

Денис Колисниченко



**Секреты**

**безопасности и анонимности  
в Интернете**

**ЮСТИ И Э  
В ТЕ**

Денис Колисниченко

# **Секреты**

## **безопасности и анонимности в Интернете**

Санкт-Петербург

«БХВ-Петербург»

2021



УДК 004.738.5+004.056  
ББК 32.973.26-018.2  
К60

**Колисниченко Д. Н.**

**К60      Секреты безопасности и анонимности в Интернете. — СПб.:  
БХВ-Петербург, 2021. — 256 с.: ил.**

**ISBN 978-5-9775-6605-6**

Даже новички знают, что вычислить любого пользователя в Интернете совсем несложно. Книга рассказывает, как скрыть свое местонахождение и IP-адрес, используя анонимные сервисы и сеть Tor, посетить заблокированные администратором сайты, защитить личную переписку, домашние устройства и беспроводную сеть. Рассматриваются способы предотвратить утечку персональных данных, обеспечить безопасность мобильных устройств под управлением Android. Особое внимание уделено вопросам конфиденциальности в социальных сетях и личной переписки. В книге рассматриваются самые актуальные технологии информационной безопасности и современные версии программ.

*Для широкого круга пользователей*

УДК 004.738.5+004.056  
ББК 32.973.26-018.2

#### **Группа подготовки издания:**

Руководитель проекта	<i>Павел Шалин</i>
Зав. редакцией	<i>Екатерина Сависте</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн обложки	<i>Карины Соловьевой</i>

Подписано в печать 07.07.20.  
Формат 70×100<sup>1/8</sup>. Печать офсетная. Усл. печ. л. 20,64.  
Тираж 1000 экз. Заказ №11502.  
"БХВ-Петербург", 191038, Санкт-Петербург, Гончарная ул., 20.  
Отпечатано с готового оригинал-макета  
ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-6605-6

© ООО "БХВ", 2021  
© Оформление. ООО "БХВ-Петербург", 2021

# Оглавление

<b>Введение .....</b>	<b>9</b>
<b>Глава 1. Как стать анонимным в Интернете?.....</b>	<b>11</b>
1.1. Анонимность и вы .....	11
1.2. Анонимайзеры: сокрытие IP-адреса.....	12
1.3. Анонимные прокси-серверы: сокрытие IP-адреса и местонахождения.....	15
1.3.1. Прокси-сервер — что это? .....	15
1.3.2. Настраиваем анонимный прокси-сервер .....	16
1.3.3. Достоинства и недостатки анонимных прокси-серверов .....	21
1.4. Локальная анонимность .....	21
1.5. Отключение слежки Windows 10.....	25
1.6. Что еще нужно знать об анонимности в Интернете?.....	28
1.7. Анонимность и закон .....	29
<b>Глава 2. Тог: замечаем следы. Как просто и эффективно скрыть свой IP-адрес .....</b>	<b>33</b>
2.1. Как работает Тог? Заходим в «Одноклассники» с работы .....	33
2.2. Тог или анонимные прокси-серверы и анонимайзеры. Кто кого?.....	36
2.3. Критика Тог и скандалы вокруг этой сети.....	37
2.4. Установка и использование Тог .....	38
2.4.1. Быстро, просто и портательно: Тог на флешке .....	38
2.4.2. Настройка почтового клиента Mozilla Thunderbird .....	44
2.4.3. Настройка программы интернет-телефонии Skype.....	47
Воспользоваться VPN-сервисами .....	47
Настроить браузер Chrome для работы через Тог.....	48
2.4.4. Настройка браузера Opera.....	50
2.4.5. Настройка FTP-клиента FileZilla .....	51
2.5. Когда Тог бессильна. Дополнительные расширения для Firefox.....	52
2.6. Ограничения и недостатки сети Тог.....	52
2.7. Этика использования сети Тог.....	53
<b>Глава 3. Что такое VPN и «с чем его едят»? Защита передаваемых по сети данных от прослушивания .....</b>	<b>55</b>
3.1. Зачем нужен VPN?.....	55

3.2. Выбор VPN-сервиса .....	56
3.2.1. VPN Shield .....	56
3.2.2. IPVanish VPN .....	57
3.2.3. HideMyAss (HMA) .....	58
3.2.4. Private Internet Access .....	58
3.2.5. StrongVPN .....	59
3.2.6. ExpressVPN .....	60
3.2.7. SecurityKISS .....	60
3.3. Организация VPN-соединения .....	61
3.4. Opera VPN: осторожно! .....	63
3.5. Что лучше: VPN или Tor? .....	64

## **Глава 4. Воображаемая безопасность: выбираем безопасный мессенджер..... 67**

4.1. Критерии оценки .....	67
4.2. Мессенджеры .....	70
4.2.1. Telegram .....	70
4.2.2. Signal .....	72
4.2.3. Viber .....	73
4.2.4. WhatsApp .....	74
4.2.5. Briar .....	75
4.2.6. ТамТам .....	76
4.2.7. VK (ВКонтакте) .....	76
4.2.8. Facebook Messenger .....	76
4.2.9. Wire .....	77
4.2.10. Jabber .....	77
4.2.11. Riot Matrix .....	78
4.2.12. Status .....	78
4.2.13. Threema .....	80
4.3. Заключение .....	81

## **Глава 5. Анонимность в социальной сети..... 83**

5.1. Нужна ли вам анонимность? .....	83
5.2. Зачем нужна анонимность в социальной сети? .....	84
5.3. Обеспечение анонимности .....	84

## **Глава 6. Способы взлома и защиты электронной почты..... 89**

6.1. Способы взлома почтового ящика .....	89
6.1.1. Троянский конь .....	89
6.1.2. Взлом по номеру телефона .....	93
6.1.3. Физический доступ к компьютеру .....	94
Кейлоггер .....	94
Программы для «восстановления» паролей почтовых учетных записей .....	95
6.1.4. Социальная инженерия, или просто обман .....	96
6.1.5. Модное слово «фишинг» .....	97
6.1.6. «Вспоминаем» пароль .....	101
6.1.7. Кража Cookies .....	101
6.1.8. XSS-уязвимости .....	101
6.1.9. Метод грубой силы .....	103
6.2. Защита почтового ящика .....	103



6.3. Шифрование электронной почты .....	105
6.3.1. Немного теории: S/MIME, PKI и PGP .....	105
6.3.2. Как будем защищать почту? .....	107
6.3.3. Использование OpenSSL .....	107
6.4. Настройка почтовых клиентов на шифрование .....	112
6.4.1. Настройка Microsoft Outlook .....	112
6.4.2. Настройка Mozilla Thunderbird .....	118
<b>Глава 7. Шифрование данных .....</b>	<b>121</b>
7.1. Выбор средства защиты данных .....	121
7.1.1. Шифрование всего диска .....	121
7.1.2. Шифрование одного из разделов диска .....	122
7.1.3. Криптоконтейнеры, или виртуальные диски .....	125
7.1.4. Прозрачное шифрование .....	126
7.2. Шифрование стандартными средствами операционной системы .....	127
7.2.1. Прозрачное шифрование с помощью EFS .....	127
Преимущества и недостатки EFS .....	127
Шифрование с помощью EFS .....	129
7.2.2. Шифрование диска с помощью BitLocker .....	130
Что такое BitLocker? .....	130
Что можно зашифровать, а что — нет? .....	131
Шифруем диск с помощью BitLocker .....	131
Работа с зашифрованным BitLocker диском .....	136
7.2.3. Файловая система eCryptfs в Linux .....	140
Шифрование папки .....	140
Храним пароль на флешке .....	142
7.2.4. Можно ли доверять стандартному шифрованию? .....	143
7.3. Сторонние программные продукты .....	144
7.3.1. Выбор сторонней программы для шифрования .....	144
7.3.2. История TrueCrypt, и что случилось с проектом .....	144
7.3.3. Использование TrueCrypt .....	146
Установка программы .....	146
Создание виртуального диска .....	148
Шифрование раздела .....	156
7.3.4. Программа VeraCrypt .....	160
7.3.5. Программа CipherShed .....	162
7.3.6. Шифрование файла для передачи .....	162
7.3.7. Производительность зашифрованных дисков .....	163
7.4. Скрытие файлов .....	165
7.5. Шифрование данных на предприятиях .....	167
<b>Глава 8. Безопасность устройств на ОС Android .....</b>	<b>171</b>
8.1. Включение кода разблокировки устройства .....	171
8.2. Отказ от установки приложений из неизвестных источников .....	171
8.3. Осторожно: неизвестные сети Wi-Fi! Шифруем передаваемые данные .....	172
8.4. Анонимность в Android: установите Tor .....	174
8.5. Блокируем запуск приложений .....	176
8.6. Шифрование данных в Android .....	178
8.6.1. Шифрование стандартными средствами .....	178

8.6.2. Сторонние программы шифрования .....	179
Программа LUKS Manager .....	179
Программа EDS Lite .....	179
8.7. Шифруем почту .....	184
8.7.1. Необходимые приложения .....	184
8.7.2. Настройка Crypto Plugin .....	184
8.7.3. Настройка MailDroid .....	186
8.7.4. Последний шаг .....	188
8.8. Отключение GPS-модуля .....	189
<b>Глава 9. Устраняем утечки информации .....</b>	<b>191</b>
9.1. Чем грозит утечка персональных данных? .....	191
9.2. Как придумать надежный пароль? Критерии надежности. Генераторы паролей .....	194
9.2.1. Выбор хорошего пароля .....	194
9.2.2. Генераторы паролей .....	196
9.3. Как сохранить пароль? Менеджеры паролей .....	197
9.4. Секретные вопросы .....	199
9.5. Двухфакторная аутентификация .....	199
9.6. Авторизация с помощью биометрических данных .....	200
9.7. Заметаем следы правильно .....	202
9.7.1. Очистка списков недавних мест и программ .....	202
9.7.2. Очистка списка USB-накопителей .....	207
9.7.3. Очистка кэша и истории браузеров .....	210
9.7.4. Удаляем записи DNS .....	213
9.7.5. Очистка Flash Cookies .....	213
9.7.6. Удаление списка последних документов MS Office .....	213
9.7.7. Автоматизируем очистку с помощью CCleaner .....	215
9.7.8. Реальное удаление файлов .....	216
9.7.9. Создаем bat-файл для очистки всего .....	217
9.7.10. Создаем AutoHotkey-скрипт для очистки всего .....	218
<b>Глава 10. Мой дом — моя крепость: безопасность домашних устройств .....</b>	<b>219</b>
10.1. Стоит ли защищать домашнюю сеть? .....	219
10.2. Защита маршрутизатора .....	221
10.2.1. Изменение пароля доступа к маршрутизатору .....	221
10.2.2. Изменение имени сети (SSID). Соккрытие SSID .....	223
10.2.3. Отключения гостевой сети .....	223
10.2.4. Изменение IP-адреса маршрутизатора .....	225
10.2.5. Используйте WPA или WPA2 .....	225
10.2.6. Фильтрация MAC-адресов .....	226
10.2.7. Понижение мощности передачи .....	227
10.3. Защита веб-камеры и микрофона .....	229
10.4. Защита принтера .....	231
<b>Глава 11. Безвозвратное удаление данных .....</b>	<b>233</b>
11.1. Уничтожение информации на жестком диске .....	234
11.2. Приложения для безопасного удаления данных с жестких дисков .....	235
11.3. Удаление информации с SSD .....	236

<b>Глава 12. Ошибки, ведущие к утрате анонимности .....</b>	<b>241</b>
12.1. Как не совершать ошибок? .....	241
12.2. Как не попасть под лингвистический анализ? .....	242
12.3. Наиболее частые ошибки .....	244
<b>Глава 13. Программы с «сюрпризами» и без.....</b>	<b>245</b>
13.1. Программы с открытым кодом.....	245
13.2. Выбор программ .....	246
13.2.1. Выбор браузера.....	247
13.2.2. Выбор почтового клиента.....	250
13.2.3. Программы для загрузки файлов и FTP-клиенты .....	250
13.3. Плагины .....	252
<b>Заключение.....</b>	<b>254</b>
<b>Предметный указатель .....</b>	<b>255</b>





# Введение

Стремление государства и некоторых коммерческих структур знать все о каждом человеке в последнее время начинает откровенно раздражать. Как правило, все прикрываются благородными целями: борьбой с мошенничеством, терроризмом и т. п. Известно, однако, что благими намерениями вымощена дорога в ад.

Изначально Интернет был «территорией свободы» — единственным, пожалуй, местом с полной свободой слова, где каждый имел право высказать свое мнение. Сейчас же технический прогресс работает против этой самой свободы: опубликовал заметку в своем блоге или в социальной сети — и жди звонка в дверь... Были случаи судебных разбирательств даже за репост записи, не только за ее публикацию. Так что тема «как не сесть за репост» становится весьма актуальной.

Впрочем, законопослушным пользователям, может, и нечего бояться. Если забыть о свободе слова, конечно. Броди по Интернету, читай анекдоты, смотри фильмы. Но знай, что за каждым твоим шагом — наблюдают. И осознание этой истины реально бесит. В конце концов, у каждого есть право на тайну переписки и личной жизни. И реализовать его вам поможет эта книга, как раз и посвященная анонимной и безопасной (во всех смыслах этого слова) работе в Интернете.

В *первых трех главах* вы узнаете, как скрыть свой IP-адрес, как посетить сайт, заблокированный администратором сети, как зашифровать передаваемые по Сети данные, а также познакомитесь с двумя системами анонимизации трафика: Tor и VPN.

В *четвертой главе* мы поговорим о выборе безопасного мессенджера. Как оказалось, популярные мессенджеры не совсем безопасные. Но не будем забегать вперед.

*Пятая глава* расскажет, как оставаться анонимным в социальных сетях, хотя это не всегда просто.

В *шестой главе* мы поговорим о защите электронной почты. Вы узнаете, как зашифровать свои сообщения, чтобы даже после взлома вашего почтового ящика никто не смог бы прочитать ваши письма.

*Глава 7* посвящена шифрованию информации на жестком диске. Мы разберемся, какую информацию нужно шифровать, и какие программы для этого лучше использовать.

Мобильные устройства на базе Android стали неотъемлемой частью жизни практически каждого человека. От кнопочных телефонов в силу их не очень широкого функционала давно отказались, устройства с iOS есть не у всех, а вот Android — это золотая середина: и функционально, и недорого. Поэтому обойти стороной безопасность устройств на Android было бы нельзя. Вопросы защиты таких устройств и описаны в *главе 8*.

Одна из методик защиты данных — поиск и устранения утечек информации. Об этом мы поговорим в *главе 9*.

*Десятая глава* расскажет о том, как защитить свою домашнюю сеть. А в *главе 11* мы рассмотрим процесс надежного удаления данных — чтобы их невозможно было восстановить.

Последние две главы: *12-я* и *13-я* — не менее интересные, чем предыдущие. Они помогут вам не рассекретить самого себя и подскажут, какие программы лучше всего использовать, если вы желаете остаться анонимным.

Знаю, что читатели не любят длинных введений и часто таковые игнорируют. Поэтому сейчас самое время перейти к чтению книги.



# ГЛАВА 1



## Как стать анонимным в Интернете?

### 1.1. Анонимность и вы

В последнее время Интернет становится все менее анонимным. С одной стороны — всевозможные ресурсы и вредоносные программы, собирающие различную информацию о пользователе: IP-адрес, имя, пол, возраст, место жительства, номер телефона. Такая информация может собираться как явно (вы ее сами указываете, заполняя на посещаемых сайтах различные формы-вопросники), так и неявно, когда она определяется на основании косвенных данных (например, ваше местонахождение при посещении того или иного сайта легко вычисляется по IP-адресу компьютера, с которого вы зашли в Интернет). Вся эта информация может собираться различными сайтами, например для показа вам рекламных объявлений, привязанных к вашему месту жительства, или в любых других целях. С другой стороны — силовые органы с оборудованием СОПМ (система оперативно-розыскных мероприятий), которое внедряется уже много лет.

Зачем нужна анонимность в Интернете обычному законопослушному пользователю?

#### **ПРИМЕЧАНИЕ**

В побуждения незаконнопослушных мы здесь углубляться не станем...

Причины у всех свои, но от них зависят способы достижения цели. В табл. 1.1 приводятся несколько типичных задач, которые рано или поздно приходится решать каждому интернет-пользователю.

Понимаю, что приведенные здесь способы решения поставленной задачи вам пока не ясны. Что ж, самое время разобраться со всеми этими заумными названиями: анонимайзеры, анонимные прокси-серверы, распределенные сети...

Таблица 1.1. Причины сохранения анонимности в Интернете

Задача	Зачем?	Способы решения
Нужно разово скрыть свой IP-адрес	Вы просто не хотите, чтобы ваш IP-адрес «записал» сайт, который вы собираетесь посетить. Вторая причина — ради эксперимента. Например, вы создали свой сайт, установили на нем счетчик и теперь хотите проверить, работает он или нет. Если на сайт вы заходите со своего IP-адреса (сайту известного), значение счетчика останется неизменным. Когда же вы зайдете с использованием IP-адреса скрытого (т. е. «чужого»), значение счетчика будет увеличено. Значит, все работает как надо	Анонимные прокси-серверы Анонимайзеры
«Смена жительства»	Некоторые сайты разрешают доступ, если ваш IP-адрес относится к определенной стране. Пользователям других стран доступ на сайт запрещен	Анонимные прокси-серверы Распределенная сеть Tor
Постоянное анонимное посещение сайтов	Вероятно, вы или скрывающийся блоггер (в последнее время — это популярный род деятельности), или же просто не хотите, чтобы администратор (вашей офисной сети или сети провайдера) узнал, какие сайты вы посещаете	Распределенная сеть Tor Проект I2P
Нужно скрыть посещенные сайты от глаз коллег и родственников	У вас нет паранойи и вам все равно, следят ли за вами администратор, но вы просто не хотите, чтобы ваши родственники или коллеги узнали, на каких сайтах вы бываете	Не нужно никаких специальных средств, достаточно правильно очистить историю браузера или использовать режим приватного просмотра браузера Firefox. Об этом мы поговорим далее в этой главе
Нужно посетить заблокированный администратором сайт	«Злой» администратор закрыл доступ к «Одноклассникам» или «ВКонтакте»? Решение, как всегда, есть!	Распределенная сеть Tor
Зашифровать всю передаваемую вами информацию	Иногда анонимного посещения сайтов мало, важно, чтобы никто не узнал, какую информацию вы передавали этим сайтам (например, какие анкетные данные указывали)	Распределенная сеть Tor

## 1.2. Анонимайзеры: сокрытие IP-адреса

Представим, что вы собрались разово скрыть свой IP-адрес. Зачем это вам, мне дела нет. Снимаю с себя всякую ответственность, если ваши цели идут вразрез с существующим законодательством. Все мы помним, что Раскольников сделал с помощью топора, однако холодным оружием топор не считается...

### Из личного опыта...

В свое время анонимайзер помог мне в весьма неординарной ситуации. Известно, что пакеты, исходящие от нашего компьютера к компьютеру назначения (веб-серверу сайта, который мы хотим посетить), отправляются не напрямую, а проходят по определенному маршруту через некоторое количество маршрутизаторов. Так вот, один маршрутизатор на пути от моего компьютера к моему же сайту вышел из строя. В результате я не мог зайти на свой сайт, хотя он был вполне доступен, и на него могли зайти пользователи других провайдеров, пакеты которых проходили по иным маршрутам. Ждать пока маршрутизатор восстановят мне, разумеется, не хотелось, поэтому я и воспользовался анонимайзером — чтобы, во-первых, убедиться в доступности сайта, а во-вторых, посмотреть, что же на нем творится.

Итак, что же представляет собой *анонимайзер* (anonymizer)? Это такой сайт в Интернете. Вы на него заходите, вводите в специальное поле адрес сайта, который хотите посетить анонимно, и вуаля — вы на сайте, но сайт записал в свои протоколы не ваш IP-адрес, а адрес анонимайзера. При переходе по ссылке также фиксируется IP-адрес анонимайзера — до тех пор, пока вы не закрыли окно (или вкладку) браузера, в котором изначально был открыт анонимайзер. Весьма удобно, а главное — просто.

Найти подходящий анонимайзер несложно — введите в Google запрос анонимайзер (или anonymizer), и будет найдено множество сайтов, предоставляющих такие услуги. Некоторые из них — бесплатные (они содержатся за счет размещаемой рекламы, которую вы вынуждены просматривать, пользуясь анонимайзером), за использование других придется заплатить.

Платный или бесплатный? Если вам просто надо анонимно посетить пару страничек, выбирайте бесплатный анонимайзер. А вот если вы хотите не просто посетить некий сайт, а еще и скачать оттуда какую-либо информацию, лучше выбрать платный. Дело в том, что бесплатные анонимайзеры часто ограничивают максимальный размер загружаемого объекта, — порой вам дадут скачать лишь 1–2 мегабайта, что по современным меркам откровенно мало. А вот платные разрешают скачивать файлы в несколько десятков и сотен мегабайт. Кроме того, некоторые платные анонимайзеры разрешают выбрать IP-адрес из диапазона адресов определенной страны (по выбору), что иногда полезно (см. табл. 1.1).

К достоинствам анонимайзеров можно отнести:

- ☐ удобство и простоту использования — вам не понадобится устанавливать дополнительное программное обеспечение, не придется вносить изменения в параметры браузера или системы. Просто открыли сайт анонимайзера, ввели нужный интернет-адрес, и ваш IP-адрес скрыт;
- ☐ возможность блокировки баннеров — некоторые анонимайзеры для уменьшения количества ненужной информации, пропускаемой через их сервер, блокируют рекламные баннеры. Иногда эта функция становится доступной только после оплаты. К сожалению, большинство бесплатных анонимайзеров только добавляют свою дополнительную рекламу...

А вот недостатков у анонимайзеров очень много:

- ☐ не выполняется шифрование передаваемых данных — да, с помощью анонимайзера вы можете скрыть свой IP-адрес — посещаемый вами сайт «запомнит»



IP-адрес анонимайзера, но не ваш. Но от всевидящего ока администратора вашего офиса (или вашего интернет-провайдера) вам не скрыться. Он не только сможет легко вычислить, какие сайты вы посещали, но и при желании перехватит передаваемую информацию (например, анкетные данные, которые вы оставляли на сайте). Так что анонимайзеры не обеспечивают полной анонимности;

- ❑ не всегда можно выбрать IP-адрес нужной страны — предположим, что анонимайзер находится в США. И если вы попытаетесь с его помощью зайти на сайт, который разрешает доступ пользователям только, скажем, из Германии, то у вас ничего не получится — ведь IP-адрес будет американский. Ради справедливости нужно отметить, что некоторые анонимайзеры предлагают выбрать IP-адрес нужной страны, но это больше исключение, чем правило, да и не факт, что нужная вам страна окажется в списке;
- ❑ не всегда скорость анонимного доступа будет высокой — тут все зависит от загрузки сервера анонимайзера и от того, как быстро пакеты от вашего компьютера передаются на сервер анонимайзера (т. е. важна скорость передачи данных между вашим компьютером и сервером анонимайзера). Впрочем, все средства обеспечения анонимности снижают скорость соединения, и вы должны быть к этому готовы;
- ❑ ограничение размера перекачиваемых файлов — об этом мы уже говорили, поэтому не вижу смысла повторяться, — не следует надеяться, что вы скачаете через анонимайзер пиратский фильм объемом в несколько гигабайт;
- ❑ нет гарантий приватности — никто не гарантирует, что анонимайзеры (а их огромное количество) не записывают адреса сайтов, которые вы посещаете, и не передают потом заинтересованным лицам...

Подытоживая отметим: анонимайзеры подойдут для сокрытия вашего IP-адреса — удаленный сайт не сможет его определить. Но для обеспечения полной анонимности они не подходят — администраторы смогут вычислить, какие сайты вы посещали, и даже посмотреть, какие данные вы передавали этим сайтам (поскольку анонимайзеры не производят шифрование данных).

Как администратор вычислит сайты, которые вы посещали? Очень просто. Анонимайзер перезаписывает все ссылки сайта, которые вы хотите посетить, добавляя в их начало свой адрес (чтобы ссылка была открыта не напрямую, а через анонимайзер). Допустим, я зашел на популярный анонимайзер [anonymouse.org](http://anonymouse.org), а через него — на сайт [www.bhv.ru](http://www.bhv.ru). И в адресной строке браузера увидел следующий адрес: <http://anonymouse.org/cgi-bin/anon-www.cgi/http://www.bhv.ru> (рис. 1.1).

Эта же строка попадет в журналы администратора вашей сети. Как видите, вычислить, какие сайты вы посещали, не составляет никакого труда. Более того, по таким ссылкам администратор узнает, какие сайты вы посещали анонимно, и поймет, что к этим сайтам у вас есть повышенный интерес. Поверьте, ему будет о чем рассказать вашему начальству...

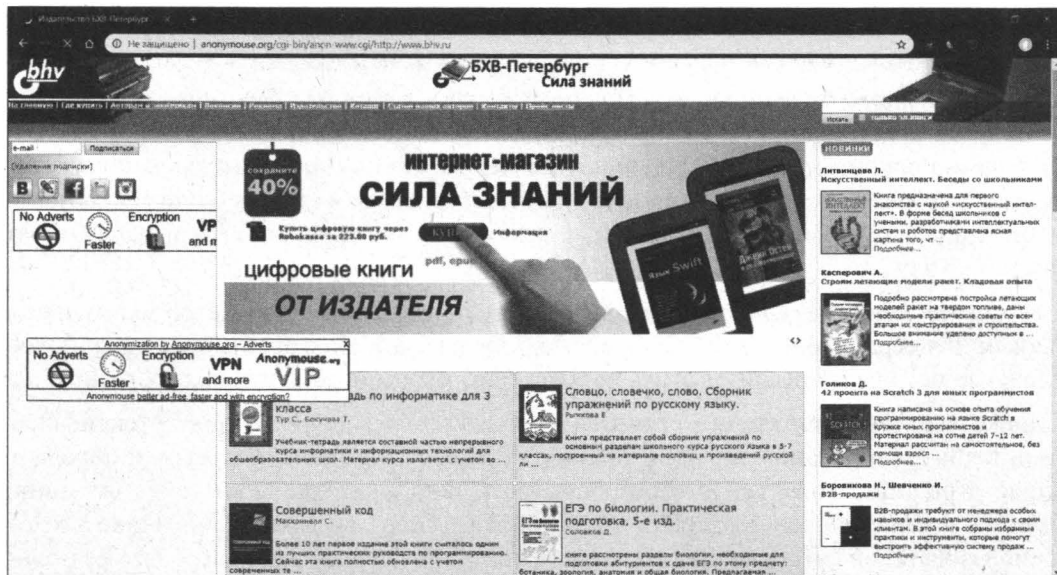


Рис. 1.1. Просмотр сайта через **anonymouse.org**:  
анонимайзер еще и добавил большой рекламный баннер

## 1.3. Анонимные прокси-серверы: сокрытие IP-адреса и местонахождения

С помощью анонимайзера скрывается не только ваш IP-адрес, но и ваше местонахождение, определяемое по IP-адресу. Но иногда нужно скрыть местонахождение более гибко, а именно — получить IP-адрес определенной страны. Как правило, к таким мерам прибегают пользователи, которым нужно посетить ограничиваемые сайты.

