые не вошли в эту книгу. В Google Play можно найти множество приложений, так или иначе связанных с шифрованием.

Рассмотреть все такие приложения – запутать пользователя. Но дать рекомендации относительно самостоятельного освоения – другое дело. В этой главе будет краткий обзор приложений шифрования данных, доступных на Google Play.

Чтобы рассмотреть все приложения шифрования данных, нужно написать книгу, посвященную только им. Но вряд ли она будет пользоваться спросом. Поэтому в качестве бонуса в этой главе мы рассмотрим самые популярные приложения и сравним их функционал.

19.2. Приложения для шифрования облака

Прежде чем мы перейдем к рассмотрению приложений, хочется выделить некоторые (табл. 19.1) приложения для шифрования облака. Это очень хорошие приложения, достойные вашего внимания.

Таблица 19.1. Продукты облачного шифрования

Название	Ссылка на Google Play
Boxcryptor Classic	https://play.google.com/store/apps/details?id=com.boxcryptor.android&hl=en
Boxcryptor	https://play.google.com/store/apps/details?id=com.boxcryptor2.android
Cloudfogger Cloud-Encryption	https://play.google.com/store/apps/details?id=com.cloudfogger.cf

Приложение Boxcryptor - довольно неплохое. Привожу ссылку на его описание:

http://www.techrepublic.com/article/easy-steps-for-better-google-drive-security/

Однако в книге оно не рассматривалось из-за того, что оно совсем не дешевое. Неограниченная версия для личного использования стоит 36 евро в год. Дороговато только для личного использования. Ладно бы просто 36 евро, но каждый год – это очень дорого для мобильного приложения. Для сравнения, тот же CyberSafe Mobile стоит менее 3 долларов, которые нужно заплатить один раз.

19.3. Краткое описание приложений шифрования

Далее приводится таблица, содержащая мое личное мнение об этих приложениях и мнение других пользователей, то есть рейтинг приложения на Google Play.

Таблица 19.2. Список конкурентов

Приложение	Краткое описание	Рейтинг
Encryption sentence	Ужасное приложение шифрования текста. Просто шифрует и расшифровывает текст. Не устанавливайте его.	3,6
SSE Universal Encryption App	Простенькая утилита – симметричное шифрование файла AES, Blowfish и подобными, менеджер паролей и шифрование текста.	4,3

Hide Pictures & Videos – VAULT	В приложении есть один криптоконтейнер, в который можно добавить файлы из Gallery (фото и видео), также можно создать фото/видео прямо из приложения, они будут помещены в этот контейнер. При первом запуске позволяет установить мастер-пароль, который используется для доступа к зашифрованным файлам.	4,4
App Encrypt Lock	Блокировка запуска приложений по паролю, есть приложения и лучше, например, AppLock, не знаю, почему это приложение в топ Google Play, да еще и по слову «шифрование» (видимо, из-за названия). В таблицу сравнения это приложение включено не будет, поскольку, по сути, не является приложением для шифрования.	3,7
Crypto Ghost – File Encryption	Шифрование AES-симметричное, шифрует отдельные файлы. Если нужно файл передать другу, то асимметричное шифрование. У друга тоже должен быть Crypto Ghost x, файл будет зашифрован его публичным ключом, созданным при установке программы.	4,8
Safe Camera – Photo Encryption	Создает криптоконтейнер для хранения фото, которое делается из программы. Позволяет задать мастер-пароль, который используется для доступа к созданным ранее фото.	4,0
Encryption	Программа шифрования текста, не устанавливайте ее.	3,8
Verschl sselung (Krypto)	Программа шифрования текста. Еще одна программа для шифрования просто текста, шифрование файлов не поддерживается.	4,0

Telegram	Мессенджер наподобие Viber, однако с функцией зашифрованного чата. Имейте в виду, что шифрование чата работает только в Android-версии программы. Есть и Windows-версия, но она не поддерживает шифрование чата.	4,3

Как видите, оказалось, что далеко не все программы, в названии которых есть слово «шифрование», являются программами для шифрования в нашем понимании этого слова. В следующей таблице такие программы рассматриваться не будут.