### Из личного опыта...

Нет, никаких мыслей о взломе! Такая операция иногда бывает необходимой самым законопослушным пользователям. В 2009 году я столкнулся с анекдотической ситуацией. Крупнейший украинский провайдер «Укртелеком» использовал IP-адреса из диапазона лондонского провайдера. В результате, когда пользователи «Укртелекома» заходили на украинские сайты, их системы статистики считали, что пользователь пришел из Великобритании. А некоторые наши особо патриотические сайты ограничивают доступ всех зарубежных пользователей. Ну надо же — купил Интернет у крупнейшего национального провайдера, а вся страна считает тебя чужаком. Как сейчас обстоят дела у «Укртелекома» не интересовался, но в то время ситуация была вполне реальной.

Выбрать IP-адрес нужной страны проживания можно с помощью анонимных *прокси-серверов*. Однако прежде, чем разбираться с анонимными прокси-серверами, поговорим сначала об прокси-серверах обычных.

### 1.3.1. Прокси-сервер — что это?

Итак, что такое прокси-сервер? Это узел сети, служащий для кэширования информации и ограничения доступа в сеть. Прокси-серверы устанавливаются как адми-

нистраторами локальной сети для нужд ее самой, так и провайдерами Интернета для нужд всех их клиентов.

Имя или IP-адрес прокси-сервера можно занести в настройки браузера. В результате браузер будет обращаться к какому-либо узлу сети не напрямую, а через указанный вами прокси-сервер (т. е. запрос будет передаваться сначала на прокси-сервер). А прокси-сервер уже может запросить имя пользователя и пароль (если такое поведение задал администратор прокси) и только потом предоставить пользователю доступ к узлу.

Некоторые ленивые администраторы самодельных локальных сетей применяют прокси для ограничения доступа своих пользователей к Интернету, поскольку более сложные методы им реализовывать неохота (или экономически нецелесообразно).

Однако большинство прокси-серверов используются все же не для аутентификации, а для кэширования страниц. Браузер обращается к прокси-серверу и передает адрес страницы, которую хочет просмотреть пользователь. Если такая страница имеется в кэше прокси-сервера (а это возможно, если эту страницу недавно кто-то из пользователей сети уже просматривал), то прокси-сервер сразу передает ее пользователю. В результате обращение к удаленному узлу даже не производится, что снижает нагрузку на интернет-канал, экономит деньги, ресурсы удаленного узла и повышает скорость доступа к Интернету. Одно дело передать данные по локальной сети, где скорость соединения доходит до 1000 Мбит/с (в случае с Gigabit Ethernet), другое дело — передать данные по интернет-каналу, где скорость доступа порой ниже 5 Мбит/с.

Дальнейшее развитие прокси-серверов — *прозрачные прокси-серверы*. Суть их заключается в том, что весь веб-трафик с помощью правил брандмауэра сети перенаправляется на прокси-сервер, в результате чего ускоряется доступ к прокэшированным страницам и устраняется необходимость настраивать отдельно каждый клиентский компьютер (точнее, каждый браузер на каждом клиентском компьютере).

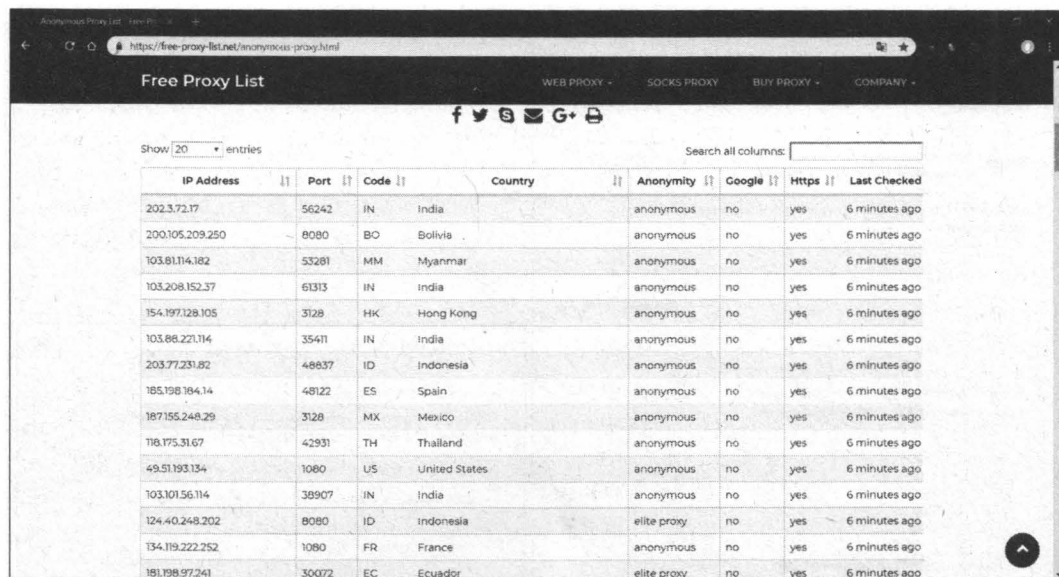
### 1.3.2. Настраиваем анонимный прокси-сервер

Теперь вернемся к рассмотрению *анонимных прокси-серверов*. Как правило, анонимный прокси-сервер — это обычный прокси-сервер, но неправильно настроенный. Администраторы таких серверов забывают запретить доступ к своему серверу чужим узлам. Впрочем, есть и публичные (открытые) прокси, которые намеренно разрешают доступ всем желающим.

Для обеспечения анонимности вам нужно просто указать IP-адрес такого прокси-сервера в настройках браузера.

Где достать адрес анонимного прокси? Списки таких адресов публикуются на различных ресурсах — например, на <https://free-proxy-list.net/anonymous-proxy.html>. Здесь вы найдете IP-адреса прокси-серверов из разных стран (рис. 1.2). Дополнительные IP-адреса можно найти по запросу Free proxy. Вот еще один полезный сайт: <http://spys.ru/aproxy/>.

Найдя заветный IP-адрес, пропишите его в настройках браузера.



The screenshot shows a web browser displaying the 'Free Proxy List' website. The page has a dark header with navigation links: WEB PROXY, SOCKS PROXY, BUY PROXY, and COMPANY. Below the header is a search bar and a table of proxy servers. The table has columns for IP Address, Port, Code, Country, Anonymity, Google, Https, and Last Checked. The table lists 18 proxy servers from various countries, including India, Bolivia, Myanmar, Hong Kong, Indonesia, Spain, Mexico, Thailand, United States, and Ecuador. Most are marked as 'anonymous' and 'yes' for Https.

IP Address	Port	Code	Country	Anonymity	Google	Https	Last Checked
202.3.72.17	56242	IN	India	anonymous	no	yes	6 minutes ago
200.105.209.250	8080	BO	Bolivia	anonymous	no	yes	6 minutes ago
103.81.114.182	53281	MM	Myanmar	anonymous	no	yes	6 minutes ago
103.208.152.37	61313	IN	India	anonymous	no	yes	6 minutes ago
154.197.128.105	3128	HK	Hong Kong	anonymous	no	yes	6 minutes ago
103.88.221.114	35411	IN	India	anonymous	no	yes	6 minutes ago
203.77.231.82	48837	ID	Indonesia	anonymous	no	yes	6 minutes ago
185.198.184.14	48122	ES	Spain	anonymous	no	yes	6 minutes ago
187.155.248.29	3128	MX	Mexico	anonymous	no	yes	6 minutes ago
118.175.31.67	42931	TH	Thailand	anonymous	no	yes	6 minutes ago
49.51.193.134	1080	US	United States	anonymous	no	yes	6 minutes ago
103.101.56.114	38907	IN	India	anonymous	no	yes	6 minutes ago
124.40.248.202	8080	ID	Indonesia	elite proxy	no	yes	6 minutes ago
134.119.222.252	1080	FR	France	anonymous	no	yes	6 minutes ago
181.198.97.241	30072	EC	Ecuador	elite proxy	no	yes	6 minutes ago

Рис. 1.2. Списки анонимных прокси-серверов

Если вы еще пользуетесь браузером Internet Explorer (IE), для этого нужно выполнить следующие действия:

1. Выберите команду меню **Свойства обозревателя**.
2. Перейдите на вкладку **Подключения** (рис. 1.3).
3. Нажмите кнопку **Настройка сети**. В открывшемся окне (рис. 1.4) установите флажок **Использовать прокси-сервер для локальных подключений** (не применяется для коммутируемых или VPN-подключений).
4. Введите в соответствующие поля IP-адрес прокси-сервера и его порт. Обычно порт указывается в списке прокси-серверов в отдельной колонке или через двоеточие, например, так: 192.168.2.100:3128 (здесь 3128 — номер порта). Стандартные номера портов для прокси: 80, 3128, 8080.

На рис. 1.4 браузер настроен на локальный прокси-сервер сети Tor: IP-адрес 127.0.0.1 и порт 9150. Об этом мы еще поговорим, когда будем рассматривать распределенную сеть Tor (см. главу 2).

5. Чтобы установить для различных сетевых ресурсов (HTTP, FTP и т. п.) разные прокси-серверы, нажмите кнопку **Дополнительно** и введите соответствующие адреса (рис. 1.5).

Браузеры Microsoft Edge, Google Chrome и Opera используют те же параметры прокси, что и Internet Explorer, — они попадают в системные настройки. Другими словами, определив прокси-сервер, как показано здесь для Internet Explorer, вы установите его для всех четырех браузеров: IE, Edge, Chrome и Opera, разве что последовательность действий будет для каждого браузера своя.

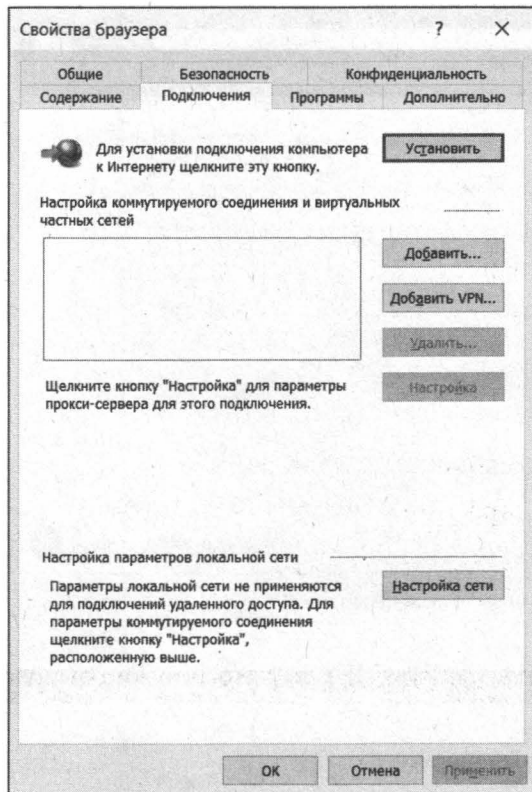


Рис. 1.3. Свойства браузера Internet Explorer: вкладка Подключения

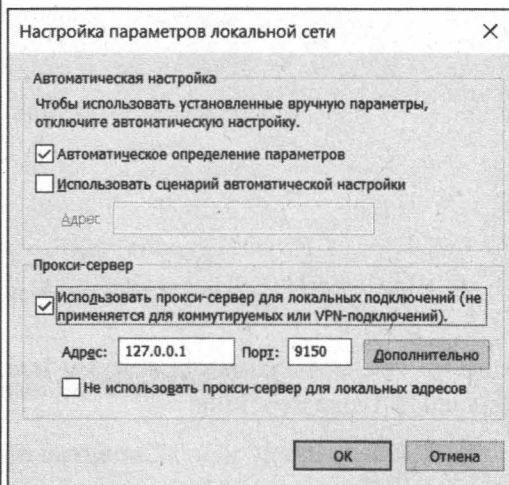


Рис. 1.4. Окно настройки параметров локальной сети браузера Internet Explorer

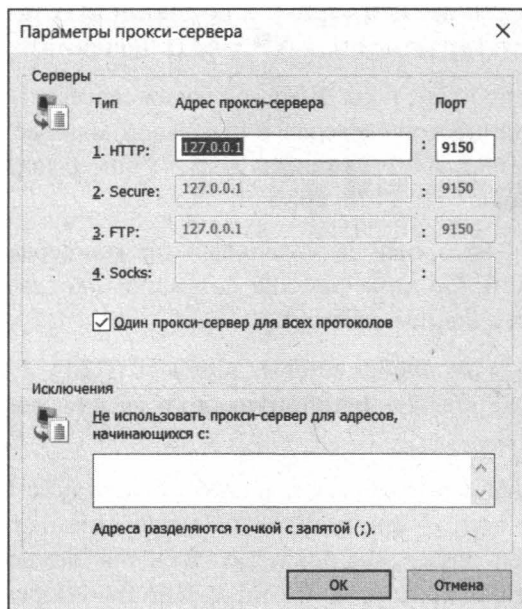



Рис. 1.5. Окно параметров прокси-сервера браузера Internet Explorer

Так, если вам удобно открыть окно параметров прокси через Google Chrome, то выполните следующие действия:

1. Нажмите кнопку вызова меню — три вертикальные точки в правом верхнем углу окна браузера .
2. В открывшемся окне выберите команду **Настройки**.
3. Перейдите в раздел **Дополнительные | Система** и в открывшейся панели нажмите кнопку **Настройки прокси-сервера**.
4. Откроется уже знакомое окно (см. рис. 1.3) параметров браузера IE (браузер Google Chrome использует некоторые настройки IE). Дальнейшая последовательность действий такая же, как и для IE.

Если вы предпочитаете браузер Mozilla Firefox:

1. Выберите команду меню **Firefox | Настройки**.
2. Прокрутите открывшуюся страницу настроек до конца (рис. 1.6).
3. Нажмите кнопку **Настроить**. В открывшемся окне (рис. 1.7) выберите **Ручная настройка прокси** и введите в поле **HTTP прокси** IP-адрес прокси-сервера и его порт.

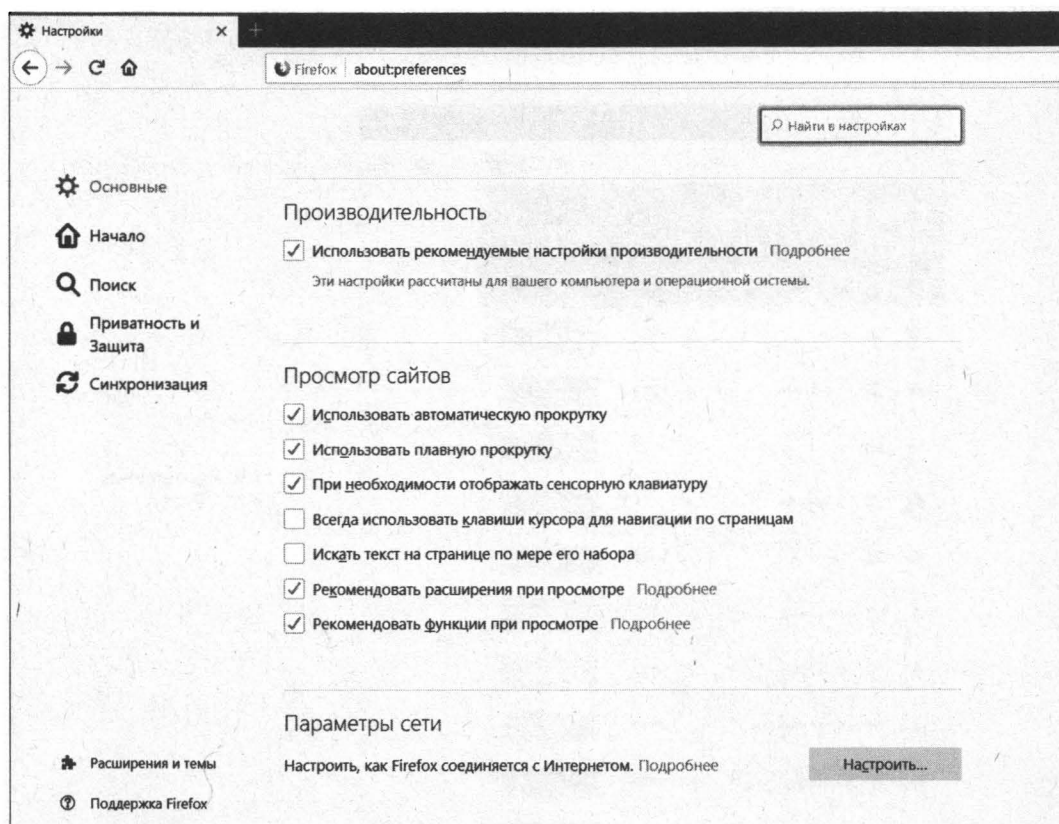


Рис. 1.6. Фрагмент страницы настроек браузера Firefox



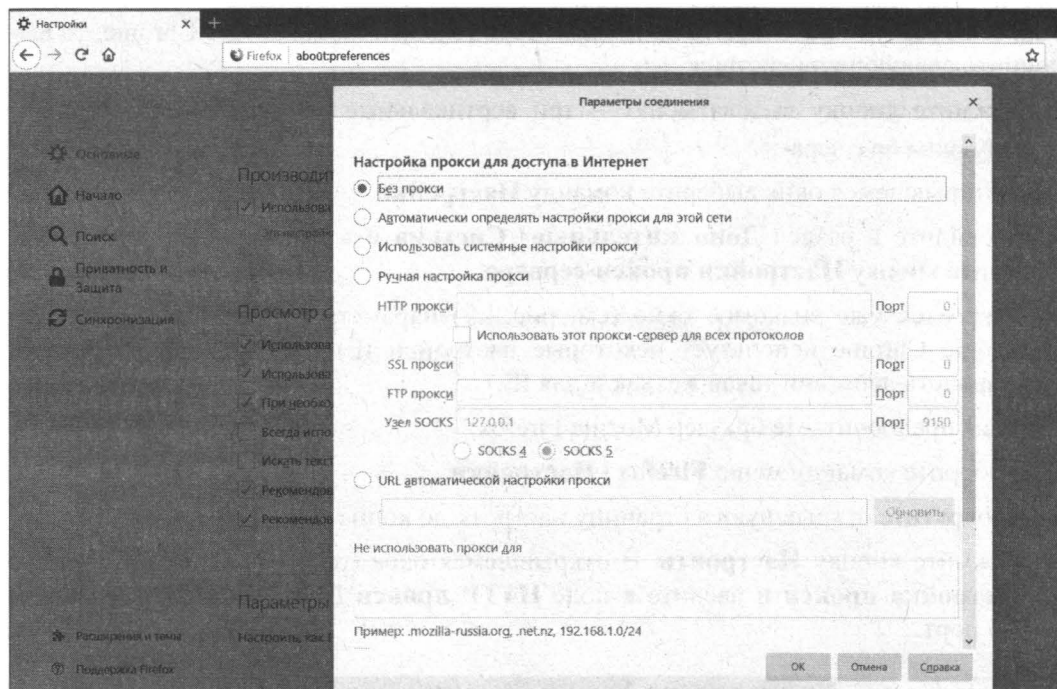


Рис. 1.7. Окно настроек параметров соединения браузера Firefox

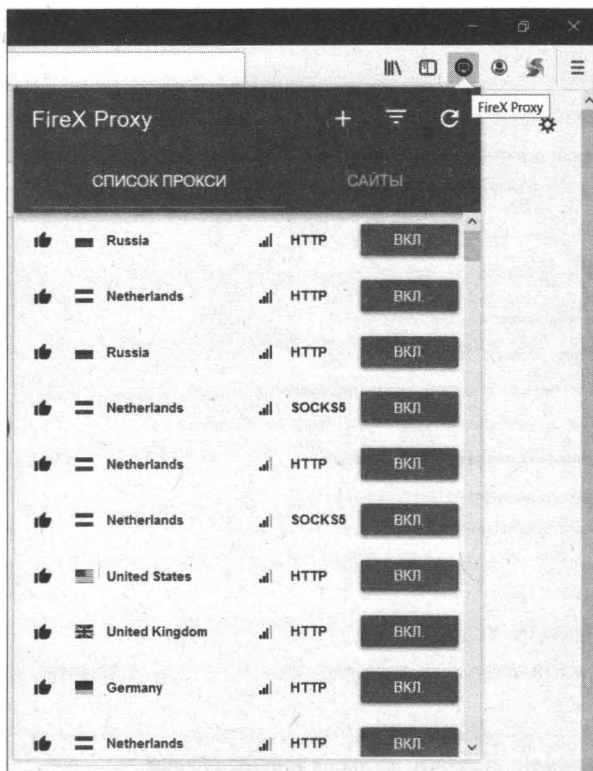


Рис. 1.8. Расширение FireX Proxy

Кстати, для Firefox имеется удобное расширение FireX Proxy (рис. 1.8), позволяющее быстро переключаться между прокси-серверами. Список прокси здесь, конечно, ограниченный — на сайтах со списками прокси-серверов выбор побогаче, но для мирных целей сгодится и такой.

### 1.3.3. Достоинства и недостатки анонимных прокси-серверов

Особых преимуществ перед анонимайзерами у анонимных прокси-серверов нет, если не считать того, что вы можете выбрать анонимный прокси с нужным вам IP-адресом. А вот недостатков достаточно:

- ☐ непостоянство — как уже отмечалось, некоторые анонимные прокси-серверы это плохо настроенные обычные. Когда администратор поймет, что его прокси используется в качестве публичного (анонимного), он закроет доступ, и вы больше не сможете использовать привычный IP-адрес;
- ☐ низкая скорость доступа — подобрать анонимный прокси с высокой скоростью доступа не всегда получается;
- ☐ не все анонимные прокси являются в полном смысле слова анонимными — некоторые из них передают узлу в заголовках запроса ваш IP-адрес. К тому же нет никакой гарантии, что такие прокси не ведут журнал посещений и не пересылают эту информацию третьим лицам;
- ☐ данные передаются по незашифрованному каналу — стало быть, существует возможность перехватить передаваемые вами данные. Некоторые анонимные прокси шифруют соединения, но они, как правило, требуют оплаты;
- ☐ неизвестна цель создания анонимного прокси — не все преследуют благие намерения. А вдруг выбранный вами прокси перехватывает ваши данные, в том числе пароли к аккаунтам, платежную информацию и т. п.?

Неоднозначно и с объемом передаваемых данных — некоторые прокси могут ограничивать его, а некоторые — нет. Если прокси является публичным из-за ошибки администратора, передача больших объемов информации может быть замечена администратором...

## 1.4. Локальная анонимность

Часто пользователям бывает все равно, следит ли за ними грозный администратор или кто-либо еще. Главное, чтобы коллеги по работе или родственники не видели, какие сайты посещались с их локального компьютера.

Просто очистить историю посещений мало, ведь остаются еще и «косвенные улики»: при загрузке страниц их копии и копии изображений и других объектов, внедренных в страницу, сохраняются в локальном кэше браузера. Проанализировав этот кэш, а также состав Cookies и сохраненные пароли, можно узнать, на каких сайтах вы бывали и какие страницы посещали.



Разберемся, как правильно очистить приватные данные браузера. Начнем с Google Chrome:

1. Нажмите комбинацию клавиш <Ctrl>+<Shift>+<Delete>.
2. В открывшемся окне (рис. 1.9) установите все флажки и нажмите кнопку **Удалить данные**.

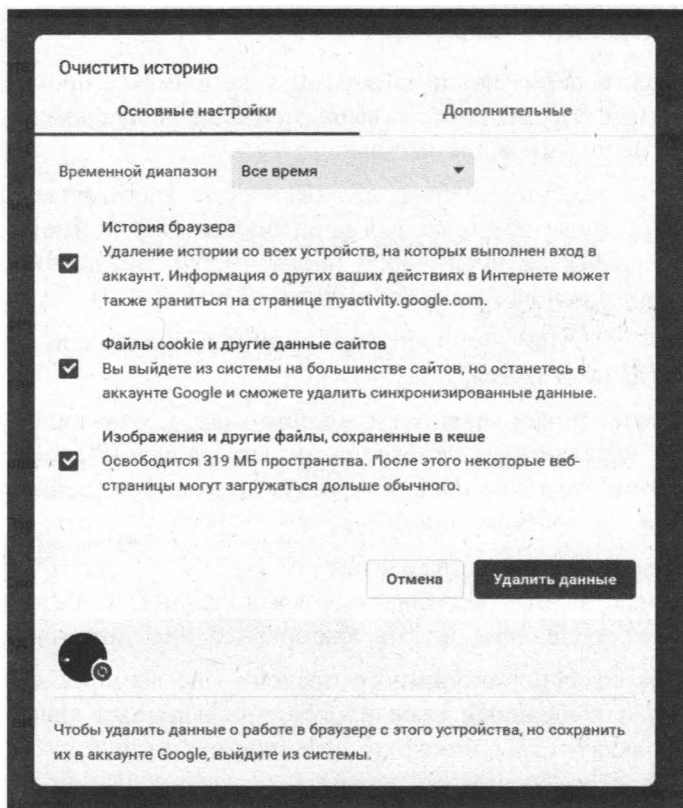


Рис. 1.9. Заметаем следы в браузере Google Chrome

Чтобы данные снова не начали накапливаться, из меню браузера выберите команду **Новое окно в режиме инкогнито** или нажмите комбинацию клавиш <Ctrl>+<Shift>+<N>.

В браузере Firefox комбинация очистки истории, кэша и Cookies такая же: <Ctrl>+<Shift>+<Del>. Установите в открывшемся окне все флажки и нажмите кнопку **Удалить сейчас** (рис. 1.10).

Здесь также перед посещением подозрительных сайтов лучше всего выбрать команду **Firefox | Новое приватное окно** (рис. 1.11). Это оптимальное решение, поскольку удаление информации о просмотренных страницах может вызвать подозрение и некоторые неудобства — ведь будет удалена вся история, все пароли. А в режиме приватного просмотра история, пароли и другие «улики» не сохраняются. Однако не путайте режим приватного просмотра с анонимностью — просто

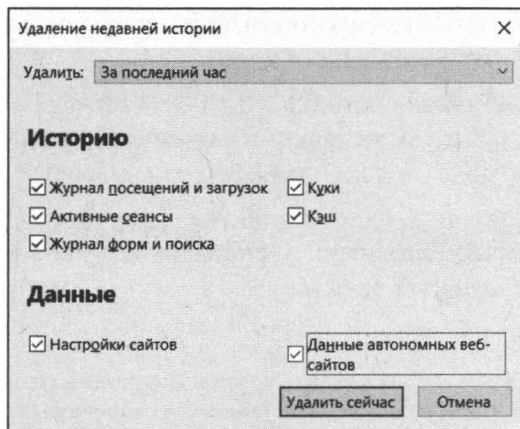


Рис. 1.10. Замечаем следы в браузере Firefox

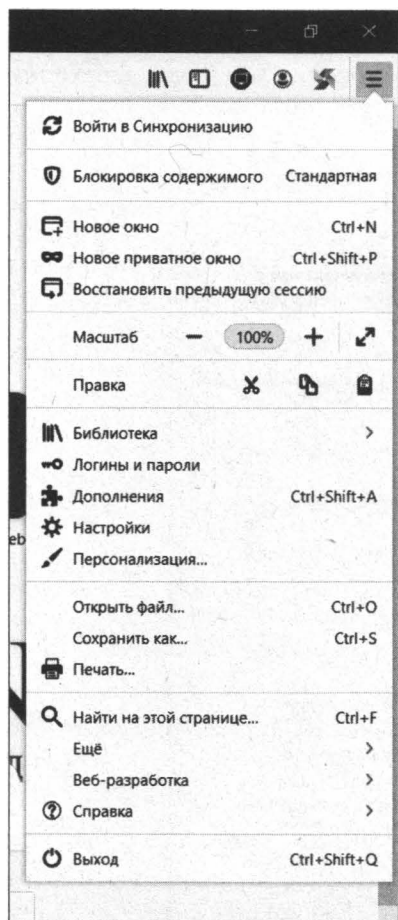


Рис. 1.11. Режим приватного просмотра в браузере Firefox

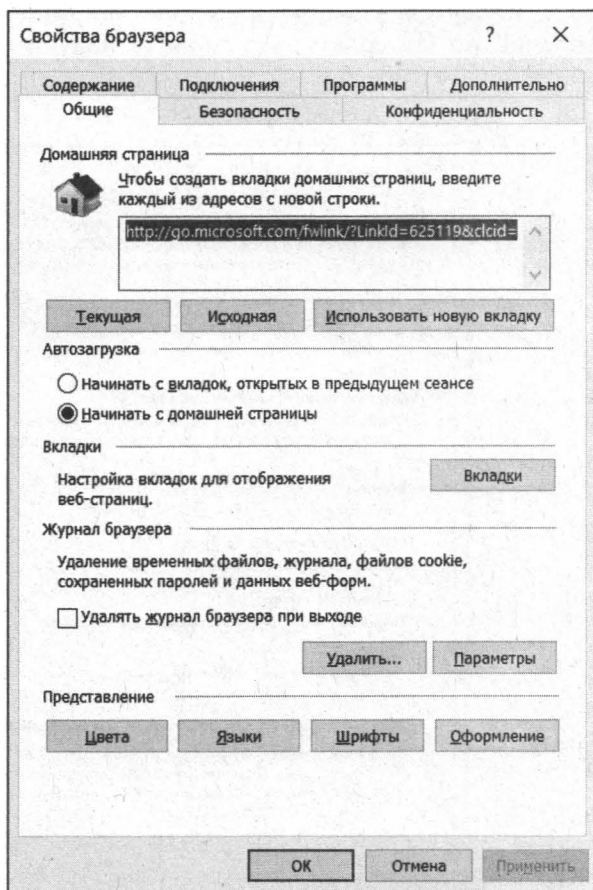


Рис. 1.12. Свойства браузера Internet Explorer: вкладка Общие

браузер не будет сохранять историю посещений и другие служебные данные, но удаленный узел сможет получить ваш IP-адрес.

В браузере Opera комбинация клавиш <Ctrl>+<Shift>+<Delete> тоже работает, а окошко очистки выглядит так же, как и в случае с Chrome, — ничего удивительного, этот браузер использует тот же «движок», что и Google Chrome.

В Internet Explorer откройте окно **Свойства браузера** и на вкладке **Общие** (рис. 1.12) нажмите кнопку **Удалить**. В открывшемся окне (рис. 1.13) установите все флажки и нажмите кнопку **Удалить**.

#### ПРИМЕЧАНИЕ

И тем не менее, даже если вы удалите временные файлы (кэш браузера), Cookies, сохраненные пароли и другие служебные данные, сохраняемые браузером, это не обеспечит вам истинной анонимности, поскольку по журналам провайдера заинтересованные и имеющие соответствующие полномочия службы могут легко восстановить всю историю вашей работы в Интернете. Поэтому читаем дальше...

Дополнительную информацию о том, как вычистить из браузера все следы ваших хождений по Интернету, вы сможете получить в *главе 9*, а мы пока переходим к следующему разделу.

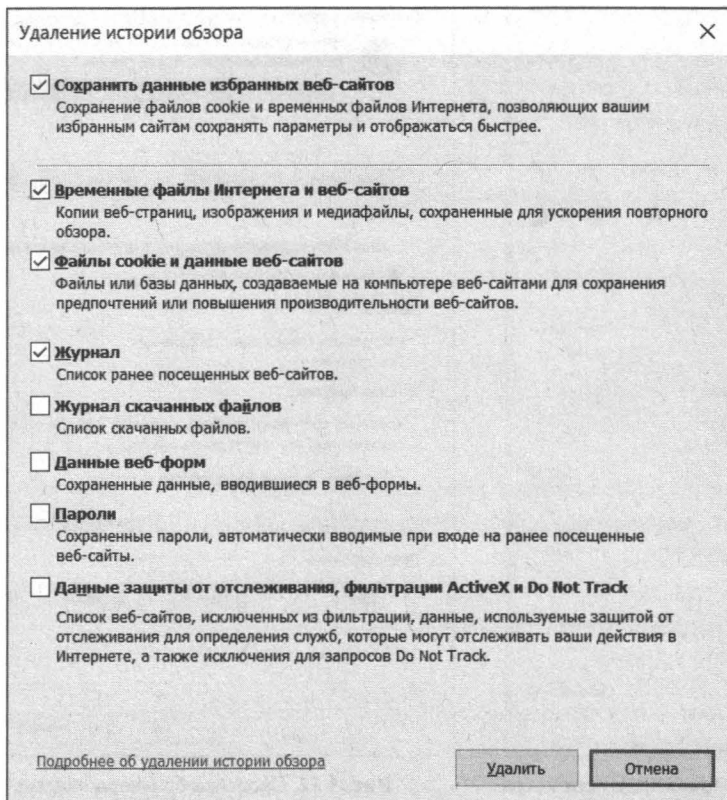


Рис. 1.13. Удаляем историю обзора в браузере Internet Explorer

## 1.5. Отключение слежки Windows 10

Сложно оставаться анонимным, если за тобой следит сама операционная система. Попробуем это исправить. Откройте окно параметров Windows 10 и перейдите в раздел **Конфиденциальность**. В разделе **Общие** отключаем все — чтобы вид окна стал таким, как показано на рис. 1.14.

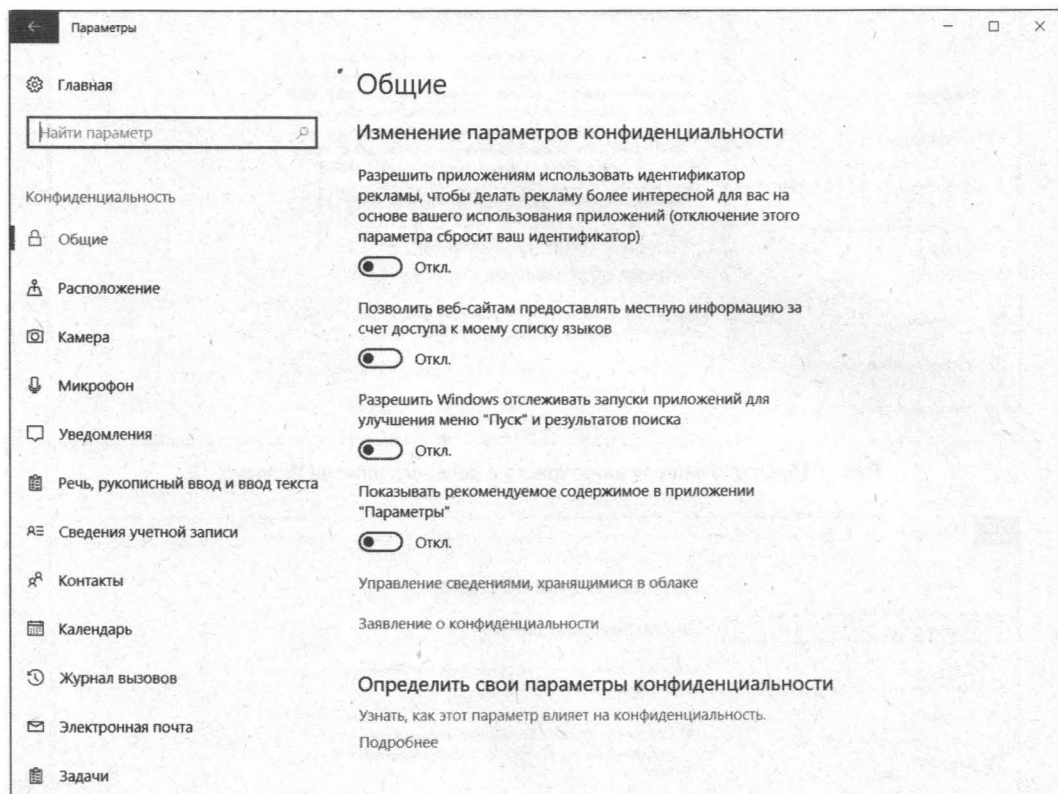


Рис. 1.14. Общие параметры конфиденциальности Windows 10

Затем перейдите в раздел **Речь, рукописный ввод и ввод текста** и нажмите кнопку **Остановить изучение**. Дело в том, что Windows 10 передает ваш голос, а также все, что вы вводите с клавиатуры, на серверы Microsoft якобы в ваших же интересах. Но не многим это нравится. Поэтому убедитесь, что все это безобразие выключено, а окно раздела **Речь, рукописный ввод и ввод текста** выглядит так, как показано на рис. 1.15.

В разделе **Отзывы и диагностика** нужно установить значение **Никогда** для параметра **Windows должна запрашивать мои отзывы**. Для параметра **Диагностические данные** выбираем **Основной**, а параметр **Разрешить корпорации Майкрософт...** отключаем (рис. 1.16).

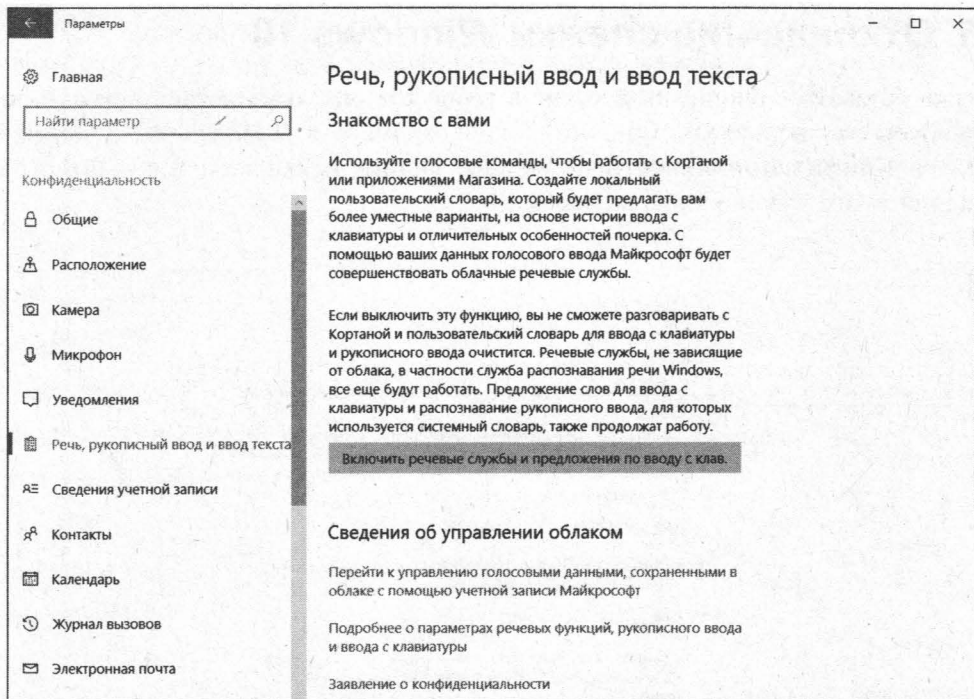


Рис. 1.15. Отключение клавиатурного и речевого шпиона Windows 10

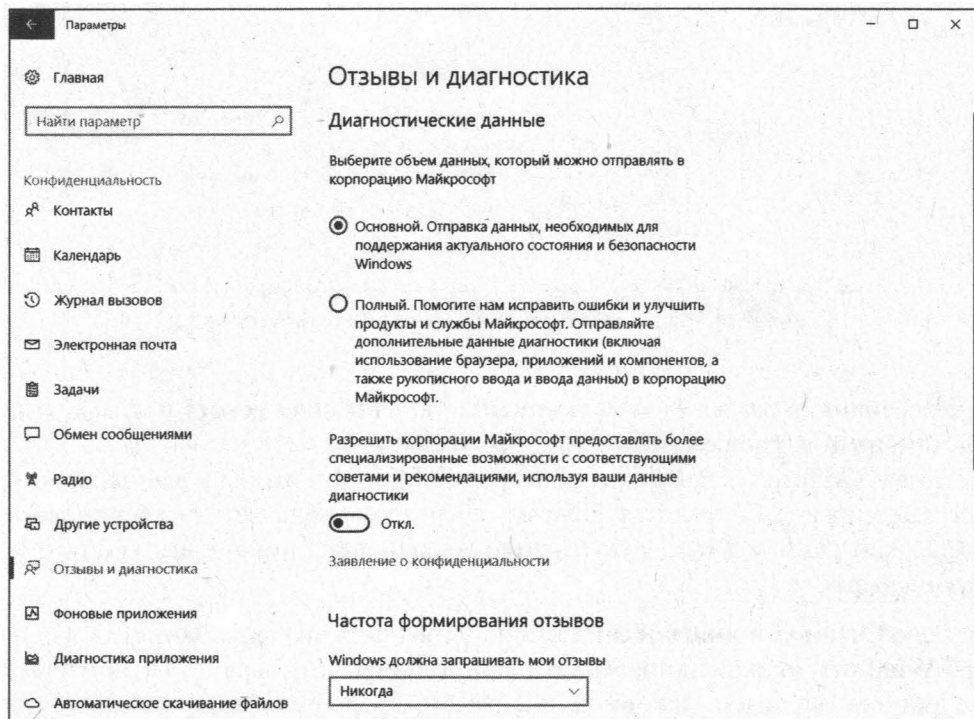


Рис. 1.16. Раздел Отзывы и диагностика параметров конфиденциальности Windows 10

В разделах **Камера** и **Микрофон** можно либо вообще отключить использование камеры и микрофона, либо же выбрать приложения, которые могут использовать эти устройства. На своем компьютере я разрешил доступ к камере и микрофону только приложению Skype (рис. 1.17), хотя некоторые пользователи наверняка захотят отключить доступ к камере и микрофону полностью.

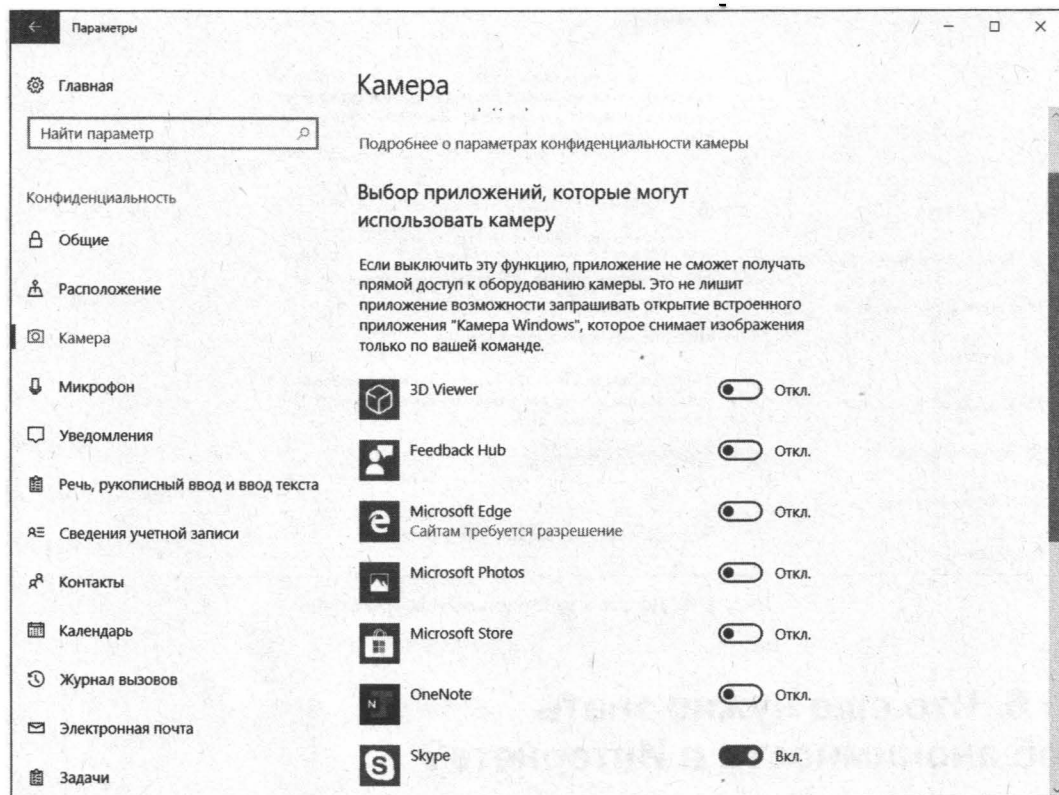


Рис. 1.17. Раздел **Камера** параметров конфиденциальности Windows 10

Ну и конечно же, раздел **Расположение** — здесь нужно выключить определение местоположения устройства (рис. 1.18). По желанию доступ к местоположению можно разрешить строго определенным приложениям.

На этом все. Если вам этого мало, тогда можно использовать специальные утилиты для отключения слежки, например: DWS (Destroy Windows 10 Spying). Скачать это приложение можно по адресу <https://github.com/Nummer/Destroy-Windows-10-Spying/releases>. Оно на русском языке, постоянно обновляется и позволяет, помимо всего прочего, также отключить обновление Windows 10 и удалить встроенные приложения.



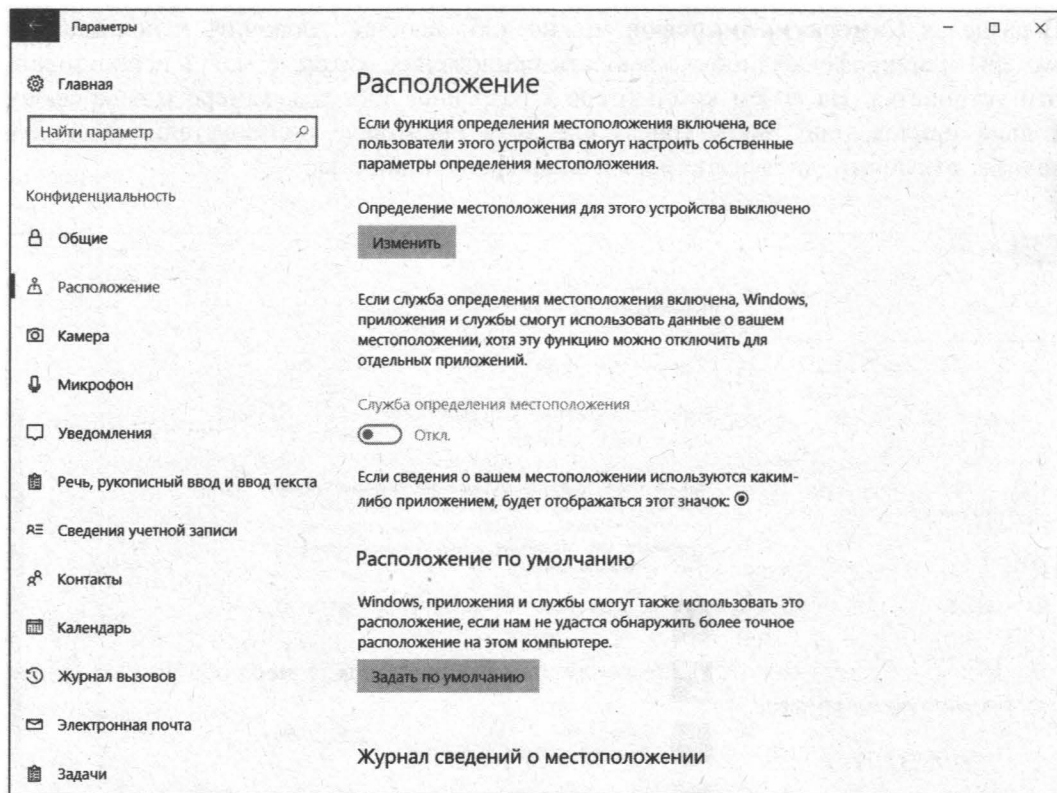


Рис. 1.18. Доступ к местоположению выключен

## 1.6. Что еще нужно знать об анонимности в Интернете?

Итак, приведем ряд источников информации, из-за которых анонимность пользователя подвергается угрозам.

- ❑ **Служебные данные, сохраняемые браузером.** Мы только что узнали, как от них избавиться.
- ❑ **Журналы удаленного узла.** Администратор такого узла, проанализировав свои журналы, сможет узнать, кто посещал его сайт, и какие файлы он загружал. Как ускользнуть от внимания администратора удаленного узла, мы уже тоже знаем — нужно использовать анонимные прокси-серверы или анонимайзеры. В этом случае в журнал удаленного узла будет записан не ваш IP-адрес, а IP-адрес анонимного прокси.
- ❑ **Журналы шлюза провайдера.** Администратор вашего интернет-провайдера при желании легко определит, какие страницы вы посещали и какие файлы загружали, — ведь вся эта информация проходит через его сервер. Замести следы поможет распределенная сеть Tor, которая будет рассмотрена в главе 2.

- ❑ **Перехват трафика.** Находясь в одной сети с «жертвой», злоумышленник может легко перехватить передающиеся по сети данные, увидеть кто и какие сайты загружает, даже прочитать вашу переписку в мессенджере или по емайлу. И для этого не нужно быть «крутым хакером» — в Интернете можно легко найти и скачать утилиты, делающие всю «грязную работу» по перехвату и организации информации. Злоумышленнику достаточно просто запустить такую программу и подождать. Сами понимаете, для этого особыми знаниями и навыками обладать не нужно.

## 1.7. Анонимность и закон

Здесь я постараюсь объяснить читателю, что все действия, описываемые далее в этой книге, — абсолютно законны, чтобы ко мне не было никаких претензий (мол, рассказываете, как совершать незаконные действия, или побуждаете к совершению таковых).

В следующих двух главах будут рассмотрены системы анонимизации и шифрования трафика. Но законно ли использование таких систем в Российской Федерации? Некоторые пользователи боятся использовать программное обеспечение подобного рода, поскольку не знают, какие последствия могут быть, и чего ожидать от нашего любимого государства.

### **ВНИМАНИЕ!**

Перед тем как продолжить, сразу хочу вас предупредить: я не юрист, никогда им не был и, судя по всему, вряд ли уже им стану. Все, что будет написано далее, — это результат моего собственного анализа и компиляции всевозможных законов и кодексов (знать законы обязан каждый, поскольку незнание этих самых законов никаким чудодейственным образом не освобождает от ответственности за их нарушение). Поэтому, если вы найдете здесь какие-либо неточности, буду рад выслушать ваши комментарии. Связаться со мной можно через издательство «БХВ-Петербург» ([mail@bhv.ru](mailto:mail@bhv.ru)) или напрямую на сайте [www.dkws.org.ua](http://www.dkws.org.ua) (пользователь *den*).

Первым делом определимся, чем являются программы шифрования и анонимизации трафика вроде Tor и I2P. Это сетевые приложения, использующие шифрование при передаче данных по сети. В законодательстве ничего не сказано об анонимизации, поэтому будем считать эти программы приложениями, использующими *алгоритмы стойкого шифрования*.

Мы используем наши приложения бесплатно и сами не получаем от их использования никакой выгоды, поскольку на их основе не оказываем никаких коммерческих услуг. И действительно — не будем же мы шифровать трафик соседа, пусть сам себе установит Tor и использует на здоровье.

Теперь обратимся к следующим правовым актам:

- ❑ Конституция РФ, ст. 23 (декларирует в том числе право на личную неприкосновенность и тайну переписки).
- ❑ Федеральный закон об информации, информационных технологиях и защите информации № 149-ФЗ.



□ Начнем с 23-й статьи Конституции РФ:

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Прочитаем внимательно гарантируемые права применительно к нашим проблемам. Выходит, что системы анонимизации и шифрования трафика стоят на страже конституционных прав человека — они технически обеспечивают ваше право на тайну переписки.

Если кто-то запрещает вам использовать подобное программное обеспечение, значит, он нарушает ваши непосредственные конституционные права. Этот кто-то должен ознакомить вас с судебным постановлением, где прямым текстом указан запрет на использование средств защиты данных. Другими словами, если тот или иной администратор с синдромом Наполеона пытается вам запретить использовать средства анонимизации трафика (а как же, ведь он не сможет посмотреть, какие сайты вы посещаете, — тем самым вы ограничиваете его властное чувство), можете смело подать на него в суд.

Что же касается контролирующих органов (не буду перечислять, их очень много на постсоветском пространстве), то они могут утверждать, что защиту личных данных гарантирует государство и оно же регулирует право доступа к ним этих самых контролирующих органов. С другой стороны, нигде в Конституции прямо не сказано, что гражданин не имеет право предпринимать самостоятельные действия по защите своей частной жизни.

Настало время обратиться к Федеральному закону № 149-ФЗ. Весь текст закона я приводить здесь не стану, а ограничусь лишь той его частью, которая относится к нашей ситуации (вот фрагмент из ст. 6):

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:
  - 1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
  - 2) использовать информацию, в том числе распространять ее, по своему усмотрению;
  - 3) передавать информацию другим лицам по договору или на ином установленном законом основании;
  - 4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
  - 5) осуществлять иные действия с информацией или разрешать осуществление таких действий.
4. Обладатель информации при осуществлении своих прав обязан:
  - 1) соблюдать права и законные интересы иных лиц;
  - 2) принимать меры по защите информации;
  - 3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Получается вот какая картина. Согласно п. 4 ст. 6 Федерального закона № 149-ФЗ *вы можете предпринимать меры по защите информации* и защищать свои права в случае незаконного получения информации — ведь попытка узнать, какие сайты вы посещаете, это и есть незаконное получение информации, поскольку разрешения на получение такой информации, скорее всего, у администратора или еще кого-то нет.

Требование не использовать средства анонимизации и шифрования трафика может быть расценено как нарушение п. 8 ст. 9 Федерального закона № 149-ФЗ:

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

На основании приведенных правовых актов использование средств анонимизации и шифрования трафика не является незаконным в РФ. Конечно, если у вас возникнут проблемы с использованием подобного ПО, обратитесь к квалифицированному юристу — может, появились дополнительные правовые акты, регулирующие использование программ для шифрования информации.

\* \* \*

В следующей главе мы поговорим о том, как безопасно посетить заблокированные администратором сайты, а также как зашифровать передаваемые вами по сети данные. Да, вы все правильно поняли — речь пойдет о распределенной сети Tor.



## ГЛАВА 2



# Тор: замечаем следы. Как просто и эффективно скрыть свой IP-адрес

## 2.1. Как работает Тор?

### Заходим в «Одноклассники» с работы

В главе 1 мы разобрались, как с помощью анонимных прокси-серверов и анонимайзеров скрыть свой IP-адрес. Но, как было показано, оба эти метода не предоставляют нужной степени анонимности.

Усложним поставленную задачу: теперь нам нужно не только скрыть свой IP-адрес от удаленного узла, но и полностью «замаскироваться», — чтобы администратор нашей сети или кто-либо еще не смогли определить, какие узлы мы посещаем, и чтобы никто не смог «подслушать» передаваемые нами данные.

Именно для решения таких задач и была создана *распределенная сеть Тор*. Тор (аббревиатура от The Onion Routing, «луковая» маршрутизация) — это свободное (т. е. свободно распространяемое и абсолютно бесплатное) программное обеспечение, использующееся для анонимизации трафика.

#### **ПРИМЕЧАНИЕ**

Поскольку исходный код Тор открыт всем желающим, любой пользователь может контролировать Тор на наличие/отсутствие «черного хода», специально созданного для спецслужб или еще кого бы то ни было. До настоящего момента сеть Тор не скомпрометировала себя — ее репутация незапятнанна.