19.4. Сравнение приложений для шифрования

Далее приводится сравнение функционала программ шифрования. Также в эту таблицу были включены рассмотренные ранее программы – EDS Lite и CyberSafe Mobile.

Таблица 19.3. Сравнение функционала программ шифрования

Функция	EDS Lite	Cyber-Safe Mobile	SSE Universal Encryption App	Hide Pictures & Videos – VAULT	Crypto Ghost	Safe Camera – Photo Encryption
Хранение файлов в криптоконтейнере	+	+	-	+	-	+
Монтирование контейнера	+	+	-	-	-	-
Синхронизация контейнера с Google Drive	-	+	-	-	-	-
Расшаривание файлов	-	+	-	-	+	-

Шифрование папок Google Drive	-	+	-	-	-	-
Операции с файлами Google Drive	-	+	-	-	-	-
Менеджер паролей	-	-	+	-	-	-
Шифрование отдельных файлов	+ (*)	+ (*)	+	-	+	-
Шифрование текста	-	-	+	-	-	-
Создание фото/видео сразу в зашифрованный контейнер	+ (**)	+ (**)	-	+	-	+

(*) Можно создать контейнер и поместить в него 1 файл
(**) Нужны права root, чтобы подмонтировать контейнер к папке ФС

В настоящее время мы вступили в эру облачных вычислений. Поэтому все мобильные приложения без поддержки облачного шифрования подобны вымирающим мамонтам. Это касается всех приложений в таблице 19.3, кроме CyberSafe Mobile. Чтобы можно было эту программу сравнить полноценно, нужно подобрать сильных конкурентов. Именно с этой целью на «закуску» я оставил сравнение приложения с Boxcryptor и Cloudfogger Cloud-Encryption. Приложения Boxcryptor и Boxcryptor Classic – по сути одно и то же, но Classic со старым интерфейсом. В Boxcryptor добавлены новые функции и новый интерфейс. Программы до версии 1.5 называются Boxcryptor Classic, а начиная с 1.5 – просто Boxcryptor. В таблице 19.4 приводится сравнение функционала программ облачного шифрования.

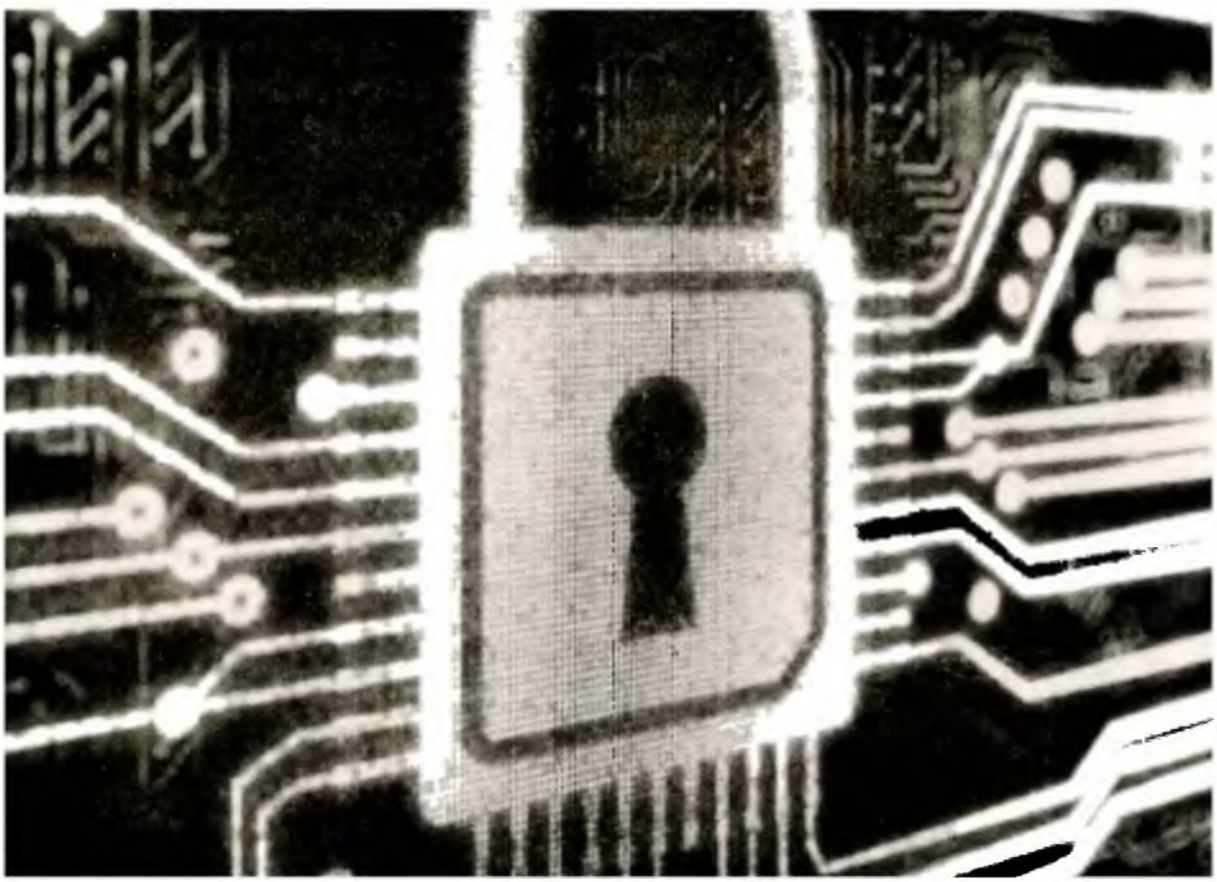
Таблица 19.4. Сравнение приложений облачного шифрования