Сеть Тор обеспечивает надежную анонимизацию и защищает пользователя от слежки как за посетителями конкретного сайта, так и за всей активностью самого пользователя. К тому же, все передаваемые пользователем данные шифруются, что исключает их прослушивание.

Вкратце принцип работы Тор заключается в следующем: при передаче данных от узла А (ваш компьютер) к узлу Б (удаленный сайт) и обратно данные передаются в зашифрованном виде через цепочку промежуточных узлов сети.

Отсюда следует еще одно преимущество использования Тор, которое наверняка оценят пользователи корпоративных сетей. Поскольку узел А обращается к узлу Б

не напрямую, а через промежуточные узлы, то это позволяет обойти «черный список» брандмауэра сети.

Рассмотрим конкретный пример. Предположим, у вас в офисе «злой» администратор заблокировал доступ сотрудников к социальной сети — к тем же «Одноклассникам» (наверное, это самая популярная сеть на наших просторах, хотя есть и не менее популярные: «ВКонтакте», «Мой Мир», Facebook и др.). Вы же, несмотря на это, все же хотите в свою социальную сеть попасть. Сайт [www.ok.ru](http://www.ok.ru) и будет узлом Б, а ваш рабочий компьютер — это узел А.

Вы запускаете программу Тог и вводите адрес узла Б. Программа строит цепочку от узла А к узлу Б из случайно выбранных ею сотен узлов сети — допустим, В, Г и Д (по умолчанию таких узлов три), причем узел В считается входным, Г — промежуточным, а Д — выходным. После этого программа шифрует содержимое сообщения (в рассматриваемом случае — адрес сервера Б, куда мы хотим попасть) и генерирует зашифрованное сообщение для каждого промежуточного узла, используя полученные при построении цепочки ключи шифрования участвующих в цепочке узлов, и указывая в этих сообщениях, какой из них будет следующим. В результате сообщения, передаваемые по цепочке, получают «слоистую» структуру, в которой необходимо расшифровать внешний слой, чтобы получить доступ к внутреннему (вот она — «луковая» маршрутизация в действии — слои шифрования покрывают ваши данные как слои луковицы). Каждый узел, получающий сообщение, «сдирает» свой слой шифрования и расшифровывает своим ключом содержимое сообщения: предназначенные этому узлу инструкции по маршрутизации и зашифрованные инструкции для узлов, расположенных дальше по цепочке. Последний узел снимает последний слой шифрования и отправляет сообщение адресату (т. е. в искомую социальную сеть). Иными словами, перед отправлением пакет последовательно шифруется тремя ключами: сначала для третьего узла, потом для второго и, в конце, для первого. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (аналогия с тем, как чистят луковицу) и узнает, куда отправить пакет дальше. Второй и третий узлы поступают аналогичным образом.

Понятно, что на последнем участке (от узла Д к узлу Б) данные будут узлом Д зашифрованы и переданы узлу Б в незашифрованном виде, поскольку узел Б не поддерживает открытые ключи сети Тог (если бы это было так, то весь Интернет был бы анонимным).

Обратное путешествие ответа сервера (узла Б в нашем примере) будет совершаться по той же цепочке — от узла Д к узлу В — с таким же «луковым» шифрованием и расшифровкой на последнем ее звене.

Посмотрите на рис. 2.1 — на нем изображен процесс передачи данных между вашим и удаленным компьютерами через сеть Тог. Проанализировав его, можно сделать следующие выводы:

- ❑ администратор вашей сети (или администратор провайдера) не сможет узнать, какие данные вы передаете, поскольку данные передаются в зашифрованном виде;
- ❑ администратор вашей сети не сможет узнать, какой узел вы посещаете, поскольку вместо интересующего вас узла ([www.ok.ru](http://www.ok.ru), [www.vk.ru](http://www.vk.ru) и т. п.) ваш узел

формально будет обращаться к одному из узлов сети Тог — ничем не примечательному узлу Интернета с непонятным доменным именем. Тем более, что при каждом новом подключении к Тог первый узел цепочки будет другим;

- ❑ если администратор сети заблокировал на брандмауэре доступ к интересующему вас узлу ([www.ok.ru](http://www.ok.ru), [www.vk.ru](http://www.vk.ru) и т. п.), вы сможете обойти это ограничение, поскольку фактически ваш компьютер подключается к совершенно другому узлу (к первому узлу цепочки Тог). Запрещать доступ к этому узлу нет смысла, т. к. при следующем подключении к Тог или при принудительной смене цепочки узел входа в Тог будет изменен;
- ❑ удаленный узел «увидит» только IP-адрес последнего узла цепочки, ваш IP-адрес будет скрыт;
- ❑ теоретически перехват данных возможен на последнем участке пути — от последнего узла цепочки Тог до удаленного узла. Но для этого нужно отследить всю цепочку Тог, что технически сделать очень сложно, поскольку она может состоять из десятков узлов. Если же получить доступ к удаленному узлу, то все равно нельзя будет понять, откуда исходил запрос, поскольку для этого нужно знать как минимум точку входа и точку выхода сети Тог.

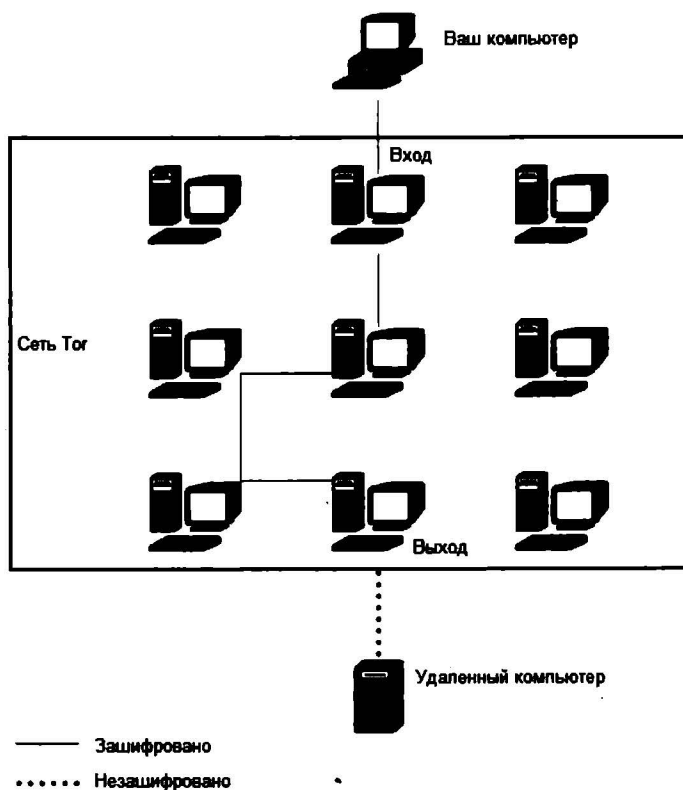


Рис. 2.1. Передача данных через распределенную сеть Тог

**ПРИМЕЧАНИЕ**

Способы рассекречивания цепочек Tor все же существуют — это вы тоже должны понимать. Однако цель должна оправдывать средства, учитывая необходимые для рассекречивания такой цепочки ресурсы. Если вы ничего не «натворили», а просто не хотите, чтобы кто-то узнал, какие сайты вы посещаете, никто не будет специально предпринимать серьезные действия, чтобы лишить вас анонимности.

Как уже было отмечено, при подключении к сети Tor для вашего компьютера определяются точка входа (выбирается случайный узел из сотен тысяч узлов Tor), «тоннель» и точка выхода — т. е. строится цепочка. В процессе работы с сетью иногда возникает необходимость сменить цепочку — это можно сделать без перезагрузки программного обеспечения (позже будет показано, как), что делает работу с сетью максимально комфортной.

Смена цепочки может понадобиться в двух случаях:

- ☐ когда нужно сменить конечный IP-адрес (например, чтобы получить IP-адрес, относящийся к определенной стране или городу);
- ☐ когда полученная цепочка оказалась слишком медленной. Скорость передачи информации зависит от каналов передачи данных от одного узла цепочки к другому, поэтому сгенерированная цепочка может оказаться нерасторопной. Вы же можете создать другую цепочку — вдруг она окажется быстрее?

**ПРИМЕЧАНИЕ**

Несколько лет назад Tor работала весьма медленно — иногда приходилось даже отключать загрузку картинок, чтобы загрузка страницы производилась побыстрее. Сейчас с производительностью все нормально, и прямой необходимости отключать загрузку картинок нет.

## 2.2. Tor или анонимные прокси-серверы и анонимайзеры. Кто кого?

Если вам стал понятен принцип работы сети Tor, то и ее преимущества тоже должны быть ясны, но на всякий случай сравним Tor с анонимными прокси-серверами и анонимайзерами:

- ☐ Анонимайзеры и анонимные прокси не шифруют передаваемые данные, поэтому администратору вашей сети (или сети провайдера) будет легко вычислить, какие сайты вы посещали и какие данные передавали.

Сеть Tor шифрует всю передаваемую информацию, поэтому, даже если кто-то перехватит данные, передающиеся по вашему каналу связи, он получит лишь бессмысленные наборы байтов. Однако за все нужно платить — Tor работает медленнее, чем анонимайзеры, хотя быстрее, чем некоторые анонимные прокси.

- ☐ Некоторые анонимные прокси-серверы на самом деле таковыми не являются, поскольку сообщают ваш IP-адрес удаленному узлу в заголовках HTTP-запроса. Без специальной проверки (а для этого вам нужно приобрести свой сервер или хотя бы купить хостинг и написать сценарий, анализирующий заголовки HTTP-

запросов от анонимного прокси) нельзя узнать, является ли прокси-сервер действительно анонимным.

При использовании Тог скрыт не только ваш IP-адрес (от внимания администратора удаленного узла), но и адрес назначения (от внимания администратора вашей сети).

- При использовании анонимного прокси-сервера проследить цепочку весьма просто — в ней будут присутствовать всего три элемента: ваш компьютер, анонимный прокси и удаленный компьютер. Ваша анонимность, по сути, зависит только от одного псевдоанонимного прокси-сервера. А вдруг этот анонимный прокси передает информацию заинтересованным лицам?

При использовании Тог вы доверяете передаваемые данные нескольким случайным серверам, которые выбраны из тысяч доступных узлов сети Тог. Многие эти узлы представляют собой обычные домашние компьютеры добровольных помощников. Чтобы отследить передаваемые данные, ваш противник (пусть это будет тот самый «злой» администратор сети) должен контролировать все эти случайно выбранные узлы, разбросанные по всему миру. Сами понимаете, что вероятность такого контроля ничтожно мала.

- Некоторые анонимные прокси (или анонимайзеры) предлагают зашифрованный обмен данными (между вами и прокси), но такие серверы, как правило, платные.

Сеть Тог абсолютно бесплатна, и при этом использование Тог ни к чему вас не обязывает — вы можете быть как обычным клиентом, так и узлом сети Тог, — режим работы выбирается по вашему желанию.

- Анонимные прокси обычно поддерживают только HTTP-трафик, а сеть Тог теоретически можно настроить на поддержку любого TCP-соединения.
- Тог, в отличие от других подобных систем (имею в виду JAP<sup>1</sup>) и некоторых анонимных прокси, ни разу себя не скомпрометировала и имеет незапятнанную репутацию — ведь ее исходный код открыт, и любой желающий может с ним ознакомиться. А вот разработчики JAP были пойманы на добавлении «черного хода» по запросу спецслужб.

## 2.3. Критика Тог и скандалы вокруг этой сети

Некоторые специалисты критикуют Тог, поскольку она может использоваться для организации преступных действий. Ряд стран даже объявили войну Тог — например, в 2006 году спецслужбы Германии захватили шесть компьютеров, работающих узлами сети Тог, а в 2007 году немецкая полиция арестовала владельца одного из узлов сети Тог, поскольку через его узел неизвестный отправил ложное сообще-

---

<sup>1</sup> Программа JAP — одна из программ, обеспечивающих анонимность в Интернете. Она скрывает реальный IP-адрес, перемешивая данные всех пользователей JAP с помощью микс-прокси до тех пор, пока отследить реальный адрес станет невозможно.



ние о теракте. В 2009 году в Китае были заблокированы до 80% IP-адресов публичных серверов Тог. В 2016 году Тог был заблокирован в Турции.

Однако возможность применения в преступных целях не делает Тог оружием злоумышленников. Наоборот, они предпочитают использовать другие методы: *spruware*, вирусы, взлом прокси-серверов, использование краденых мобильных телефонов и т. п. Злоумышленник может украсть мобильный телефон, выйти в Интернет, передать провокационное сообщение, а затем выбросить телефон в реку — зачем ему сложности с Тог?

Сеть Тог в большинстве случаев используется законопослушными пользователями, пытающимися обойти ограничения брандмауэра «родной» сети, а также не желающими, чтобы за ними следили.

Впрочем, не нужно думать, что Тог — это панацея, и если вы ее используете, то на 100% анонимны. Нет. Вас все же могут рассекретить. Методы различны: от клавиатурного шпиона, установленного на вашем компьютере, до создания выходного сервера Тог, который будет перехватывать весь трафик. И если ваш трафик будет выходить из сети Тог через этот сервер, то он может быть перехвачен злоумышленником.

### **Из истории вопроса...**

В 2007 году национальная полиция Швеции арестовала эксперта по компьютерной безопасности Дена Эгерстада (Dan Egerstad), поскольку он неправомочно получил доступ к компьютерной информации. Эгерстад создал пять выходных серверов Тог и перехватывал незашифрованный трафик, в результате чего получил пароли к электронной почте посольств, государственных организаций, правоохранительных органов разных стран и т. п.

Подробнее об этом и других интересных фактах вы сможете прочитать на страничке Википедии (не вижу смысла приводить эту информацию в книге, если вы можете прочитать ее бесплатно): <http://ru.wikipedia.org/wiki/Tor>. Настоятельно рекомендую на досуге посетить приведенную ссылку — вы узнаете много интересных фактов о сети Тог, а мы тем временем перейдем к практике — к использованию Тог.

## **2.4. Установка и использование Тог**

### **2.4.1. Быстро, просто и портативно: Тог на флешке**

Программное обеспечение Тог можно сравнить со швейцарскими часами — последние можно покупать только в фирменном магазине, чтобы не нарваться на подделку. Также и Тог следует скачивать только с ее официального сайта по адресу: <https://www.torproject.org/ru/> (рис. 2.2).

Не рекомендую загружать программное обеспечение Тог из всевозможных каталогов программ — такое «нефирменное» программное обеспечение может быть модифицировано разного рода злоумышленниками для слежки за вами или передачи вашей информации (паролей, электронных писем и т. п.) третьим лицам. Помните, что исходный код Тог доступен каждому, и это основное ее преимущество, но и

основной недостаток тоже. Ведь каждый может скачать и модифицировать комплект Тог, а затем выложить на своем сайте (например, комплект Тог с браузером Firefox, в котором установлены дополнительные плагины) якобы с благими намерениями. А вы, загрузив и установив такую модифицированную версию Тог, получите систему, которая будет передавать злоумышленнику всю информацию о вас. Поэтому идем на официальный сайт и скачиваем все там.

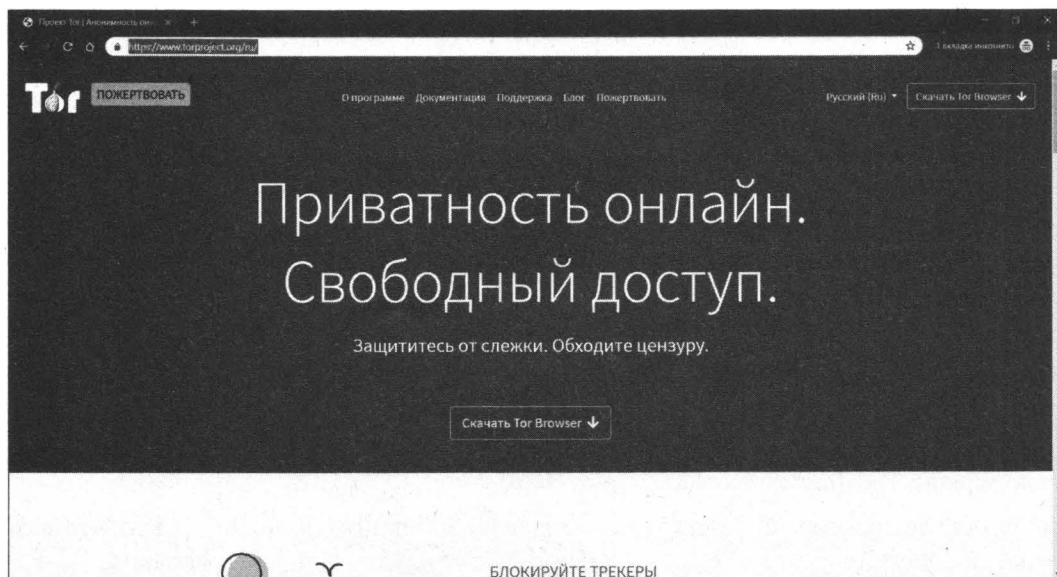


Рис. 2.2. Официальный сайт Тог

Надо отметить, что тут существуют варианты:

- ☐ можно скачать уже преднастроенный комплект программного обеспечения (Tor Browser): вам надо будет запустить только одну программу, немного подождать, пока осуществится подключение к сети Тог, и вы готовы к работе,
- ☐ а можно скачать все необходимое по отдельности и настраивать привязку компонентов вручную.

Мы будем ориентироваться на уже готовый комплект, поскольку так меньше вероятность допустить при настройке ошибку, из-за которой анонимность не будет обеспечиваться.

Преимущества преднастроенного пакета очевидны. Во-первых, вам не придется ничего настраивать, следовательно, вы не сможете совершить ошибку. Во-вторых, вы можете распаковать загруженный архив прямо на флешку, и комплект программ для анонимизации трафика будет всегда с вами. А это значит, что вы можете не бояться заходить в Интернет с чужих компьютеров, — при условии, что на компьютере не установлен клавиатурный шпион, никто не перехватит ваши данные.

Настройка Тог вручную может понадобиться в двух случаях: если у вас уже есть настроенный браузер Firefox или же вам нужно настроить другую сетевую про-

грамму (которая не является браузером или клиентом обмена сообщениями) на работу через Tor.

Рассмотрим первый случай. Пусть на вашем компьютере работает Firefox с уже установленными плагинами. Как известно, при включении режима анонимизации трафика (плагин Torbutton) большинство полезных плагинов будут отключены. Однако Torbutton не может знать обо всех плагинах, потенциально способных передавать ваш IP-адрес третьей стороне, поэтому из соображений безопасности свой браузер использовать не рекомендуется — лучше воспользоваться «чистым» браузером, входящим в комплект Tor Browser.

Второй случай актуален при настройке сторонних программ. Но опять-таки, вам никто не мешает загрузить пакет Tor Browser и использовать его компоненты для анонимизации трафика сторонней программы. Далее будет показано, как настроить для работы через Tor Browser почтовый клиент Thunderbird (см. *разд. 2.4.2*), как обеспечить работу программы интернет-телефонии Skype через специальным образом подготовленный браузер Google Chrome (см. *разд. 2.4.3*), как настроить для работы через Tor браузер Opera (см. *разд. 2.4.4*) и FTP-клиент FileZilla (см. *разд. 2.4.5*).

Прямая ссылка на загрузку последней версии Tor Browser выглядит так: [https://dist.torproject.org/torbrowser/8.5.3/torbrowser-install-win64-8.5.3\\_ru.exe](https://dist.torproject.org/torbrowser/8.5.3/torbrowser-install-win64-8.5.3_ru.exe)

Однако я все же советую вам воспользоваться кнопкой **Скачать Tor Browser** на официальном сайте Tor (см. рис. 2.2) — вы будете уверены, что загружаете самую последнюю версию Tor Browser.

Запустите загруженный файл (это самораспаковывающийся архив), и все, что вам нужно сделать, — это указать каталог, в который следует распаковать Tor (рис. 2.3). Пакет Tor Browser для Windows будет работать в версиях Windows от 7 до 10.

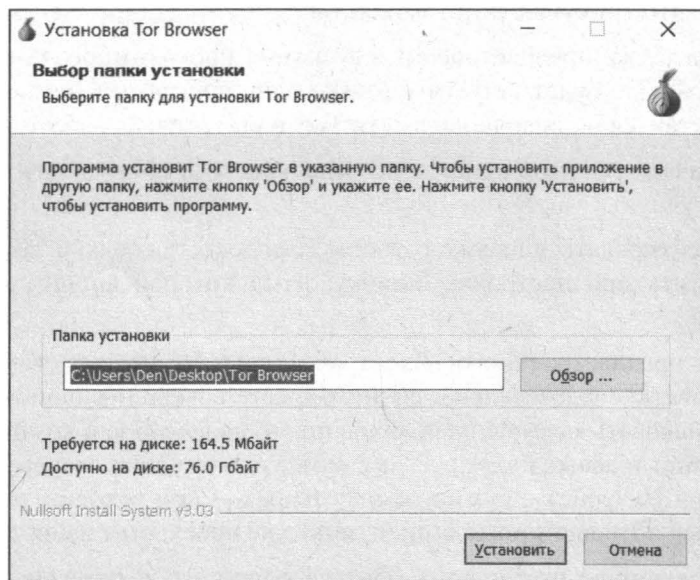


Рис. 2.3. Распаковка Tor Browser

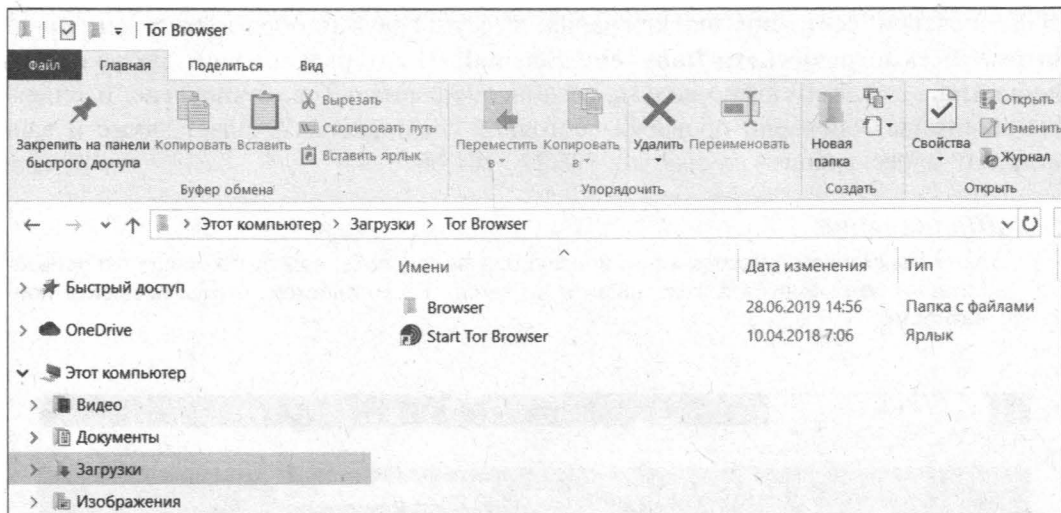


Рис. 2.4. Запустите программу, щелкнув двойным щелчком на ярлыке **Start Tor Browser**

Перейдите в каталог, в который вы распаковали Tor Browser, и запустите программу, щелкнув двойным щелчком на ярлыке **Start Tor Browser** (рис. 2.4).

При первом запуске вы увидите окно с кнопками **Соединиться** и **Настроить** (рис. 2.5). Если в стране вашего пребывания Тог не запрещен, тогда можно попытаться нажать кнопку **Соединиться**. Если же Тог запрещен, тогда у вас будет возможность настроить сетевые параметры, которые будут описаны далее.

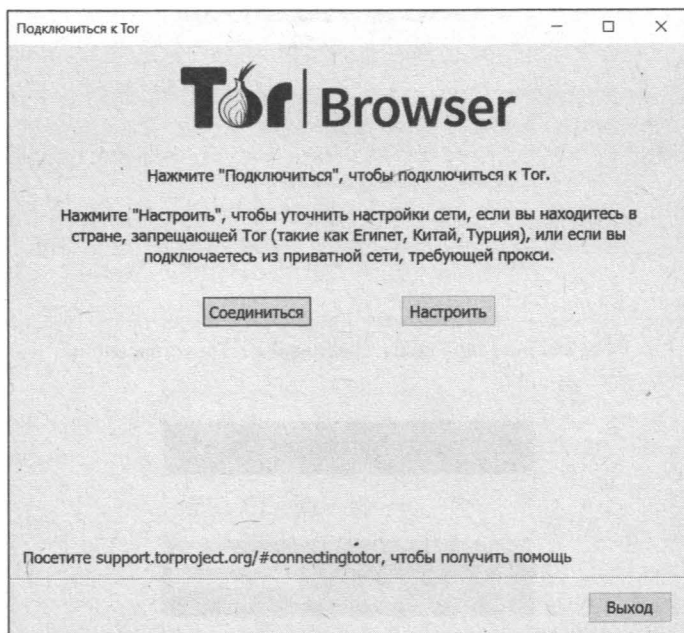


Рис. 2.5. Первый запуск Tor Browser

Для проверки состояния подключения к сети браузер обратится к сценарию <https://check.torproject.org/?lang=en-US&small=1>, который сообщит статус соединения (рис. 2.6). Как можно видеть, соединение с сетью Тор установлено, и теперь вы анонимны. Сценарий проверки состояния соединения сообщает также и ваш новый IP-адрес, в нашем случае это: 185.220.101.66.

### ПРИМЕЧАНИЕ

Хотя мы скачали русскоязычную версию браузера (чтобы вам было проще ею пользоваться), рекомендуется запрашивать страницы на английском, чтобы повысить приватность.

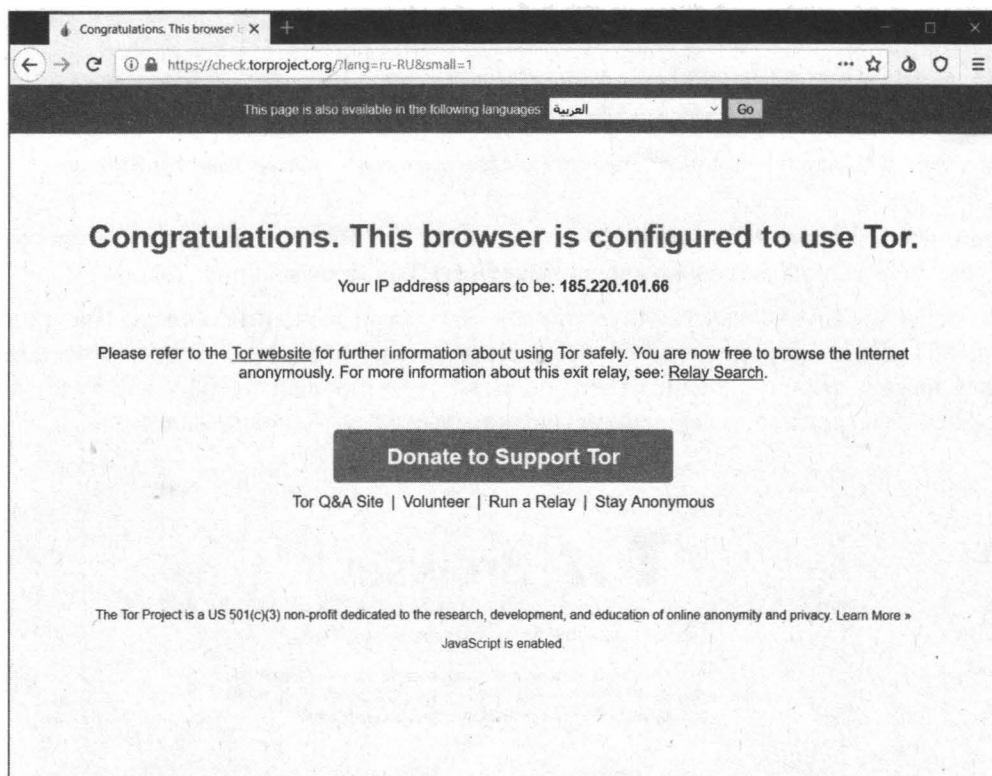


Рис. 2.6. Браузер Firefox: соединение с Тор установлено

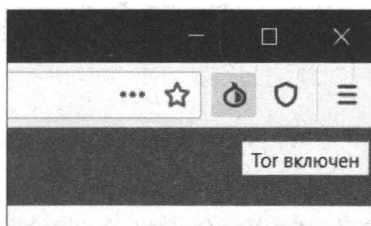



Рис. 2.7. Тор включен

Проконтролировать, работает ли Тог, можно и по-другому — в процессе анонимного серфинга. Для этого подведите указатель мыши к кнопке с изображением логотипа Тог  в правом верхнем углу окна браузера (рис. 2.7) — всплывающая подсказка покажет состояние подключения к Тог (кстати, это и есть плагин TorButton). Если нажать на эту кнопку, откроется меню. В нем, помимо других команд, будет присутствовать команда **Настройки сети Тог** (Tor Network Settings), позволяющая настроить Тог.

#### ПРИМЕЧАНИЕ

В меню, открывающемся по нажатию на кнопку Тог, вы увидите команду **Новая личность**. Используйте ее для смены IP-адреса и удаления всех собранных в процессе прошлого сеанса Cookies.

Что делать дальше? Просто вводите адрес желаемого узла и наслаждайтесь анонимным серфингом. Скорость соединения зависит от узла, к которому вы подключаетесь, и от сгенерированной цепочки.

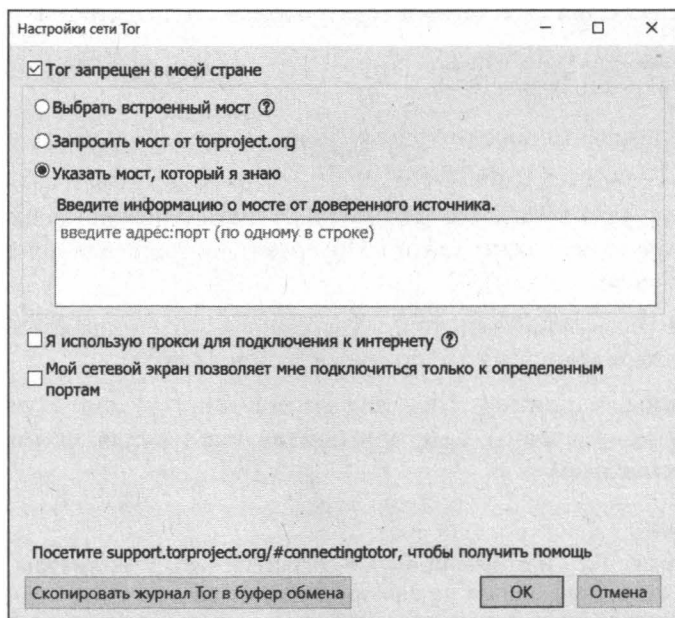


Рис. 2.8. Настройка сетевых параметров Tor Browser, если использование Тог в вашей стране запрещено

Рассмотрим теперь настройку сетевых параметров, если использование Тог в вашей стране запрещено. Чтобы открыть окно настроек, нажмите кнопку **Настроить** в окне, открывающемся при первом запуске Tor Browser (см. рис. 2.5), или кнопку Тог на панели браузера и из появившегося меню выберите команду **Настройки сети Тог**. В открывшемся окне (рис. 2.8) будет всего три параметра:

- ☐ флажок **Тог запрещен в моей стране** (Tor is censored in my country) — некоторые провайдеры блокируют доступ к Тог. В этом случае установите данный

флажок и укажите мосты, через которые будет осуществляться доступ к Тор (см. рис. 2.8). Список мостов доступен по адресу <https://bridges.torproject.org>;

- ☐ флажок **Я использую прокси для подключения к Интернету** (I use proxy to connect to the Internet) — если доступ к Интернету осуществляется через прокси-сервер, который вы обычно указывали в настройках браузера, установите этот флажок и укажите параметры прокси: имя узла, порт, имя пользователя и пароль (если нужно);
- ☐ флажок **Мой сетевой экран позволяет мне подключиться только к определенным портам** (This computer goes through a firewall that only allows connections to certain ports) — эта опция используется для обхода брандмауэра. После установки флажка появится поле, в котором надо ввести разрешенные порты через запятую без пробелов, — например: 80, 443, 3128.

Осталось рассмотреть еще один вопрос, а именно — выбор узлов выхода, что важно, если вы хотите получить на выходе IP-адрес определенной страны. В подкаталоге `Browser\TorBrowser\Data\Tor` каталога установки пакета `Tor Browser` находится конфигурационный файл `torrc`. Откройте его и добавьте две строки:

```
EntryNodes $fingerprint,$fingerprint,...
ExitNodes $fingerprint,$fingerprint,...
```

Первый параметр задает список входных узлов, а второй — выходных. Вместо переменной `$fingerprint` вы можете задать:

- ☐ идентификатор узла в сети Тор (его можно узнать с помощью карты активности сети Тор, которую несложно найти в Интернете, осуществив поиск по соответствующим ключевым словам);
- ☐ IP-адрес узла (но нужно быть точно уверенным, что он является сервером сети Тор, — это тоже можно узнать с помощью той же карты);
- ☐ ISO-код страны, например, {de} для Германии, {ru} для России и т. д. Для определения кода страны вам пригодится следующая ссылка: <http://www.perfekt.ru/dict/cc.html>.

#### **ПРИМЕЧАНИЕ**

Разработчики Тор не рекомендуют использовать параметры `EntryNodes` и `ExitNodes` (это плохо влияет на анонимность), но вы можете поступать так в крайних случаях — когда нужно получить цепочку с жестко заданными входными и выходными узлами.

## **2.4.2. Настройка почтового клиента Mozilla Thunderbird**

Программный продукт Тор сам по себе является прокси. Поэтому настройка работы любой программы через Тор сводится к ее настройке к работе через этот прокси. Так давайте рассмотрим процесс настройки популярных программ на работу через Тор.

Ранее в состав пакета Тор входила панель управления `Vidalia`. С ее помощью можно было управлять запуском и остановом прокси-сервера. В современных версиях раз-



работчики отказались от нее. Можно или запускать программу tor вручную (файл tor.exe), или, что гораздо проще, запускать уже знакомый нам браузер Тог. По сути Tor Browser — это обычный браузер Firefox с двумя плагинами: Torbutton и TorLauncher (рис. 2.9). Первый плагин — это та самая кнопка с логотипом Тог, о которой мы уже говорили. Второй — обеспечивает запуск Тог на вашем компьютере. Другими словами, для запуска прокси-сервера Тог достаточно запустить браузер Тог — Tor Browser.

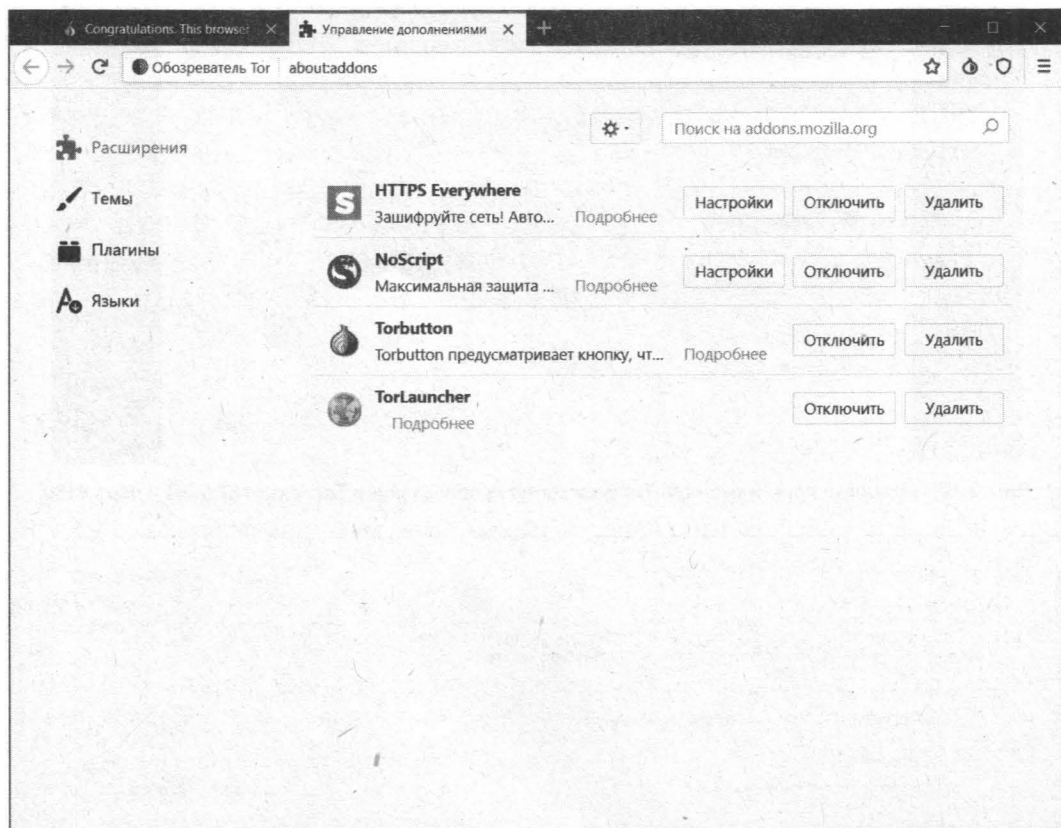


Рис. 2.9. Плагины Tor Browser: Torbutton и TorLauncher

Главное отличие Tor Browser от обычного браузера Firefox — Tor Browser изначально настроен на использование Тог, т. е. в настройках его прокси-сервера указан порт Тог (рис. 2.10). Именно эти параметры и нужно указать в настройках программы, чтобы она работала через Тог: узел 127.0.0.1 и порт 9150.

Рассмотрим настройку почтового клиента для работы с сетью Тог на примере программы Mozilla Thunderbird. Выполните следующие действия:

1. Запустите Tor Browser и убедитесь, что подключены к сети Тог.
2. Запустите Mozilla Thunderbird
3. Выберите команду **Настройки | Настройки**.





4. Перейдите в раздел **Дополнительные**, далее — на вкладку **Сеть и дисковое пространство** (рис. 2.11).
5. Нажмите кнопку **Настроить**. В открывшемся окне установите параметры так, как показано на рис. 2.12.

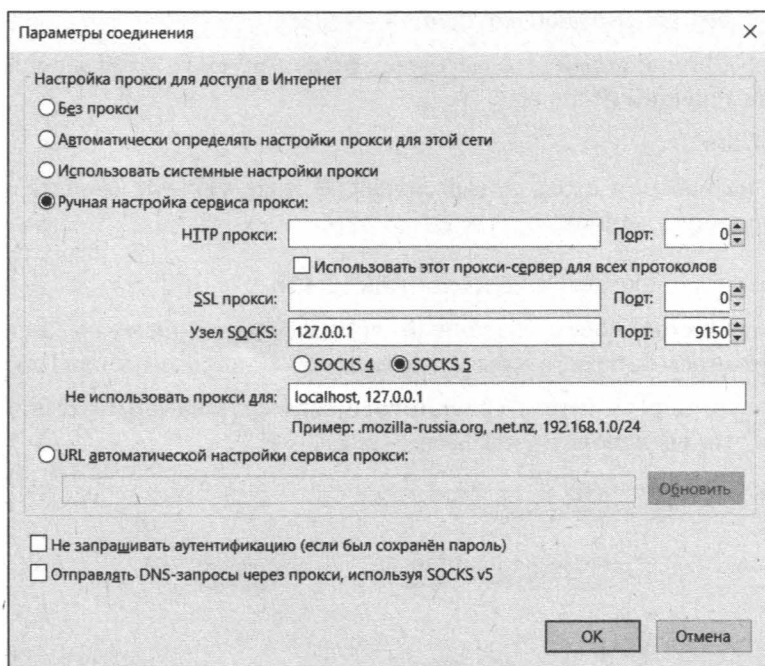


Рис. 2.12. Настройка параметров прокси-сервера почтового клиента Mozilla Thunderbird для работы с сетью Tor

### 2.4.3. Настройка программы интернет-телефонии Skype

К сожалению, современные версии Skype не позволяют указать настройки прокси, а старые уже не подключаются к сети Skype. Так что использовать Skype анонимно «в лоб» уже не выйдет. Но у нас есть две обходные возможности.

#### Воспользоваться VPN-сервисами

Если вас беспокоит перехват трафика Skype третьими лицами (хотя трафик Skype зашифрован и непонятно, что эти третьи лица будут делать с зашифрованными данными), то для дополнительной безопасности можно воспользоваться VPN-сервисами (см. главу 3). При создании VPN-соединения весь трафик помещается в так называемый *туннель*, что обеспечивает его дополнительное шифрование. Получается, ваш трафик будет шифроваться дважды: средствами Skype и в VPN-туннеле.

## Настроить браузер Chrome для работы через Tor

Вторая возможность — воспользоваться веб-приложением [web.skype.com](https://web.skype.com) (веб-версия Skype). Однако открыть его через Tor Browser не получается: нужны Edge, Opera или Chrome. Для настройки Chrome через Tor выполните следующие действия:

1. Убедитесь, что Tor Browser запущен.
2. В браузере Chrome перейдите по адресу <https://pr-cy.ru/browser-details/>, чтобы узнать ваш текущий IP-адрес.
3. Закройте Chrome.
4. Создайте на рабочем столе новый ярлык. В поле **Объект** свойств ярлыка введите следующую запись: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" -proxy-server="socks5://localhost:9150" --host-resolver-rules="MAP \* 0.0.0.0 , EXCLUDE localhost" (рис. 2.13).
5. Запустите Chrome через созданный ярлык и перейдите по адресу <https://pr-cy.ru/browser-details/>, чтобы убедиться, что IP-адрес изменен (рис. 2.14).
6. Перейдите по адресу <https://check.torproject.org/?lang=en-US&small=1>, чтобы убедиться, что вы используете Chrome (рис. 2.14).

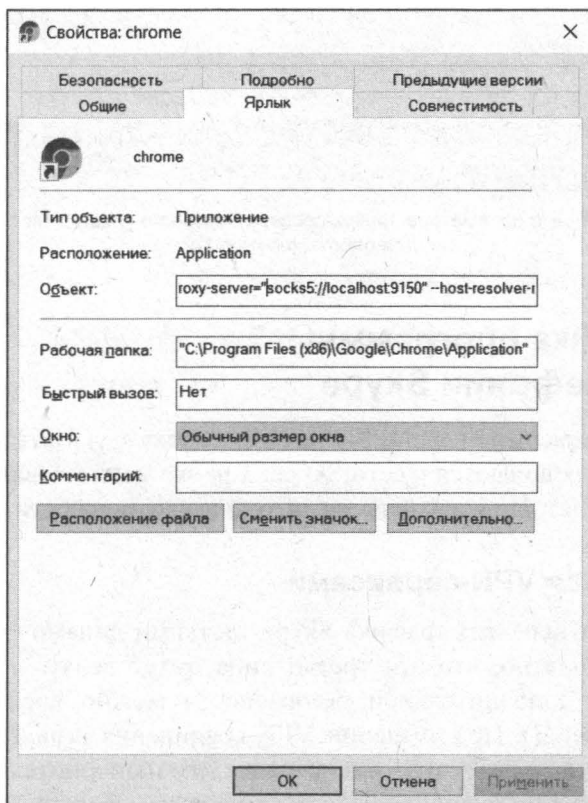


Рис. 2.13. Ярлык для запуска Chrome через Tor

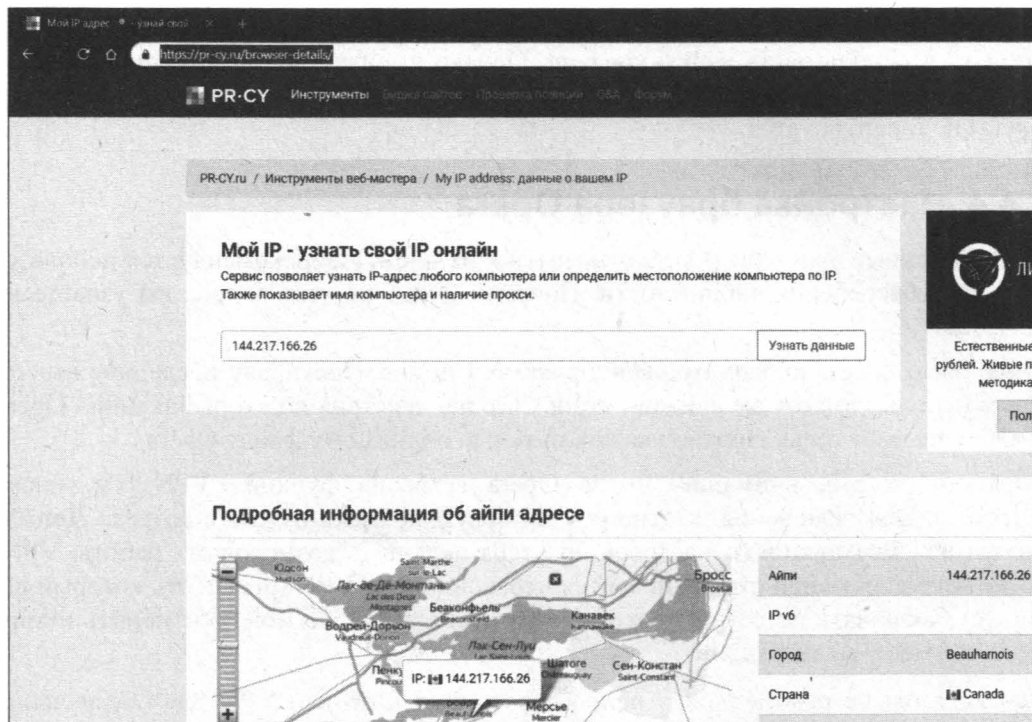


Рис. 2.14. IP-адрес изменен

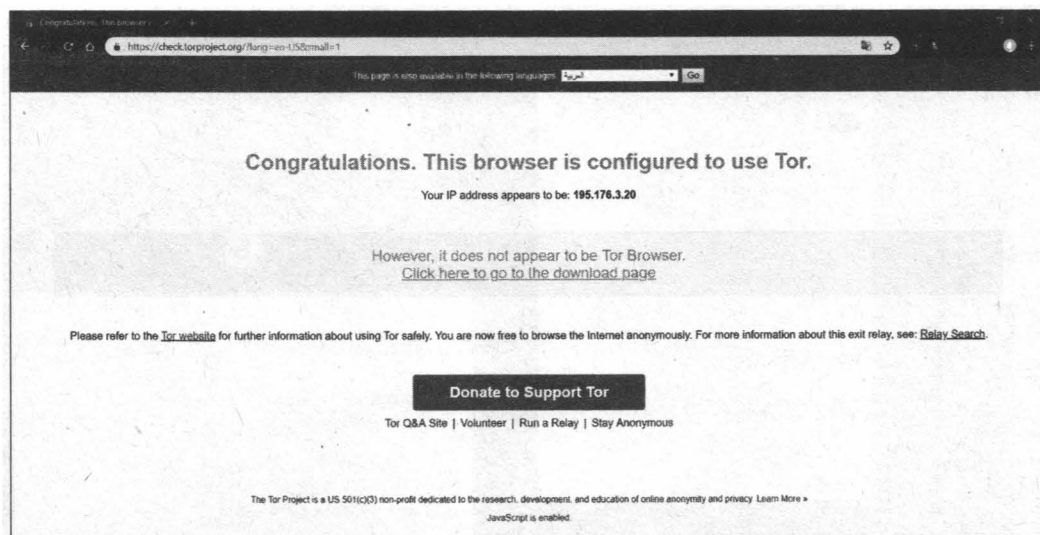


Рис. 2.16. Tor в Chrome

Обратите внимание: на рис. 2.14 и 2.15 указаны разные IP-адреса. По идее IP-адреса должны быть одинаковые. Почему так происходит, и сервис pr-cy.ru «видит» другой IP-адрес — непонятно. Но ни один из этих адресов не является моим IP-адресом, поэтому можно считать, что мы добились успеха.

Вот теперь можно в подготовленном таким образом браузере Google Chrome открыть и использовать **web.skype.com**. Однако имейте в виду, что ваша анонимность при использовании браузеров с закрытым исходным кодом (Edge, Chrome, Opera) не гарантируется.

## 2.4.4. Настройка браузера Opera

Проприетарные браузеры (Opera относится к их числу) не рекомендуется использовать для обеспечения анонимности. Почему? Ответ на этот вопрос вы узнаете из главы 12.

Ранее было показано, как «торифицировать» Chrome. Поскольку последние версии Opera используют тот же движок, что и Chrome, действия по «торификации» Opera аналогичные — только нужно указать путь к исполняемому файлу Opera.

Обратите, кстати, внимание, что в Opera встроена функция VPN (см. также разд. 3.4). Для включения штатного VPN браузера Opera нужно в разделе **Дополнительно | Возможности** настроек браузера включить возможность работы VPN, после чего в адресной строке появится переключатель VPN (рис. 2.16), который вы сможете включать по возникновению надобности. Там же можно изменить и виртуальное месторасположение.

Однако я бы не рекомендовал использовать этот штатный VPN для обеспечения анонимности — все равно браузер знает о вас все, и все ваши действия тщательным

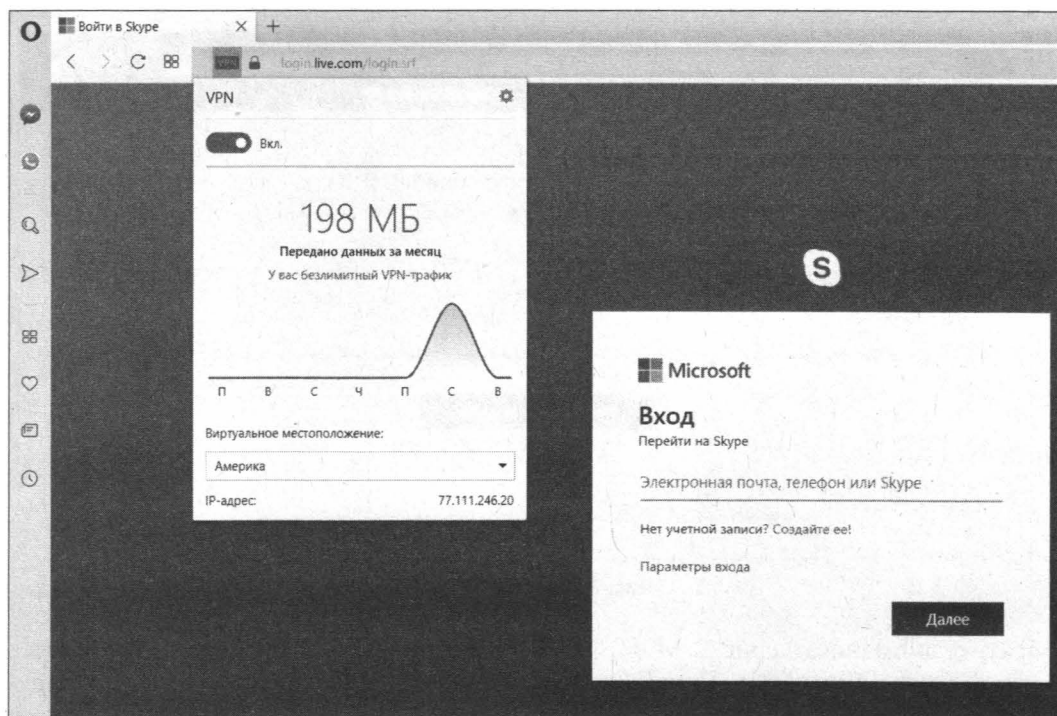


Рис. 2.16. Включение VPN в браузере Opera: через него также можно войти в Skype

образом логируются на серверах Орега. Также мною было замечено, что этот сервис иногда «отваливается», и сайтам становится виден ваш реальный IP-адрес. Скажем так: для обхода узла, заблокированного администратором или провайдером, эта опция браузера Орега сгодится, а для обеспечения анонимности лучше использовать Tor Browser.

## 2.4.5. Настройка FTP-клиента FileZilla

Чтобы не создавать лишнюю нагрузку на сеть Тог, рекомендуется не передавать через нее по FTP огромные файлы. Но все же Тог использовать для обмена файлами по протоколу FTP можно — ведь когда обновляешь свой сайт, в большинстве случаев размер каждого из передаваемых файлов составляет всего несколько килобайт и редко доходит до мегабайта. Конечно, ISO-образы дистрибутивов операционных систем лучше через Тог не выкладывать (большие объемы трафика снижают производительность всей сети — потом не удивляйтесь, что Тог работает медленно). Впрочем, я не утверждаю, что через Тог нельзя передать, скажем, ISO-образ размером 650 Мбайт или даже 4 Гбайт. Технически такая возможность есть, но перед тем, как начать передачу, ознакомьтесь с *разд. 2.7*. А вот для передачи небольших файлов Тог вполне сгодится.

Для настройки FileZilla на использование Тог выполните команду меню **Редактирование | Настройка**. В открывшемся окне перейдите в раздел **Базовый прокси** (рис. 12.17), установите тип прокси **SOCKS 5**, введите в поле **Хост прокси** имя

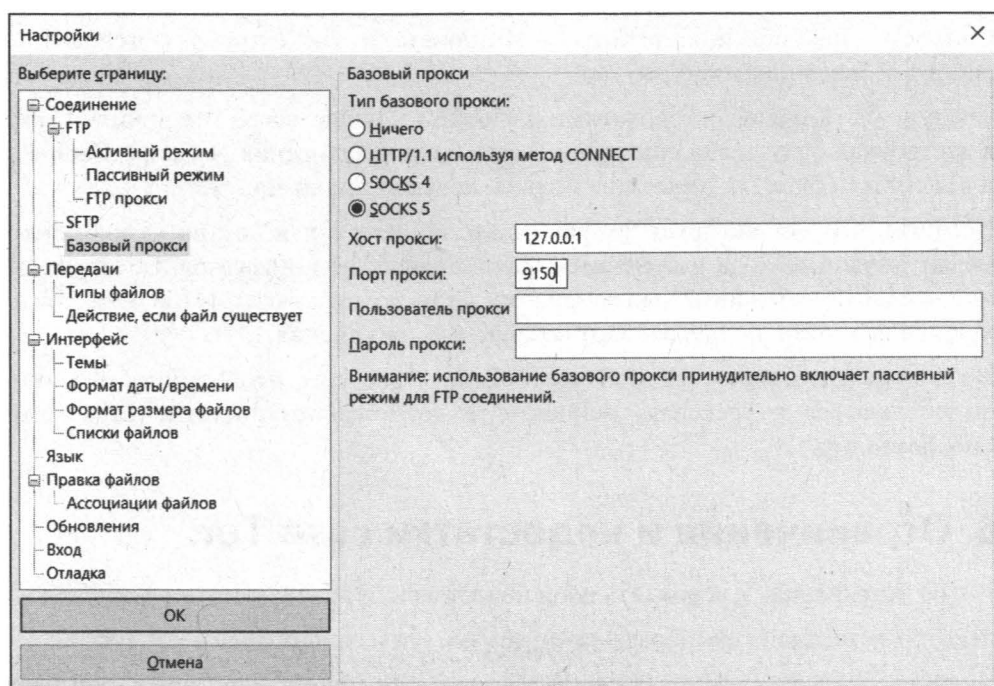


Рис. 12.17. Настройка FTP-клиента FileZilla на использование Тог



прокси: 127.0.0.1 и в поле **Порт прокси порт:** 9150. Не забудьте нажать кнопку **ОК** для сохранения настроек.