Функция	CSM	Boxcryptor	Cloudfogger Cloud-Encryption
Хранение файлов в криптоконтейнере	+	-	-
Монтирование контейнера	+	-	-
Синхронизация контейнера с облачным хранилищем (ОХ)	+	-	-
Синхронизация папки с ОХ	+ (*)	+	+
Поддерживаемые ОХ	Google Drive	Google Drive, Яндекс.Диск, Dropbox, OneDrive и др.	Google Drive, Dropbox, OneDrive и др.
Расшаривание файлов	+	+	+
Шифрование папок ОХ	+	+	+
Операции с файлами ОХ	+	+	+
Синхронизация с Windows ПК	+	+	+
Поддерживаемые платформы	Android/Windows	Android/Windows	Android/Windows iOS/MacOS
Доп. преимущества			Сертификат DIN EN ISO 9001:2008

(*) Если сейф подмонтировать к папке, то нужны права root

Преимущества приложений BoxCryptor и CloudFogger в том, что они могут шифровать различные облачные хранилища, а не только Google Drive. CloudFogger можно также использовать на iOS/MacOS, что обеспечивает больший охват аудитории. С другой стороны, ни BoxCryptor, ни CloudFogger не поддерживают криптоконтейнеры, то есть не могут защитить данные на локальном устройстве.

Заключение



В книге были рассмотрены различные способы защиты информации на разных устройствах. Было показано, как защитить электронную почту, данные на жестком диске компьютера и SD-карте мобильного устройства. Надеюсь, что книга вам понравилась.

Уважаемые читатели!

Книги издательства «Наука и Техника»

Вы можете заказать наложенным платежом
в нашем интернет-магазине

www.nit.com.ru,

а также приобрести

в г. Москве:

Т Д «БИБЛИО-ГЛОБУС»	ул. Мясницкая, д. 6/3, стр. 1, ст. М «Лубянка» тел. (495) 781-19-00, 624-46-80
Московский Дом Книги, «ДК на Новом Арбате»	ул.Новый Арбат, 8, ст. М «Арбатская», тел. (495) 789-35-91
Московский Дом Книги, «Дом технической книги»	Ленинский пр., д.40, ст. М «Ленинский пр.», тел. (499) 137-60-19
Московский Дом Книги, «Дом медицинской книги»	Комсомольский пр., д. 25, ст. М «Фрунзенская», тел. (499) 245-39-27
Дом книги «Молодая гвардия»	ул. Б. Полянка, д. 28, стр. 1, ст. М «Полянка» тел. (499) 238-50-01
«Новый книжный» Сеть магазинов	тел. (495) 937-85-81, (499) 177-22-11