## 2.5. Когда Tor бессильна. Дополнительные расширения для Firefox

Не нужно думать, что если вы установили Tor, то теперь полностью анонимны. Начинаящие пользователи часто допускают ряд ошибок, которые приводят к их раскреживанию. При использовании Tor нужно помнить следующее:

- ❑ Tor защищает те программы, которые работают через нее. Если вы установили Tor Browser, но не настраивали на работу через Tor остальные сетевые программы, то о никакой анонимности можно и не мечтать. Наиболее частая ошибка пользователей заключается в следующем. Пользователь устанавливает и запускает Tor Browser, а затем запускает другой браузер — например, Opera или Chrome, и думает, что его трафик анонимизирован. Но это не так, поскольку эти браузеры не настроены на использование Tor.
- ❑ Разработчики Tor рекомендуют использовать браузер Firefox с плагином Torbutton. Этот плагин отслеживает статус сети Tor и отключает потенциально опасные плагины (Flash, ActiveX, Java и т. п.). В настройках Torbutton вы можете запретить отключение плагинов, но в этом случае Tor не гарантирует вам анонимность. Порой различные плагины могут идти в обход Tor и передавать приватную информацию. Лучше всего использовать два браузера: например, Google Chrome — для обычной работы в Интернете и Tor Browser (Firefox с Torbutton) — для анонимной работы.
- ❑ Следует быть очень осторожными с Cookies. Лучше всего отключить Cookies в настройках браузера, а еще лучше установить расширения NoScript, CookieSafe или Permit Cookies, которые еще больше повысят анонимность.
- ❑ Помните, что Tor шифрует трафик от вас до сети Tor и внутри самой сети, но между точкой выхода и конечным узлом трафик не шифруется. Если есть возможность, подключайтесь к конечному узлу по протоколу HTTPS. К сожалению, не все сайты поддерживают безопасные соединения.
- ❑ Не используйте через Tor BitTorrent. Если у вас есть необходимость анонимно обращаться к трекерам, используйте возможности системы Tails (<http://tails.boum.org/>).

## 2.6. Ограничения и недостатки сети Tor

Tor — не безупречна. У всего есть свои недостатки, и вот недостатки Tor:

- ❑ некоторые интернет-ресурсы запрещают доступ из анонимной сети Tor;
- ❑ скорость доступа к интернет-ресурсам через Tor существенно ниже, чем напрямую, но это плата за анонимность;

- ❑ хотя Тог можно настроить для работы с любым TCP-соединением, ряд портов закрыты в выходной политике Тог, поэтому некоторые действия через Тог выполнить нельзя. Очень часто закрывается порт 25 — отправить почту не получится. Делается это специально, чтобы компьютеры не использовались для рассылки спама;
- ❑ некоторые сайты блокируют доступ пользователей из других стран. Если выходной IP-адрес будет принадлежать другой стране, зайти на искомый сайт у вас не получится. Отчасти можно решить проблему, выбрав выходной узел в нужной стране, но это создает небольшие неудобства.

## 2.7. Этика использования сети Тог

При использовании Тог придерживайтесь следующих правил:

- ❑ не используйте Тог для действий, не требующих анонимности: онлайн-игры, интернет-радио, онлайн-видео, загрузка больших файлов. Все эти действия создают ненужную и бесполезную нагрузку на сеть Тог, и ей трудно справиться с такой нагрузкой;
- ❑ не используйте Тог для нанесения вреда сайтам, рассылки спама и других вредоносных действий. Иначе у администраторов разных ресурсов появятся причины закрыть доступ из сети Тог, и она станет бесполезной. Этим вы повредите пользователям всего мира, которым действительно нужна анонимность.





## ГЛАВА 3



# Что такое VPN и «с чем его едят»? Защита передаваемых по сети данных от прослушивания

## 3.1. Зачем нужен VPN?

В этой главе мы поговорим о защите данных, передаваемых по сети. Другими словами: вы не пытаетесь быть анонимным, но хотите защитить передаваемые по сети данные, чтобы они не были доступны третьим лицам.

Надо иметь в виду, что все данные (за исключением передаваемых по безопасным HTTPS-соединениям) пересылаются по сети в открытом виде. И когда вы передаете по сети какие-либо данные (просматриваете веб-страницы, вводите пароли, получаете и отправляете почту, заполняете на сайтах те или иные формы, получаете и пересылаете файлы), они могут быть перехвачены. Но кем? Да кем угодно, в этом заинтересованным.

Если вы подключаетесь к Интернету по Wi-Fi, то данные могут быть перехвачены на отрезке компьютер/смартфон — маршрутизатор Wi-Fi, их могут перехватить и на самом маршрутизаторе Wi-Fi, кроме того, данные перехватывает и анализирует оборудование провайдера, предоставляющего доступ к Интернету владельцу беспроводного маршрутизатора. Другими словами, даже предположить сложно, в каком именно месте ваши данные могут быть перехвачены.

При подключении к Интернету через сеть мобильного оператора на участке от смартфона/планшета до базовой станции перехват данных организовать не в пример сложнее. Но, ясное дело, их вполне может перехватывать сам мобильный оператор — точнее, он их может записать, поскольку ваш трафик и так проходит через его оборудование. Действительно записывает он ваш трафик или нет — никто не знает, но то, что фиксируются посещенные вами сайты и другая ваша сетевая активность, — это точно.

Как защитить себя? Выход один — использование VPN (Virtual Private Network, виртуальная частная сеть). Объяснять здесь, что такое VPN и откуда она взялась, я не стану. Достаточно отметить, что через VPN-соединение весь обмен данными

происходит в зашифрованном виде, и ни «перехватчик» в локальной сети (при подключении Wi-Fi), ни интернет-провайдер, ни мобильный оператор перехватить ваши данные не смогут. Точнее, перехватить-то они как раз смогут, но вот расшифровать — вряд ли...

Для организации VPN-соединения вам нужно найти подходящий VPN-сервис и подключиться к нему. Тогда ваши данные будут в зашифрованном виде отправляться на VPN-сервер, а оттуда пересылаться тому узлу, с которым вы фактически желаете работать. Провайдер же увидит только обращение к VPN-сервису и то, что вы передаете какие-то данные. Но определить, куда фактически идут дальше данные, и что именно вы отправляете, он не может.

Проблема здесь в том, что хорошие и быстрые VPN-сервисы — платные, хоть и плата эта невелика. Далее мы поговорим о выборе VPN-сервиса.

### **ВНИМАНИЕ!**

Большинство VPN-сервисов (даже платных) предупреждают, что хранят данные о клиенте, в том числе историю вашего перемещения по сети (конкретно кто и что хранит — зависит от сервиса). Также отмечается, что эта информация может быть передана соответствующим органам по решению суда. Однако особо беспокоиться не нужно. Во-первых, ваши данные не будут анализироваться и перехватываться кем попало: вашим соседом, провайдером, оператором и т. п. — они увидят только зашифрованный трафик. Во-вторых, даже если вы что-то и натворите противозаконного, до решения суда еще нужно дойти. К тому же, поскольку большинство VPN-сервисов находятся в США, это только усложняет процесс выдачи информации о вас.

### **ВАЖНО!**

Все американские VPN-сервисы подписали акт Digital Millennium Copyright Act. Если вы будете заниматься электронным пиратством, о вас сообщат непосредственно правообладателю. Поэтому для кражи и распространения контента лучше поискать не американские сервисы. Вы даже можете не знать, что *распространяете* контент. Вы можете скачать, скажем, фильм или MP3-файл через торренты и оставить Torrent-клиент включенным, что даст другим пользователям возможность скачать этот контент с вашего смартфона. Это и есть распространение.

## **3.2. Выбор VPN-сервиса**

Сравнение популярных VPN-сервисов можно найти в Интернете, здесь же мы рассмотрим несколько тех, на которые вам следует обратить внимание.

### **3.2.1. VPN Shield**

Ранее это был самый доступный по цене VPN-сервис<sup>1</sup>, однако компания пересмотрела цены на свои услуги, и сервис существенно подорожал. Впрочем, он все равно остается самым дешевым сервисом — далее вы поймете почему, посмотрев на цены конкурентов.

---

<sup>1</sup> См. <http://www.vpnshieldapp.com/>.

При оплате на три года действует специальное предложение — по 2,78\$ в месяц. Это не очень дорого. Однако если платить помесечно, то стоимость составит уже 5,99\$. Годовая подписка обойдется в 39,99\$. Зато за эти деньги вы получаете неограниченный трафик — у некоторых конкурентов оплата производится за трафик, что не всегда выгодно. Также в один аккаунт можно добавить до пяти устройств, и сумма при этом не изменится. То есть за 5,99\$ в месяц можно защитить все свои устройства (в большинстве случаев нужно защищать один стационарный компьютер и один-два смартфона). Имеется и бесплатная пробная версия на 1 день.

Компания находится в Люксембурге, а это означает, что законодательство США на нее не распространяется, но у компании есть серверы в США, Германии, Англии, Нидерландах и Китае.

Сервис поддерживает все популярные протоколы: PPTP, L2TP, IPsec, OpenVPN. VPN-клиент сервиса поддерживает Windows 7/8/10, macOS, Android, iOS.

К недостаткам сервиса можно отнести службу поддержки, работающую только через e-mail — не очень оперативное средство связи.

Зато компания не собирает (а если и собирает, то явно об этом не сказано) информацию о пользователях.

Преимущества:

- ☐ компания не собирает данные о пользователях;
- ☐ поддержка всевозможных операционных систем;
- ☐ поддержка до пяти устройств в одном аккаунте;
- ☐ безлимитный трафик;
- ☐ бесплатная пробная версия.

Недостатки:

- ☐ техническая поддержка только по e-mail.

### 3.2.2. IPVanish VPN

Штаб-квартира этого сервиса<sup>1</sup> находится в США. Это крупный американский VPN-провайдер.

Тарифных планов три: или каждый месяц 10\$, или каждые три месяца 26,99\$, или раз в год, но 77,99\$. Трафик (вне зависимости от выбранного тарифного плана) не ограничивается.

Точек присутствия не так много, как у предыдущего провайдера, но и не мало. Серверы находятся в США, Канаде, Великобритании, Франции, Японии, Малазии, Венгрии, Нидерландах, Южной Африке, Испании, Швеции и Южной Корее.

Этот сервис собирает информацию о пользователях и работает в рамках акта DMCA Copyright Policy. Однако на сайте сказано, что собирается только самая необходимая информация, но какая именно — не уточняется.

---

<sup>1</sup> См. <https://www.ipvanish.com/>.

Поддерживаются протоколы PPTP, L2TP и OpenVPN. Протокол IPSec не поддерживается. VPN-клиент сервиса поддерживает операционные системы Windows, Windows Phone, Linux, macOS, Chrome OS, Android, iOS, операционные системы роутеров. Не ограничиваются ни трафик, ни пропускная полоса.

Преимущества:

- ☐ поддержка самых разных операционных систем;
- ☐ круглосуточная техническая поддержка;
- ☐ неограниченная пропускная полоса.

Недостатки:

- ☐ запись информации о пользователе;
- ☐ отсутствие возможности использования протокола IPSec;
- ☐ цена.

### 3.2.3. HideMyAss (HMA)

Штаб-квартира этого сервиса<sup>1</sup> находится в Англии, но точки присутствия есть в 61 стране мира (всего насчитывается 448 серверов).

Сервис предоставляет огромное число дополнительных сервисов, однако описание большинства из них не соответствует тому, что указано на сайте. Стоимость же услуг зашкаливает: за один месяц нужно заплатить 11,99\$, за год цена более приятная: 83,88\$ (или 6,99\$ в месяц). Тестового периода нет, но есть гарантия возврата средств в течение 30 дней с момента оплаты. Как и у VPN Shield, в одном аккаунте могут находиться до 5 устройств. Ни трафик, ни пропускная полоса не ограничиваются.

Есть поддержка протоколов L2TP, OpenVPN, PPTP (IPSec не поддерживается). Сервис рекомендует использовать протокол OpenVPN.

Недостатки у этого сервиса тоже есть, и существенные. Сервис собирает много информации о деятельности пользователя и хранит информацию два года. Так что название сервиса не совсем соответствует действительности. Также нет возможности использования протокола IPSec и нет клиентов для Android.

### 3.2.4. Private Internet Access

Private Internet Access<sup>2</sup> — один из старейших VPN-сервисов, предоставляющих услуги анонимизации в сети. Кроме привычных услуг: анонимизация, обеспечение конфиденциальности, шифрование — предоставляют защиту от изменения DNS-серверов (DNS leak protection). Также у пользователя есть возможность использовать до трех устройств одновременно.

---

<sup>1</sup> См. <https://hidemyass.com/>.

<sup>2</sup> См. <https://privateinternetaccess.com/>.

Первое, на что пользователи обращают внимание при выборе VPN-сервиса (да и всего прочего в большинстве случаев), — это тарифные планы. Стоимость за месяц составляет 9,95\$, при оплате за год стоимость одного месяца составит 5,99\$ (71,88\$ за год).

Все тарифные планы предоставляют одинаковые сервисы и возможность использовать различные типы подключений (OpenVPN, PPTP и IPSec), неограниченный трафик (т. е. 9,95\$ — это окончательная стоимость, больше ни за что платить не нужно) и возможность выбрать шлюз в любой стране, где работает сервис, а именно: США, Великобритания, Германия, Канада, Франция, Швеция, Швейцария, Нидерланды, Гонконг (Китайская Народная Республика), Румыния и др. Всего в список входят 32 страны (на момент написания этих строк).

Сервис предоставляет бесплатный тестовый доступ сроком на 7 дней. Также есть гарантированный возврат денег в течение 7 дней, если вам что-то не понравится.

Техническая поддержка осуществляется по e-mail и через чат сайта. На самом же сайте есть весьма обширный список часто задаваемых вопросов.

Конечно, как у всего на свете, у этого сервиса есть недостатки:

- ☐ не предоставляется информация о загруженности каналов передачи данных и серверов. Выбирая сервер, вы не знаете, насколько быстрым он будет;
- ☐ если пользователь нарушит авторские права, информация о нем будет отправлена непосредственно правообладателю (акт Digital Millennium Copyright Act).

### 3.2.5. StrongVPN

Сервис StrongVPN<sup>1</sup> тоже родом из США. Является одним из первых провайдеров, предоставляющих услуги шифрования передаваемой информации.

На сайте сервиса вы найдете много разных и достаточно гибких тарифных планов и огромное количество документации, с помощью которой вы настроите любое устройство, поддерживающее VPN.

Тарифных планов всего два: или по 10 долларов каждый месяц, или 69,99\$ за год (по 5,83\$ в месяц).

Тестового периода нет, но компания гарантирует возврат денег (moneyback), если у вас не получилось настроить или использовать VPN-подключение в течение 7 дней, независимо от выбранного тарифного плана.

Как и в предыдущем случае, можно использовать протоколы OpenVPN, L2TP/IPSec и PPTP. Если что-то не получится, к вашим услугам круглосуточная поддержка (в чате, по e-mail, по телефону и Skype). Да, поддержка, как и в предыдущем случае, осуществляется на английском языке.

Огромный недостаток этого сервиса — то, что он полностью работает в рамках законов США, т. е. компания сохраняет всю информацию о пользователе, включая журналы доступа, персональную информацию, время подключения и даже ваш

---

<sup>1</sup> См. <https://strongvpn.com/>.

IP-адрес в вашей внутренней сети за вашим маршрутизатором. Если вам нужна анонимность и конфиденциальность, то это явно не ваш выбор.

### 3.2.6. ExpressVPN

Молодой VPN-провайдер<sup>1</sup> с весьма высокими ценами. За один месяц нужно отдать 12,95\$ или 99,95\$ за один год. Компания гарантирует возврат денег в течение 30 дней, если у вас возникли проблемы с использованием сервиса.

Точек присутствия достаточно: 160 мест в 94 странах мира. Пользователь может выбрать любой из сервисов и переключаться между ними. Скорость и трафик не ограничиваются.

К достоинствам этого сервиса можно отнести удобное программное обеспечение для Windows, Linux, macOS и, конечно же, Android. Поддерживаются только протоколы PPTP и OpenVPN.

Недостатки:

- ☐ много негативных отзывов о службе технической поддержки сервиса от пользователей в Интернете;
- ☐ нет поддержки протоколов L2TP и IPSec;
- ☐ компания хранит много информации о пользователе, которая может быть передана третьим лицам в соответствии с законодательством США.

### 3.2.7. SecurityKISS

Еще один VPN-сервис<sup>2</sup> с очень умеренными ценами. Есть даже бесплатный тарифный план GREEN. Пока что это самый дешевый VPN-сервис.

Множество тарифных планов<sup>3</sup> позволяют оптимизировать ваши расходы. Так, цена тарифа OLIVINE за год составит всего 23,9 евро — такой цены нет ни у одного из сервисов. Кроме того, вы можете пользоваться бесплатным планом GREEN, но будете ограничены всего 300 мегабайтами в сутки. Все зависит от того, зачем вам VPN. Если нет необходимости пользоваться VPN постоянно и шифровать весь свой трафик, бесплатный тарифный план вполне сгодится. Например, вы находитесь в стране, где заблокирован нужный вам ресурс. Зайти на этот ресурс и прочитать последние новости — для этого вполне достаточно 300 Мбайт в сутки. Этого хватит даже, чтобы опубликовать какую-нибудь статью в блоге (если вы желаете сохранить анонимность).

Конечно, есть и подвох. Как же без него... Во всех тарифных планах, кроме EMERALD, есть ограничение по трафику. Например, в том же OLIVINE ограничение составляет 20 Гбайт в месяц (или около 660 Мбайт в день). Также в этом

---

<sup>1</sup> См. <https://www.express-vpn.com/>.

<sup>2</sup> См. <https://www.securitykiss.com/>.

<sup>3</sup> См. <https://www.securitykiss.com/pricing/>.

тарифном плане не поддерживается работа почтовых программ (закрыты необходимые порты), поэтому почту читать придется только через веб-интерфейс. Если хочется работать с привычными программами, то нужно выбирать план MALACHITE, который стоит дороже, но тоже не заоблачно: или 3,99 евро в месяц, или 35,9 евро в год (получится по 2,99 евро в месяц). При этом вы получите 30 Гбайт трафика в месяц. Самый дорогой — безлимитный — тариф EMERALD обойдется в 89,90 евро в год, но это все равно дешевле, чем у некоторых других провайдеров.

Не всем нужны безлимитные тарифные планы, поэтому тарифы от SecurityKISS позволяют экономить.

К преимуществам этого сервиса можно отнести то, что компания не хранит никакой личной информации, а также не собирает какой-либо финансовой информации вроде номеров кредитных карт. Однако сервис фиксирует время и длительность VPN-сессии, используемую пропускную полосу, а также IP-адрес пользователя. Эта информация ему нужна для генерирования статистики. Журналы автоматически удаляются через 10 дней.

Имеются клиенты для Windows, macOS, iOS, Linux, Android.

Преимущества:

- ☐ экономичные тарифы;
- ☐ наличие бесплатного тарифного плана;
- ☐ поддержка популярных операционных систем;
- ☐ не собирается информация о пользователе.

Недостатки:

- ☐ в одном аккаунте может быть только одно устройство. Исключение: тарифы JADEITE и EMERALD — там можно один аккаунт использовать на нескольких устройствах;
- ☐ во всех тарифах (кроме EMERALD) есть ограничение по трафику и ряд других, с которыми можно ознакомиться на страничке с тарифами (см. ранее ссылку).

### 3.3. Организация VPN-соединения

Для упрощения настройки все VPN-сервисы предоставляют собственные VPN-клиенты. Все, что вам нужно сделать — это установить клиент, запустить его, выбрать сервер и подключиться. Не нужно настраивать операционную систему: ни компьютера, ни смартфона. После этого весь трафик всех программ будет направлен по VPN-туннелю. Поэтому VPN-соединение может защитить трафик всех программ, даже если они не поддерживают установку сетевых параметров (адрес прокси и его порт) — в отличие от Tor, где нужно настраивать каждую программу отдельно.

На рис. 3.1 показан VPN-клиент от SecurityKISS. Все, что нужно сделать — это нажать кнопку **Connect**. Кнопка в нижнем правом углу (с изображением серверов) позволяет выбрать другой сервер. На рис. 3.2 показано, что соединение установлено (обратите внимание на внешний IP-адрес).



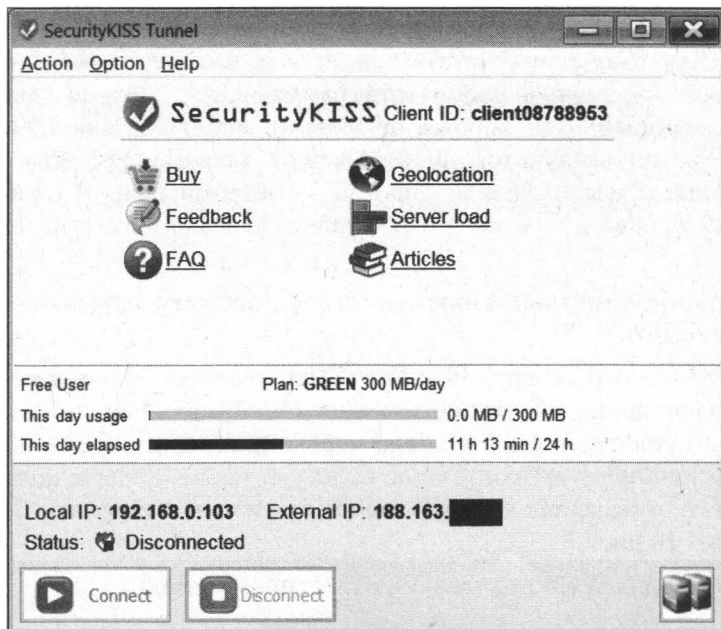


Рис. 3.1. VPN-клиент от SecurityKISS

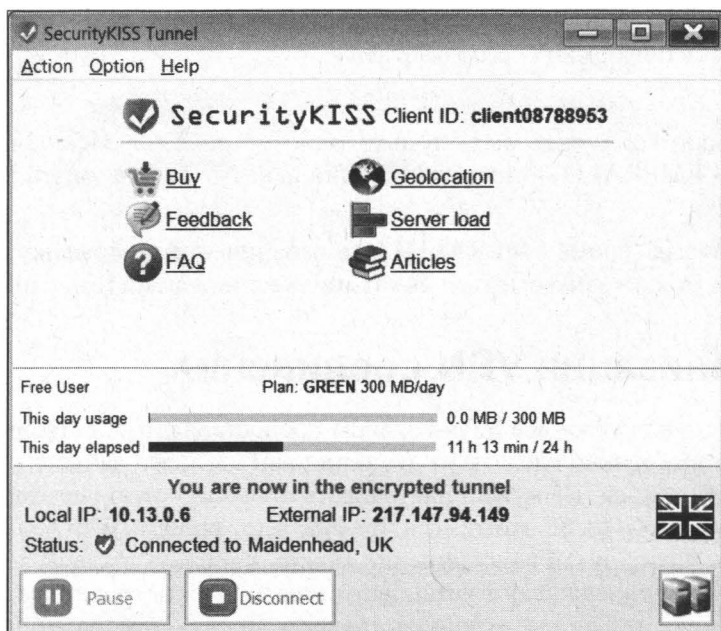


Рис. 3.2. VPN-соединение установлено

## 3.4. Opera VPN: осторожно!

В браузер Орега уже встроен бесплатный VPN-сервис. Для его активации нужно сначала включить VPN в разделе **Дополнительно** настроек браузера (рис. 3.3), а затем использовать переключатель VPN слева от адресной строки (рис. 3.4) для включения/выключения VPN-сервиса (см. также *разд. 2.4.4*).

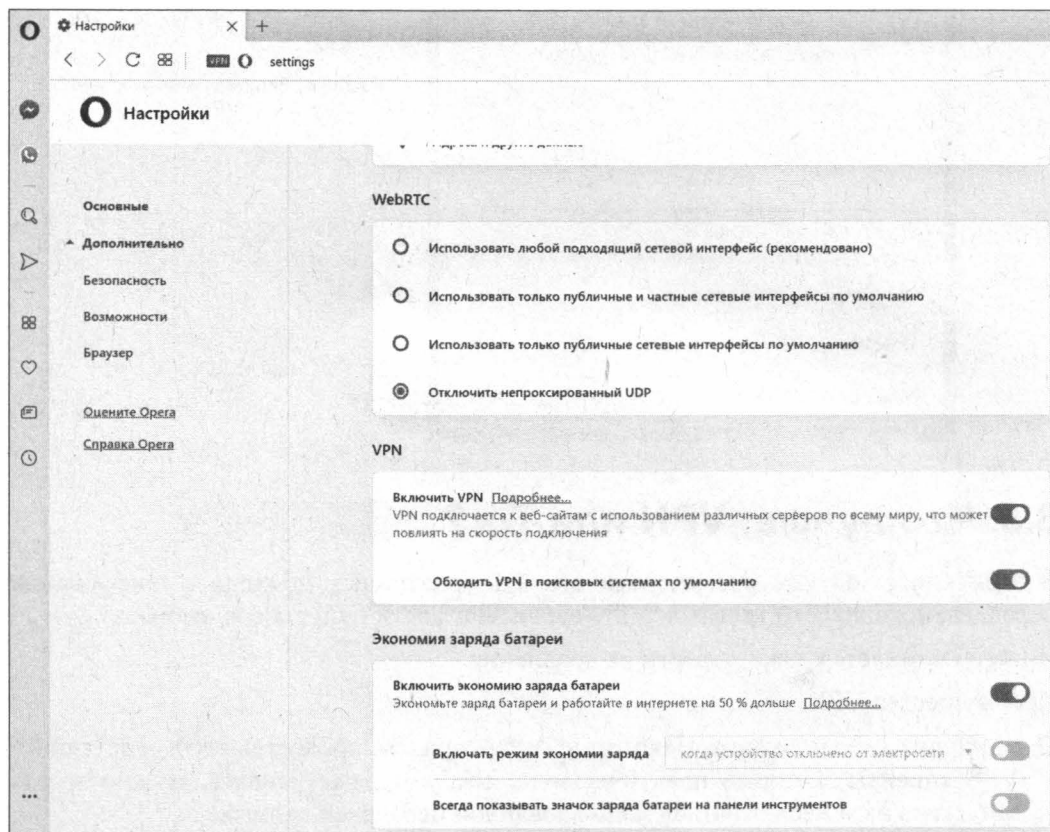


Рис. 3.3. Настройки Орега: включение возможности использования VPN

Однако сразу предупреждаю — это не полноценный VPN-сервис, а всего лишь прокси. Подробнее вы можете прочитать об этом по адресу: <https://xakep.ru/2016/04/25/opera-vpn-proxy/>. Поэтому ни о какой безопасности и анонимности при использовании штатного VPN браузера Орега речи быть не может. Им стоит воспользоваться, только если нужно открыть заблокированный на работе или в стране пребывания ресурс. На этом все. Кроме того, у этого сервиса есть ограничения по размеру загружаемых файлов — мне не удавалось скачивать через этот сервис файлы больше 65 Мбайт.

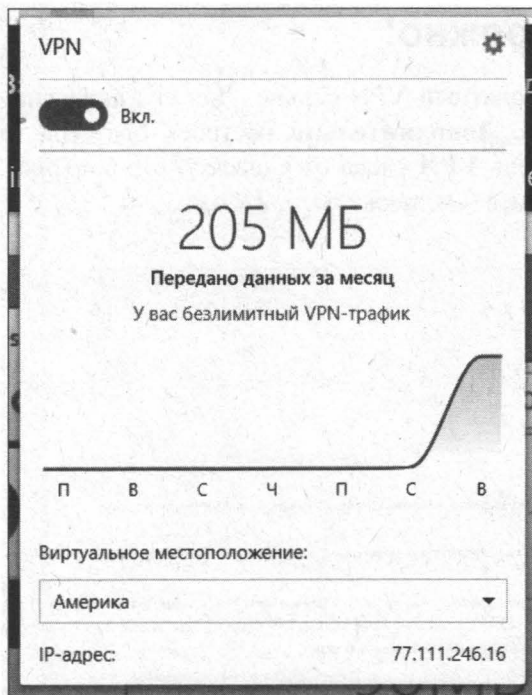


Рис. 3.4. Включение/выключение VPN

### 3.5. Что лучше: VPN или Tor?

В этой книге мы уже рассмотрели два альтернативных подхода к шифрованию передаваемого по сети трафика: VPN-сервисы и Tor. Какой способ выбрать?

Ничего не остается, как провести их сравнение.

Преимущества VPN:

- ❑ *удобство использования.* Некоторые VPN-сервисы предоставляют собственные VPN-клиенты, которые практически не требуется настраивать. Нужно только запустить их и наслаждаться зашифрованной передачей данных;
- ❑ *весь трафик, генерируемый вашим устройством, шифруется.* При этом вам не нужны права root, если ваше устройство является Android-смартфоном. В случае же с Tor для запуска прозрачной проксификации потребуются права root. В противном случае шифроваться станет трафик только тех приложений, которые поддерживают браузер Orbot, трафик остальных приложений шифроваться не будет;
- ❑ *высокая скорость доступа.* Скорость доступа к Интернету через VPN-сервис хоть и окажется немного ниже, чем скорость обычного доступа в Интернет, но все же останется на весьма высоком уровне.

На этом преимущества VPN-сервисов заканчиваются и начинаются недостатки:

- ❑ *доступ к VPN-серверам платный, и не всегда предоставляется тестовый доступ:* утром — деньги, вечером — стулья;

- ❑ часто вся ваша активность протоколируется и хранится на серверах VPN-сервиса несколько лет. Выводы делайте сами. По сути, это и есть самый значительный недостаток коммерческих VPN-сервисов;
- ❑ российские и украинские VPN-серверы из соображений конфиденциальности данных использовать вообще нельзя — при малейшем подозрении вся информация о вас будет передана, куда следует. Поэтому в этой главе рассматриваются только зарубежные серверы. Они хоть и тоже не образец конфиденциальности, но даже если кто-то сильно захочет узнать, что вы делали в Интернете и кому что передавали, международная бюрократия даст вам огромную фору во времени.

Теперь рассмотрим преимущества Тор:

- ❑ самое главное преимущество сети Тор — что это свободный проект, узлами сети Тор выступают машины энтузиастов, и никакая информация о вашей активности не записывается. К тому же каждый следующий узел в цепочке Тор не знает о вас ничего, кроме того, что данные пришли с предыдущего узла. Проследить цепочки Тор очень сложно с технической точки зрения;
- ❑ при включенной прозрачной проксификации через Тор могут работать любые сетевые приложения;
- ❑ сеть Тор абсолютно бесплатная — вы реально ни за что не платите;
- ❑ огромный выбор точек присутствия — в каждой стране есть узлы Тор, и вы можете выбрать выходной узел с любым нужным вам IP-адресом.

Недостатки у Тор тоже есть:

- ❑ не очень высокая скорость доступа. Впрочем, с каждым годом ситуация становится лучше, т. к. увеличивается пропускная способность каждого Тор-узла;
- ❑ чтобы заработала прозрачная проксификация на Android-устройствах, нужны права root, а их получение не всегда оправданно. Без прав root с сервисом Orbot (через Тор) будут работать только определенные приложения, «заточенные» под Тор, а таковых совсем мало. Однако если вам нужен только интернет-браузер, то установкой браузера Orweb эта проблема практически снимается.

Учитывая все сказанное, оптимальный выбор — Тор, даже несмотря на некоторые проблемы с прозрачной проксификацией. Окончательное слово, конечно же, за вами. Также нужно учитывать, какие цели вы преследуете. Если анонимность, то я бы рекомендовал использовать Тор. Если защита трафика, то проще использовать VPN-сервис.



## ГЛАВА 4



# Воображаемая безопасность: выбираем безопасный мессенджер

Разработчики всех мессенджеров в один голос заявляют о полной безопасности — мол, их продукты надежны, как сейф в швейцарском банке. Но так ли это? Какой мессенджер можно считать безопасным от перехвата информации посторонними, а какой подходит и для анонимного общения? Попробуем разобраться. В этой главе мы рассмотрим различные мессенджеры и попытаемся понять, какой из них более защищен.

Наш обзор популярных средств обмена сообщениями сделан с упором именно на их безопасность, и углубляться в техническую сторону мы будем ровно настолько, насколько это необходимо для «стандартного» пользователя. Рассмотрены будут как популярные, так и перспективные мессенджеры. А если вам потребуется дополнительная информация, ищите аналитику от Secure Messaging Scorecard на сайте Electronic Frontier Foundation.

## 4.1. Критерии оценки

Прежде всего нужно определиться с критериями оценки программных продуктов, чтобы было проще их сравнивать. Пусть это будут:

- ☐ открытость;
- ☐ централизация;
- ☐ анонимность;
- ☐ E2EE (End-to-End-Encryption, сквозное шифрование);
- ☐ синхронизация E2EE;
- ☐ проверка отпечатков;
- ☐ запрет на скриншоты;
- ☐ групповые E2EE-чаты;
- ☐ уведомление о проверке отпечатков в групповых E2EE-чатах;
- ☐ защита социального графа.

Теперь рассмотрим вкратце каждый из этих критериев. И начнем с первого.

□ Критерий *открытости* включает в себя несколько факторов:

- общедоступны ли исходные коды;
- если да, то учитывается ли степень взаимодействия с сообществом, ведется ли разработка открытым методом, принимаются ли pull request'ы (запросы к управляющему их репозиторию на применение изменений), наличие активности в репозитории и т. п.

□ По степени *централизации* все мессенджеры можно разделить на следующие группы:

- централизованный — требуется сервер, который возможно заблокировать. Примеры: VK, Telegram, Facebook;
- федеративный — сеть из серверов, общающихся друг с другом. Примеры: Email, Jabber (XMPP), Riot Matrix;
- децентрализованный (имеется в виду P2P) — каждый клиент является одновременно и сервером.

□ Для нас также важна возможность *анонимной* регистрации и использования. Это и есть наш третий критерий. В некоторых сервисах телефон может понадобиться только для защиты от спама при регистрации — в таком случае очень просто использовать для регистрации сервисы аренды номеров для получения SMS.

Во многих остальных сервисах необходимым требованием регистрации является номер зарегистрированного на вас мобильного телефона (смартфона). Это плохо, потому что несанкционированный доступ злоумышленника к этому смартфону без включенной двухфакторной аутентификации дает ему возможность зайти в аккаунт и слить все ваши данные. Разумеется, при этом теряется всякая анонимность. Таким образом, поскольку SIM-карты с номерами выдаются только по паспорту, мы и имеем регистрацию в сервисе по паспорту (ориентируемся на реалии РФ, других не завезли).

Впрочем, есть мессенджеры, позволяющие регистрироваться с использованием почтового ящика или учетной записи в социальной сети. Есть и такие, где учетную запись можно создать в самом мессенджере без привязки к чему бы то ни было еще.

□ E2EE (End-to-End Encryption) — это не что иное, как *сквозное шифрование*. Вы будете удивлены, но даже в наше время есть мессенджеры, не поддерживающие эту функцию или поддерживающие ее частично (например, только для частных чатов). Еще больше вы будете удивлены, когда узнаете, что это за мессенджеры.

□ Следующий критерий — *синхронизация E2EE-чатов*. Не все мессенджеры имеют такую функцию, и ее отсутствие может доставлять неудобства. С другой стороны, отсутствие этой функции можно расценивать как положительное явление. Вы только представьте, что кто-то запустит Viber, установленный на вашем

компьютере (разумеется, во время вашего отсутствия), — он сможет читать все сообщения, по крайней мере новые, которые будут получены с момента запуска Viber на этом компьютере. Функция защиты Viber паролем появилась буквально на днях, и не все ее успели включить. Проверьте, включили ли вы ее — без этого безопасно использовать Viber невозможно (рис. 4.1).

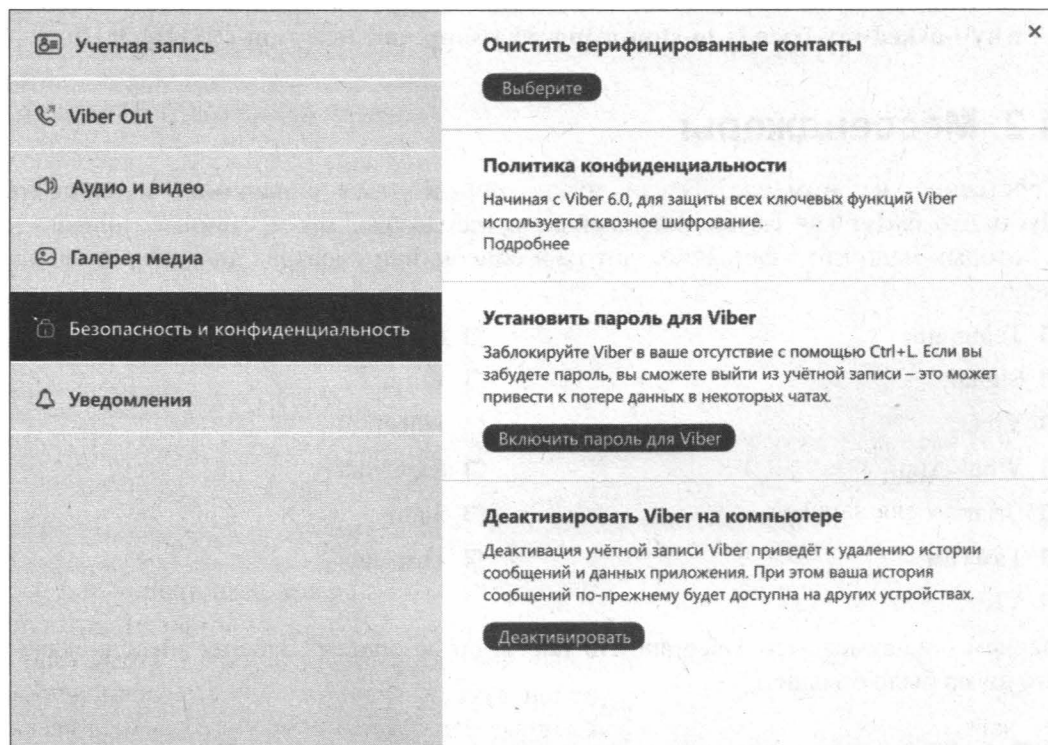


Рис. 4.1. Настройки Viber

- ❑ При запуске E2EE-чатов некоторые мессенджеры предлагают проверить *отпечатки* собеседников, другие не предлагают этого напрямую, но возможность такая существует. Однако не все мессенджеры вообще имеют функцию проверки отпечатков. Поэтому ее наличие становится еще одним критерием оценки защищенности мессенджера.
- ❑ Некоторые мессенджеры запрещают делать *скриншот* секретного чата. Функция не самая полезная, поскольку для обхода запрета достаточно иметь под рукой второй смартфон с камерой.
- ❑ Следующий критерий — *групповые E2EE-чаты*. Не такая уж необходимая функция, но весьма удобная. Правило «больше двух — говори вслух» стоит оставить в далеком детстве.
- ❑ Однако, если групповые зашифрованные чаты возможны, было бы неплохо иметь и *уведомление о необходимости проверки отпечатков E2EE* в таких чатах. При добавлении в секретный групповой чат нового собеседника, у которого



не сверены отпечатки, проверить его отпечатки предлагают не все мессенджеры. Из-за такого упущения теряется смысл секретных чатов.

- ❑ Некоторые мессенджеры собирают информацию о контактах пользователя и другую метаинформацию — например, кому звонил пользователь, как долго разговаривал (*социальный граф*). Заинтересовавшиеся читатели могут получить дополнительную информацию по ссылке: <https://medium.freecodecamp.org/why-i-asked-my-friends-to-stop-using-whatsapp-and-telegram-e93346b3c1f0>.

## 4.2. Мессенджеры

Собственно, на этом все. Теперь нужно определиться с нашими кандидатами. Пусть это будут как самые популярные мессенджеры, так и «темные лошадки», о которых мало кто знает. Итак, вот наш список, или «чертова дюжина» мессенджеров:

- |             |                       |
|-------------|-----------------------|
| ❑ Telegram; | ❑ Facebook Messenger; |
| ❑ Signal;   | ❑ Wire;               |
| ❑ Viber;    | ❑ Jabber;             |
| ❑ WhatsApp; | ❑ Riot Matrix;        |
| ❑ Briar;    | ❑ Status;             |
| ❑ ТамТам;   | ❑ Threema.            |
| ❑ VK;       |                       |

Начнем с на шумевшего Telegram. Но так ли он безопасен? Забегая вперед, скажу, что шума было больше...

### 4.2.1. Telegram

Мессенджер от Павла Дурова, построен на технологии шифрования переписки MTProto. В настоящее время заблокирован на территории России, хотя блокировку с успехом можно обойти с помощью всевозможных бесплатных прокси, при этом будут работать не только текстовые чаты, но и голосовые звонки.

Позиционируется как «опенсурсный». Исходники доступны по адресу: <https://tigrm.ru/sources>, движение в репозиториях за последние дни наблюдается, и это хорошо. Было бы плохо, если бы исходники как бы были, но изменений в них не производилось бы, тогда как обновления программы осуществлялись. Впрочем, год назад с Telegram была именно такая ситуация.

По степени централизации Telegram — мессенджер централизованный. С одной стороны, это не хорошо. С другой, полностью заблокировать его так и не вышло. Но это не заслуга централизации, а следствие работы через прокси.

К минусам Telegram однозначно относим отсутствие возможности анонимной регистрации. Кроме того, E2EE (сквозное шифрование) включается только в секретных чатах, а обычные по умолчанию не шифруются. Вы только вдумайтесь —

обычные чаты в Telegram не шифруются вообще! Именно поэтому некоторые Telegram-боты за определенную плату могут деанонимизировать пользователя по его сообщению, т. е. сообщить номер телефона этого пользователя.

Синхронизации E2EE-чатов нет, т. е. секретный чат можно использовать только с одного устройства, доступа с другого к нему уже не будет. Впрочем, это не преимущество, но и не недостаток. Просто особенность мессенджера, о которой нужно знать.

Telegram не уведомляет пользователей о необходимости проверки отпечатков E2EE. Но пользователи сами могут зайти в настройки для сравнения отпечатков (рис. 4.2).

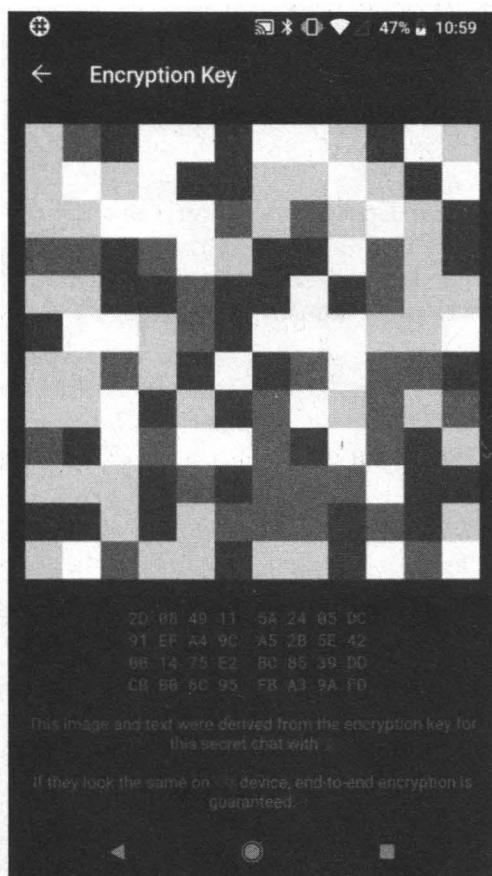


Рис. 4.2. Проверка отпечатков в Telegram

Функция запрета скриншота есть, но работает она не на каждом устройстве. Нет также у этого мессенджера ни групповых E2EE-чатов, ни защиты социального графа.

В общем, мессенджер неоднозначный. Вокруг него много шума, а в сухом остатке не понимаешь, ради чего: доступа к исходникам — практически нет, чаты по умолчанию не шифруются, нет защиты социального графа (все ваши контакты хранятся

на серверах Telegram), сообщения также хранятся на сервере (причем, как уже было отмечено, в незашифрованном виде), нет групповых E2EE-чатов, E2EE-чаты в настольной версии программы не поддерживаются — только в мобильной, мессенджер централизованный и при всем этом отсутствует возможность анонимной регистрации. Из-за чего шум-то, господа? Шум вокруг этого мессенджера больше напоминает тщательно спланированную PR-акцию.

Если вы хотите использовать Telegram, то пользуйтесь хотя бы секретными чатами. Для создания секретного чата в меню мобильной версии нужно выбрать команду **New Secret Chat**. В секретном чате сообщения шифруются и не хранятся на серверах мессенджера. Также нельзя сделать скриншот секретного чата, но ничто не мешает сделать его фотографию другим смартфоном.

Напомню, что настольная версия секретные чаты не поддерживает, следовательно, ни о какой синхронизации секретных чатов между мобильной и настольной версиями речи быть не может.

## 4.2.2. Signal

Продукт Open Whisper Systems (некоммерческой организации разработчиков открытого программного обеспечения). Исходный код доступен, и любой желающий может с ним ознакомиться<sup>1</sup>. Мессенджер децентрализованный, а значит, должен быть более надежен, чем централизованные варианты.

Signal не поддерживает анонимное использование, так что кроме регистрации по номеру телефона других вариантов нет. Хотя не анонимно, зато относительно безопасно, поскольку он поддерживает E2EE, синхронизацию E2EE-чатов и групповые E2EE-чаты.

Уведомления о необходимости проверки отпечатков E2EE нет — пользователям предлагается сканировать QR-коды друг друга и сравнить отпечатки. Также нет уведомления о необходимости проверки отпечатков в групповых чатах.

Есть защита социального графа, а функция запрета скриншота включается и выключается в настройках.

Для шифрования используется Signal Protocol (<https://signal.org/docs/>) — специально разработанный для этого мессенджера криптографический протокол, на основе которого может осуществляться сквозное (End-to-End) шифрование звонков (голосовых и видео), а также обычных сообщений. На основе Signal Protocol работают и другие мессенджеры: WhatsApp, Facebook Messenger, Google Allo.

Казалось бы, если Facebook Messenger и Google Allo используют этот же протокол, то они так же безопасны, как и Signal. Но, как показывает практика, — нет. В отличие от Signal, где шифрование включено по умолчанию, в этих мессенджерах оно выключено, и его надо включать вручную. Так, чтобы шифрование осуществлялось в Facebook Messenger, нужно включить опцию **Secret Conversations**, а в Google Allo — режим инкогнито **Incognito Mode**.

---

<sup>1</sup> См. <https://github.com/signalapp>.

На первый взгляд, мессенджер Signal достаточно безопасен. Во-первых, он децентрализованный, во-вторых, его исходный код открыт всем интересующимся, есть поддержка групповых E2EE-чатов, есть защита социального графа, поддерживаются исчезающие по таймеру сообщения (<https://signal.org/blog/disappearing-messages/>). Однако этот мессенджер не является анонимным — при регистрации нужно указывать номер телефона, к которому мессенджер и привязывается.

Что же касается исчезающих сообщений, то это «фишка» не только этого мессенджера. Подобное решение есть и в Telegram (в меню секретного чата нужно выбрать команду *Set self-destruct timer*), и в Viber.

### 4.2.3. Viber

Мессенджер для отправки бесплатных сообщений через сеть Wi-Fi или мобильные сети. Сообщения шифруются по протоколу, использующему ту же концепцию, что и Signal Protocol.

Пройдемся по порядку по нашим критериям:

- ☐ открытость — проприетарный (т. е. исходный код недоступен). Однозначно минус;
- ☐ степень централизации — централизованный;
- ☐ анонимности — нет: привязывается к номеру телефона;
- ☐ E2EE — включено по умолчанию, кроме того, есть секретные и скрытые чаты, обеспечивающие дополнительную безопасность;
- ☐ синхронизации E2EE-чатов — нет: созданный в мобильной версии секретный чат не отобразится в настольной версии. Для защиты от чтения посторонним обычных чатов предлагается установить пароль (см. рис. 4.1), чтобы ваши сообщения нельзя было прочитать с компьютера без вашего ведома;
- ☐ уведомление о необходимости проверки отпечатков E2EE — для проверки отпечатков предлагается совершить звонок собеседнику, сообщить свой идентификатор, после чего подтвердить его корректность, но уведомления о необходимости в этом для обеспечения собственной безопасности нет;
- ☐ запрет скриншота секретного чата — есть;
- ☐ групповые E2EE-чаты — есть;
- ☐ уведомления о необходимости проверки отпечатков E2EE в групповых чатах — нет;
- ☐ защиты социального графа — нет.

Viber — мессенджер интересный... С одной стороны, он проприетарный, централизованный, привязывается только к номеру телефона, не обеспечивает защиту социального графа. С другой стороны, сквозное шифрование (<https://bit.ly/2I64GhI>) включено по умолчанию, даже в настольной версии, а для дополнительной безопасности предназначены секретные чаты. Также поддерживаются групповые E2EE-чаты.

Секретные чаты позволяют настроить таймер самоуничтожения для каждого сообщения — сообщение будет удалено через установленное время после просмотра: как с вашего устройства, так и со всех устройств его получателей. Сообщения секретного чата защищены от пересылки, а скриншоты или выключены, или оставляют уведомление на экране чата.

Для перехода в секретный чат нужно открыть чат с пользователем и выбрать из его меню команду **Перейти в секретный чат**. Секретный чат будет отмечен замком.

Кроме секретных чатов, Viber поддерживает скрытые чаты, позволяющие не отображать выбранные чаты на экране чатов в приложении. Чтобы получить доступ к скрытому чату, нужно ввести установленный ранее PIN-код. Это дополнительная защита на тот случай, если смартфон попадет в чужие руки.

## 4.2.4. WhatsApp

Мессенджер для обмена разного рода сообщениями. С 2016 года используется шифрование сообщений по протоколу Signal Protocol.

Очень похож на Viber: проприетарный, централизованный, привязывается к номеру телефона, E2EE включено по умолчанию, есть синхронизация E2EE-чатов, есть уведомление о необходимости проверки отпечатков E2EE — правда, только в случае смены ключа собеседником. Чтобы уведомление пришло, необходимо зайти в настройки и включить эту функцию. А при старте чата никаких уведомлений нет. Уведомления от необходимости проверки отпечатков в групповых чатах нет, зато сами групповые E2EE-чаты поддерживаются. Нет защиты социального графа и нет запрета создания скриншота.

Как уже было отмечено, WhatsApp использует Signal Protocol. Означает ли это, что он такой же безопасный, как и Signal? Давайте посмотрим.

Конечно, этот мессенджер интересен тем, что *не хранит ваши сообщения* на своих серверах. Вместо этого сообщения хранятся на вашем телефоне. Однако при бэкапе они сохраняются на других серверах, причем уже без шифрования. Например, если у вас iPhone, то при бэкапе телефона сообщения WhatsApp будут помещены в iCloud вместе с другими данными.

Основная проблема WhatsApp в том, что он собирает всевозможную информацию о вас — так называемые *метаданные*, в том числе все телефонные номера из вашей адресной книги. WhatsApp также записывает, кому и когда вы писали, кому и во сколько звонили, сколько длился разговор, но сам разговор не записывается. Например, в 2:30 вы звонили в «секс по телефону» и ваш разговор длился 24 минуты. Согласитесь, никто «не догадается», о чем был разговор, — ведь сам разговор не записан.

Кроме того, WhatsApp собирает тонны и другой информации о пользователе: модель его смартфона, его ОС, информацию, полученную от браузера, IP-адрес, мобильный номер и т. п.

Спасает WhatsApp лишь то, что E2EE-чаты используются по умолчанию, и есть возможность групповых зашифрованных чатов.

Учитывая все сказанное и то, что мессенджер является проприетарным с закрытым кодом, выглядит это не очень хорошо. Если хотите анонимности, лучше не устанавливать его на свой смартфон. Может, никто и не перехватит ваши сообщения, но сам мессенджер будет знать о вас все.

## 4.2.5. Briar

Мессенджер Briar основан на технологии децентрализованных сетей (mesh). Может работать через Bluetooth, Wi-Fi или через Интернет (Tor). По умолчанию предусмотрено окончное шифрование сообщений. О нем мало кто знает, но это даже к лучшему.

Исходный код Briar открыт<sup>1</sup>, мессенджер децентрализованный, есть возможность анонимной регистрации и использования. Сквозное шифрование включено по умолчанию, однако нет возможности синхронизации E2EE-чатов, поскольку сейчас не поддерживается использование одной и той же учетной записи на разных устройствах.

При добавлении контакта необходимо сканировать QR-код собеседника с экрана его смартфона, другого варианта добавить контакт нет, поэтому считаем, что уведомление о проверке отпечатков имеется.

Есть групповые E2EE-чаты. В групповой чат можно добавить только собеседника из тех, чьи QR-коды уже проверены, поэтому также считаем, что соответствующее уведомление имеется. Есть запрет на создание скриншота, и есть защита социального графа.

Briar — не очень популярный мессенджер, и я готов поспорить, что далеко не каждый пользователь знает о его существовании. Но на деле он очень хорош: может работать через Tor, децентрализованный с открытым исходным кодом, есть возможность анонимной регистрации и использования, а чаты шифруются по умолчанию, причем не хранятся на серверах Briar (т. е. ваши сообщения в зашифрованном виде хранятся только на вашем смартфоне). Есть защита социального графа (никто никому не сливает вашу адресную книгу), есть групповые E2EE-чаты, но нет синхронизации E2EE-чатов между устройствами, поскольку нет возможности использовать одну и ту же учетную запись на разных устройствах.

На фоне всех остальных мессенджеров Briar выглядит идеально, если нужна анонимность общения. Но у него есть и недостатки: нет версии для iPhone, нет возможности голосовых звонков. Если с отсутствием голосовых звонков еще можно мириться — не всем они нужны, то вот отсутствие версии для iPhone существенно ограничивает круг общения.