в г. Санкт-Петербурге:

Санкт-Петербургский Дом Книги	Невский пр. 28 тел. (812) 448-23-57
Буквоед. Сеть магазинов	тел. (812) 601-0-601

в регионах России:

г. Воронеж, «Амиталь» Сеть магазинов	тел. (473) 224-24-90
г. Екатеринбург, «Дом книги» Сеть магазинов	тел. (343) 289-40-45
г. Нижний Новгород, «Дом книги» Сеть магазинов	тел. (831) 246-22-92
г. Челябинск, «Техническая книга» ул. Монакова, д. 31	тел. (904) 972 50 04
г. Владивосток, «Дом книги» Сеть магазинов	тел. (423) 263-10-54
г. Иркутск, «Продалить» Сеть магазинов	тел. (395) 298-88-82
г. Омск, «Техническая книга» ул. Пушкина, д.101	тел. (381) 230-13-64

Мы рады сотрудничеству с Вами!

Группа подготовки издания:

Зав. редакцией компьютерной литературы: *М. В. Финков*

Редактор: *Е. В. Финков*

Корректор: *А. В. Громова*

ООО «Наука и Техника»

Лицензия №000350 от 23 декабря 1999 года.

198097, г. Санкт-Петербург, ул. Маршала Говорова, д. 29.

Подписано в печать 18.11.2016. Формат 70x100 1/16.

Бумага газетная. Печать офсетная. Объем 17 п. л.

Тираж 1400. Заказ 9391.

Отпечатано с готовых файлов заказчика

в АО «Первая Образцовая типография»

филиал «УЛЬЯНОВСКИЙ ДОМ ПЕЧАТИ»

432980, г. Ульяновск, ул. Гончарова, 14.

Камский В. А.

Защита личной информации

в Интернете, смартфоне и компьютере

По статистике большинство пользователей персональных компьютеров и Интернета сами позволяют похищать/использовать свои личные данные злоумышленникам или просто подкованным в техническом плане третьим лицам. И ущерб от таких противоправных действий колеблется от незначительного до катастрофического. Никто не поможет лучше всего защитить ваши данные чем … вы Сами!

И эта книга вам в этом поможет. Простым и понятным языком здесь рассказано как эффективно защитить свою электронную почту, какими способами лучше воспользоваться для этой цели, а также приведены примеры взлома электронной почты. Вы узнаете как стать анонимным в Интернете, чтобы вас не беспокоили назойливые правила форумов, как защититься от вирусов в Интернете, что такое проект Tor и VPN-анонимайзер.

Пользователям Android-устройств (сотовых телефонов, смартфоны, планшеты) будет полезно прочитать, как защитить свои личные данные на своем портативном устройстве, что такое криптоконтейнер и как пользоваться защитой от прослушки.

Для пользователей персональных компьютеров будет важно узнать, что такое шифрование вашего жесткого диска, какими программами лучше для этого пользоваться, как защитить свои данные средствами вашей операционной системы, как защитить свою домашнюю сеть от нежданных гостей или назойливых соседей и многое другое.
Книга будет полезна всем, кто хочет быть спокойным за свои данные всегда и везде!

www.nit.com.ru

ISBN 978-5-94387-731-5

9 78- 5- 94387- 731- 5

НиТ издательство

Россия: Санкт-Петербург,
пр Обуховской обороны 107
для писем: 192029 Санкт-Петербург а/я 44
(812) 412 7025, 412 7026
e-mail: nit@mail.wplus.net

Украина: 02166, Киев, ул Курчатова, 9 21
(044) 516 3866
e-mail: nits@voliacable com