---

<sup>1</sup> См. <https://code.briarproject.org/akwizgran/briar/wikis/home>.

### 4.2.6. ТамТам

Разработан Mail.ru Group. Основной упор разработчиков был сделан на быстроту передачи сообщений и простоту использования, а не на безопасность.

Проприетарный, централизованный, отсутствует сквозное шифрование (E2EE). Да, возможна анонимная регистрация через почту Google или через социальную сеть «Одноклассники». Нет защиты социального графа.

При создании ТамТам никто не делал упор на безопасность, и это нужно учитывать при выборе этого мессенджера. Привлекает в нем то, что возможна регистрация при использовании Google-почты или через социальную сеть «Одноклассники». То есть анонимная регистрация без привязки к номеру телефона так возможна. Но, несмотря на это, шифрование сообщений не поддерживается (во всяком случае, разработчики нигде об этом не говорят), не производится защита социального графа. Другими словами, даже если пользователь анонимного регистрируется, по незашифрованным сообщениям все равно будет понятно, кто это. Так что этот мессенджер однозначно не подходит для анонимного и безопасного общения.

### 4.2.7. VK (ВКонтакте)

Еще одно детище Павла Дурова. Что тут можно сказать? — проприетарное решение, централизованное, регистрация только по номеру телефона, нет сквозного шифрования, нет защиты социального графа.

Думаю, мало кому в голову придет желание использовать «ВКонтакте» как средство для анонимного общения. Сообщения хранятся на серверах соцсети, не шифруются, регистрация только по номеру телефона — в общем, полный суповой набор. Однозначно не рекомендуется к использованию.

### 4.2.8. Facebook Messenger

Мессенджер от Facebook, построенный на базе открытого протокола MQTT (это протокол обмена сообщениями, не нужно путать его с протоколом шифрования). После его выхода была отключена возможность отправки сообщений в Facebook, что вынудило пользователей устанавливать это приложение. Но можно зарегистрироваться и не имея учетной записи в Facebook.

Если сравнивать «ВКонтакте» и Facebook Messenger, то Facebook на его фоне выглядит значительно лучше. Во-первых, есть возможность анонимной регистрации с использованием электронной почты. Во-вторых, поддерживаются E2EE-чаты, но не по умолчанию. Сквозное шифрование по умолчанию выключено, и чтобы сообщения стали шифроваться, надо включить опцию **Secret Conversations**.

Однако Facebook собирает очень много всевозможной информации о пользователе, поэтому вряд ли подойдет для безопасного общения. Проприетарный, централизованный. В нем не поддерживается синхронизация E2EE-чатов, нет уведомления о необходимости проверки отпечатков E2EE, нет групповых зашифрованных чатов,

нет запрета на создание скриншота секретного чата и нет защиты социального графа.

Если вам интересно, какую информацию собирает Facebook, прочитайте его политику конфиденциальности<sup>1</sup> или посмотрите на следующую картинку: [https://cdn-images-1.medium.com/max/1250/1\\*PaCqj-ah-7G0GyhHSimmxw.png](https://cdn-images-1.medium.com/max/1250/1*PaCqj-ah-7G0GyhHSimmxw.png).

#### 4.2.9. Wire

Передаваемые через этот мессенджер сообщения шифруются по протоколу Wire Swiss, основанному на Signal Protocol.

Мессенджер централизованный, но с открытым исходным кодом<sup>2</sup>. Поддерживается анонимная регистрация (достаточно указать адрес электронной почты), есть сквозное шифрование (включено по умолчанию), есть синхронизация E2EE-чатов, уведомления нет, но есть возможность проверки. Есть поддержка групповых E2EE-чатов. Если один из пользователей отправляет в секретный групповой чат сообщение с устройства, которое не верифицировано у другого пользователя, то, когда этот другой попытается отправить сообщение, перед ним появится предупреждение о том, что у первого новое устройство.

Адресная книга не хранится на серверах Wire, что хорошо. А вот функции запрета скриншота секретного чата нет, но это не принципиально.

Wire — претендент на звание победителя. Во-первых, есть возможность анонимной регистрации. Во-вторых, по умолчанию поддерживается сквозное (E2EE) шифрование, даже с возможностью синхронизации зашифрованных чатов. В-третьих, есть защита социального графа, поддерживаются групповые зашифрованные чаты (до 128 человек), безопасные конференц-звонки (до 10 человек), и есть возможность уведомления о необходимости проверки отпечатков E2EE. Что-то подобное мы видели в Briar, но здесь огромный выбор поддерживаемых платформ: Android, iOS, Windows, macOS, Linux. Должна быть ложка дегтя? Так и есть: мессенджер платный и стоит 6 евро в месяц. Если готовы платить за безопасность, это, пожалуй, неплохое решение.

#### 4.2.10. Jabber

А вот если за безопасность платить не хочется (хотя бы даже по той причине, чтобы не «светить» свою карточку), можно обратить свое внимание на Jabber. Да, пусть он не такой удобный, как Wire, и не поддерживает голосовые и видеозвонки, но он федеративный, поддерживает анонимную регистрацию, E2EE-шифрование (правда, понадобится установить OMEMO — расширение для открытого протокола XMPP), в том числе групповое. Конечно, возможности его слабоваты, но радует, что Jabber — это только сервис, а клиент можно выбрать любой: например, тот же

---

<sup>1</sup> См. <https://www.facebook.com/privacy/explanation>.

<sup>2</sup> См. <https://github.com/wireapp/wire>.



ChatSecure (поддерживает OMEMO) — для iOS, Conversations (также поддерживает OMEMO) — для Android, Pidgin — для Linux и т. п.

### 4.2.11. Riot Matrix

Клиент для обмена сообщениями, созданный на основе matrix-react-sdk. Его исходный код вполне доступен<sup>1</sup>. Федеративный, поддерживает анонимную регистрацию без привязки к номеру телефона или к почте. Есть E2EE, синхронизация зашифрованных чатов, есть даже уведомление о необходимости проверки отпечатков E2EE. Рядом с полем отправки сообщения есть значок замочка, когда он открыт — сообщения не шифруются, закрыт — шифруются. Это интуитивно понятно, поэтому засчитываю это как наличие уведомления.

Есть поддержка групповых зашифрованных чатов. Если в секретном групповом чате появится пользователь, чьи устройства не верифицированы другими пользователями, собеседники увидят сообщение об этом при попытке отправки сообщения.

Есть защита социального графа, но нет запрета на создание скриншота зашифрованного чата.

Это еще один малоизвестный мессенджер, поддерживающий защиту социального графа, с поддержкой групповых E2EE-чатов, синхронизацией E2EE-чатов и анонимной регистрацией без привязки к номеру телефона. Поддерживаются как Android, так и iOS, что расширяет аудиторию пользователей мессенджера.

### 4.2.12. Status

Это не просто мессенджер — это и браузер, и мессенджер, и кошелек Ethereum-валют. В нем можно общаться, анонимно посещать сайты, платить или обмениваться валютами на основе Ethereum.

Пройдемся по порядку по нашим критериям:

- ☐ открытость — исходный код доступен<sup>2</sup>;
- ☐ степень централизации — децентрализованный;
- ☐ анонимность — анонимный, не нужно указывать ни e-mail, ни номер телефона;
- ☐ E2EE — включено по умолчанию;
- ☐ синхронизация E2EE-чатов — есть;
- ☐ уведомление о необходимости проверки отпечатков E2EE — для добавления контакта нужно сканировать его QR-код или же ввести контакт-код. Считаем, что уведомление есть;
- ☐ запрета скриншота секретного чата — нет, т. к. нет такого понятия, как секретный чат. Поскольку есть возможность анонимной регистрации, и все сообщения

<sup>1</sup> См. [https://github.com/matrix-org/matrix.org/tree/master/jekyll/\\_posts/projects](https://github.com/matrix-org/matrix.org/tree/master/jekyll/_posts/projects).

<sup>2</sup> См. <https://github.com/status-im>.

шифруются по умолчанию, можно расценивать каждый Status-чат как секретный;

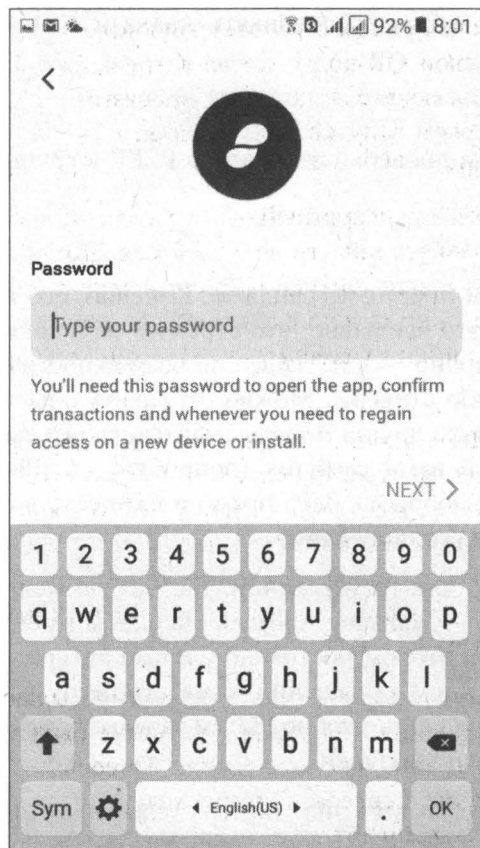
- ☐ групповых E2EE-чатов — нет;
- ☐ уведомления о необходимости проверки отпечатков E2EE в групповых чатах — нет;
- ☐ защита социального графа — есть.

Status — это нечто большее, чем просто мессенджер. Конечно, его можно использовать только для общения, но это все равно, что стрелять из пушки по воробьям. Да и общаться здесь не очень удобно — я не нашел ни возможности отправить картинку собеседнику, ни какие-либо стикеры. Можно отправить обычные смайлики, но если у собеседника кардинально другая модель смартфона, его смартфон может просто не понять отправленный вами смайлик (попробуйте с iPhone отправить смайлик на Samsung/Android и наоборот). Зато прямо в чате есть возможность отправить ETH и создать запрос на его получение.

Приложение пока находится на бета-тестировании. Да, без глюков пока никак — установил его на два смартфона — Samsung/Android. На одном из смартфонов приложение работало нормально, на втором постоянно слетала авторизация, и приходилось вводить пароль при каждом обращении к мессенджеру (считайте после каждой блокировки экрана), что не есть удобно. Затем забавная ситуация произошла с отображаемыми именами пользователей.

При регистрации не нужно указывать ни номер телефона, ни даже e-mail (рис. 4.3) — просто вводим пароль и указываем отображаемое имя, которое можно изменить при регистрации. Итак, я установил Status на два смартфона, выбрал отображаемые имена. Затем на втором смартфоне открыл QR-код, чтобы добавить второй контакт на первом. Но вместо введенного на втором смартфоне имени я получил совсем другое имя. И оно отображалось, пока я не добавил этот контакт (не нажал кнопку **Add a contact** в профиле пользователя). Может, так и задумывалось, но все равно странно — при том, что на втором телефоне имя, введенное на первом, отображалось изначально корректно.

С другой стороны — смотря, что и кому надо. Если вам нужна именно безопасность, то она здесь есть. Регистрация анонимная, сообщения все шифруются по умолчанию, так что каждый чат может расцениваться как секретный. Плохо, что сообщения хранятся и на смартфоне, и на сервере мессенджера, но они хранятся там по обещаниям разработчиков в зашифрованном виде. И ваша книга контактов не сливается на серверы мессенджера, что тоже дорогого стоит. Да, нет плюшек в виде стикеров, возможности обмена картинками, нет групповых чатов, нет таймера уничтожения чата. Если все это нужно, поищите другой мессенджер. Если же нет, то можно наслаждаться анонимным общением + анонимным переводом криптовалюты через этот мессенджер.



**Рис. 4.3. Регистрация в Status**

### 4.2.13. Threema

E2EE-мессенджер для iOS, Android и Windows Phone. Кроме текстового общения, пользователи могут совершать голосовые звонки, отправлять свое местоположение, голосовые сообщения и файлы. Поддерживает групповые чаты до 50 человек.

Проприетарный, централизованный, однако поддерживает возможность анонимной регистрации. Для регистрации не нужно указывать какие-либо данные, которые могут способствовать установлению личности: ни номер телефона, ни e-mail. При первом запуске программы случайным образом генерируется идентификатор пользователя (ID). Все это обеспечивает анонимность общения.

Поскольку для каждого устройства генерируется отдельный ID, при потере устройства вы теряете все данные. Поэтому желательно делать бэкапы. Бэкап понадобится и при смене устройства, поскольку никакого другого способа синхронизации нет.

Адресная книга по умолчанию не сливается на серверы, но при желании пользователь может предоставить мессенджеру доступ к своей адресной книге, чтобы был возможен поиск пользователей по номеру телефона.

Есть зашифрованные чаты, групповые зашифрованные чаты также есть. Threema использует три уровня доверия личности пользователя. Уровень проверки каждого

контакта отображается в виде точек рядом с соответствующим контактом. Пользователи также могут проверить свои QR-коды, когда встречаются физически. QR-код содержит открытый ключ пользователя, который привязывается к идентификатору, сгенерированному при первом запуске приложения, и не будет меняться во время всей жизни идентификатора.

Каждый чат может расцениваться как секретный — по умолчанию содержимое чата шифруется и хранится только на устройстве пользователя. Также есть приватные чаты, защищаемые PIN-кодом, т. е. для доступа к приватному чату надо будет ввести PIN-код. Такие чаты при желании можно скрыть из общего списка чатов. Приватные чаты помечены значком шпиона (шляпа и очки). Отдельной функции запрета скриншота нет как таковой.

Серверы Threema находятся в Швейцарии. Сообщения, как уже отмечалось, шифруются полностью и децентрализованным способом на устройствах пользователя, а не на серверах Threema. Способ шифрования зависит от устройства. В iOS используется функция iOS Data Protection, в Android и Windows Phone — AES-256. Шифруются сообщения, изображения и другие данные, передаваемые между пользователями. Дополнительная информация доступна здесь: [https://threema.ch/press-files/cryptography\\_whitepaper.pdf](https://threema.ch/press-files/cryptography_whitepaper.pdf).

Серверы Threema играют роль коммутатора — сообщения пересылаются через серверы, но не хранятся на них постоянно. Сообщения не могут быть расшифрованы по решению суда, т. к. хранятся только на смартфоне, и Threema не имеет доступа к секретным ключам пользователей. Серверы Threema знают только, кто отправляет сообщение и кому, но они не фиксируют эту информацию и не могут расшифровать содержимое сообщения. Подробно о том, какие данные хранятся и как долго, можно прочитать в FAQ (<https://threema.ch/en/faq>). Главное, что Threema, в отличие от того же WhatsApp, не регистрирует, кто и с кем общается, и не хранит адресную книгу пользователя на своих серверах.

Весьма неплохой мессенджер, но — платный. Бесплатной версии, увы, нет. Стоит он недорого — чуть менее 3 долларов (Android-версия). Казалось бы, идеальный мессенджер, да еще и недорогой. Но есть и ложка дегтя. Последние Android-версии приложения имеют проблемы с уведомлениями, которые попросту не отображаются, — т. е. вы не будете знать о новых сообщениях, и вам придется постоянно проверять их наличие путем запуска программы. Не очень удобно. С другой стороны, это явление временное и, думаю, скоро будет исправлено.

## 4.3. Заключение

Рекомендовать какой-либо мессенджер не стану. Книга дает лишь пищу для ума, а выводы уже пусть делает каждый для себя сам. Чтобы легче было сравнивать мессенджеры, представлю сравнительную таблицу (табл. 4.1).

Таблица 4.1. Сравнение мессенджеров

Мессенджер	Критерии									
	Открытость	Централизация	Анонимность	E2EE	Синхр. E2EE	Отпечатки	Запрет скринш.	Групповые E2EE	Увед. в групп. чатах	Защита соц. графа
Telegram	-	Центр.	-	По выбору	-	-	+	-	-	-
Signal	+	Центр.	-	+	+	-	+	+	-	+
Viber	-	Центр.	-	По выбору	-	-	+	+	-	-
WhatsApp	-	Центр.	-	+	+	-	-	+	-	-
Briar	+	Децент.	+	+	-	+	+	+	+	+
TamTam	-	Центр.	+	-	-	-	-	-	-	-
VK	-	Центр.	-	-	-	-	-	-	-	-
Facebook	-	Центр.	+	По выбору	-	-	-	-	-	-
Wire	+	Центр.	+	+	+	-	-	+	+	+
Jabber	+	Федер.	+	Плагин	+	-	-	+	-	-
Riot Matrix	+	Федер.	+	По выбору	+	+	-	+	+	+
Status	+	Децент.	+	+	Частично	+	-	-	-	+
Threema	-	Центр.	+	+	-	+	-	+	+	+

## ГЛАВА 5



# Анонимность в социальной сети

## 5.1. Нужна ли вам анонимность?

Социальные сети предназначены по большей части для виртуального общения с друзьями. Плохо, конечно, что в последнее время такое виртуальное общение вытесняет реальное, но не будем сейчас об этом.

Суть вопроса в заголовке этого раздела в том, что нужно ли обеспечивать анонимность, если вы собираетесь общаться со своими друзьями? Очевидно, что нет. Конечно, надо соблюдать определенную осторожность и не сообщать много личных данных о себе, особенно оставлять эти данные открытыми — когда их могут просмотреть не только ваши друзья, а все желающие.

Еще раз — если ваша цель — обычное общение, то анонимность соблюдать незачем. Просто себе общайтесь и, как и в обычной жизни, не говорите о себе лишнего. Чем меньше информации вы предоставите социальной сети, тем лучше. Имени и фамилии вполне достаточно, чтобы вас нашли ваши друзья и знакомые, а все остальное всем знать не обязательно.

В качестве примера рассмотрим вкладку **Информация** популярной сети Facebook. Там приводится следующая информация о пользователе:

- ☐ Места работы, учебы (вуз и школа), день рождения.
- ☐ Номер телефона и прочая контактная информация.
- ☐ Город проживания, пол.
- ☐ Семейное положение, информация о родственниках.
- ☐ События из жизни.

Теперь подумаем, нужно ли все это сообщать. Во-первых, как уже было отмечено, имя и фамилия. Пол и дату рождения — по своему желанию. Друзья и так знают, какого вы пола, и знают вашу дату рождения. Тем более, что дата рождения часто указывается при регистрации в других сервисах, и эта информация там служит для восстановления пароля. Так что задумайтесь, предоставлять ее здесь или нет.

То же самое касается и номера телефона. Сейчас мало в какой социальной сети можно зарегистрироваться, не указав номер телефона. Но показывать его всем нет никакой необходимости. Исключение — только бизнес-страницы, где указывается номер телефона компании.

Город проживания, семейное положение, места учебы — это все лишнее. Повторюсь, ваши друзья (кому нужно) и так все это знают, а тем, кто не знает, видимо, знать не обязательно.

События из жизни лучше не указывать вообще. Очень часто пользователи (хоть это и неправильно) указывают в качестве пароля даты — например, годовщины свадьбы, дату рождения ребенка и т. п. Всю эту информацию можно узнать на вкладке **События из жизни**.

Указывать ли любимые цитаты? Если хоть одну из них вы когда-либо использовали в качестве пароля к какому-либо из сервисов, — однозначно нет.

Если подытожить, то не нужно указывать никакую контактную и личную информацию. В настройках конфиденциальности выберите, чтобы список ваших друзей и ваши фотографии были доступны только вашим друзьям (список друзей можно вообще скрыть, чтобы он был доступен только вам).

А теперь попытаемся разобраться, зачем все же может быть нужна анонимность.

## 5.2. Зачем нужна анонимность в социальной сети?

На мой личный взгляд, анонимность нужна в двух случаях:

- ☐ когда вы заигрались в детектива и хотите анонимно посещать аккаунты других пользователей. Правда, касается это только «Одноклассников», поскольку другие сети не сообщают участникам, кто смотрел их страницу. А вот в «Одноклассниках», если вы не хотите, чтобы кто-то видел, что его страницу посещали именно вы, приходится создавать фейковые аккаунты (или включать режим анонимки, но он платный);
- ☐ когда вы журналист и используете социальную сеть для публикации различного рода материалов, из-за которых вас могут преследовать. К сожалению, права журналистов часто гарантируются лишь на бумаге.

## 5.3. Обеспечение анонимности

Прежде всего разберемся, какие данные просят указать при регистрации в той или иной социальной сети. Запускаем Тог и заходим поочередно на три сайта:

- ☐ **vk.com**;
- ☐ **ok.ru**;
- ☐ **facebook.com**.

Таблица 5.1. Данные, необходимые для регистрации в социальной сети

Данные	«ВКонтакте»	«Одноклассники»	Facebook
Имя и фамилия	+		+
Пол	+		+
Дата рождения	+		+
Номер телефона	+	+	Номер или e-mail
Возможна ли регистрация без указания номера телефона?	Нет	Нет	?
Возможна ли регистрация через Tor?	Да	Да	Да

Если сеть «ВКонтакте» запрашивает имя, фамилию, пол, дату рождения и только потом номер телефона, то «Одноклассники» первым делом просят указать номер телефона, а потом уже — все остальное (рис. 5.1). Именно поэтому первые три поля для этой социальной сети в табл. 5.1 не заполнены. По сути, «Одноклассникам» нужен только ваш номер телефона.

Рис. 5.1. Регистрация в сети «Одноклассники»

Повеселил Facebook (рис. 5.2) — в качестве пола можно выбрать не только мужской или женский, но еще и **Custom**. Либеральные ценности... Но зато можно указать либо номер телефона, либо e-mail. Другими словами, теоретически допускает-



ся регистрация по e-mail, но далее для подтверждения аккаунта Facebook все равно попросил указать номер телефона. Может, его смутил мой IP-адрес, может, еще что-то.

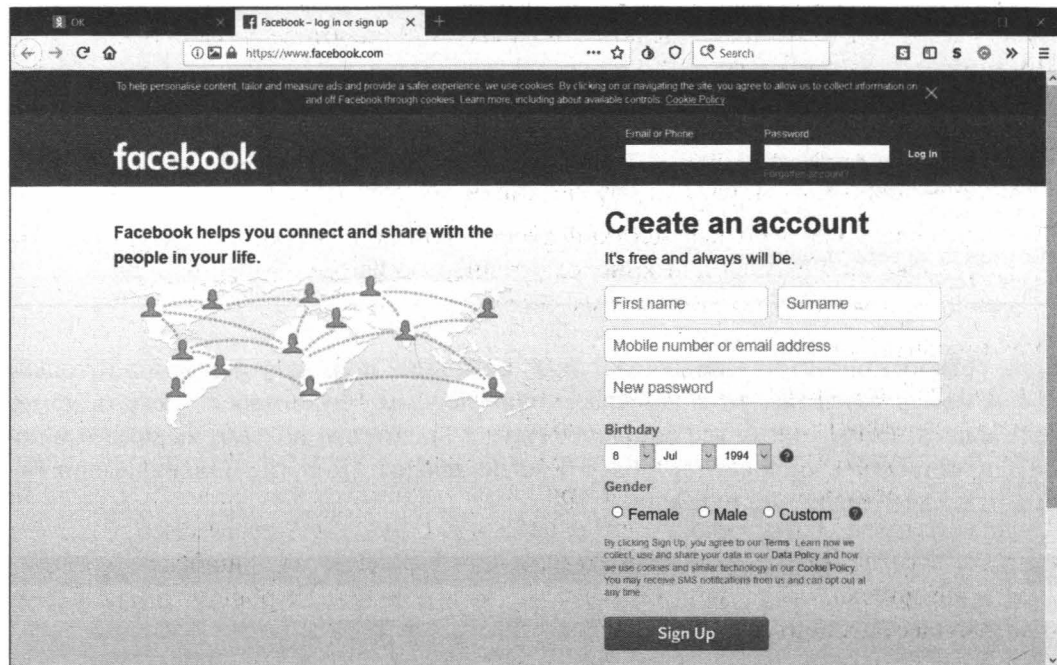


Рис. 5.2. Регистрация в Facebook

Получается, что для регистрации во всех социальных сетях нужно указывать номер телефона, а это означает, что ни о какой анонимной регистрации не может быть и речи. Указание номера телефона равносильно указанию номера паспорта, поскольку SIM-карту без паспорта не купишь.

Другими словами, если вы законопослушный пользователь, то анонимно зарегистрироваться не выйдет. Но если нет, то можно воспользоваться или чужим телефоном (о морали и законности не говорим) — если он еще не использовался для регистрации в социальных сетях, либо как-то купить SIM-карту без паспорта. Где ее взять — ищите сами. Если бываете в Украине, то купить карту без регистрации можно на законных основаниях в любом магазине. Главное сразу активировать ее, чтобы карта активировалась в Украине, а не в роуминге.

После этого регистрация пойдет активнее. При желании можно вообще не регистрироваться, а можно или найти, или купить взломанные аккаунты того же Facebook. Да, это незаконно, неправильно, но такая возможность тоже есть. Может, аккаунты и не взломанные, просто кто-то зарегистрировал несколько десятков аккаунтов, а потом продает как взломанные, — никто не знает правды.

Итак, завладев анонимной SIM-картой и используя Tor, вы сможете действительно анонимно зарегистрироваться в социальной сети.

Далее все зависит от ваших действий. Ведь любые публикуемые вами материалы могут косвенно указать на вас. Но здесь техническая по сути книга мало чем вам поможет. Соблюдайте осторожность...

Если вы журналист и публикуете различные материалы и фотографии, то вам нужно их где-то подготавливать. Делать это на своем компьютере очень и очень глупо. Правильнее поступить так:

- ☐ скачать VirtualBox и развернуть в нем виртуальную машину;
- ☐ установить в нее все программное обеспечение, необходимое для подготовки материалов: офисный пакет, графический редактор и т. п.;
- ☐ зашифровать виртуальный жесткий диск — или полностью, или создать на нем зашифрованный раздел или криптоконтейнер (приложение TrueCrypt вам в помощь) — и хранить там все свои материалы;
- ☐ установить Torg.

И в дальнейшем работайте с анонимными материалами только в виртуальной машине на зашифрованном диске. Если потребуется быстро все удалить (когда в вашу дверь уже стучатся), вам не придется тратить время на удаление с компьютера изображений и документов, очистку истории браузера и его закладок и т. п. Все равно не успеете. А вот снести файл виртуальной машины — дело пары секунд. И даже если его восстановят, что маловероятно из-за его размера, то с ошибками, а информация внутри него все равно останется зашифрованной. В общем, не забывайте о преимуществах виртуализации!



## ГЛАВА 6



# Способы взлома и защиты электронной почты

Существует множество возможностей взломать почтовый ящик. В этой главе мы рассмотрим реальные способы реализации этих возможностей. Познакомившись с этими способами, вы будете знать, как действуют злоумышленники и как от них защититься. В то же время ни автор, ни издательство не несут ответственности за неправомерное использование материала этой главы.

## 6.1. Способы взлома почтового ящика

### 6.1.1. Троянский конь

Весьма распространенным способом получения доступа к чужому почтовому ящику является рассылка электронных писем со встроенными вирусами. Точнее, вирус встраивается не в само письмо — 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. Далее все просто: пользователь переходит по ссылке, и на его компьютер загружается вредоносный код.

Вот примеры таких троянов: DarkComet RAT, SpyEye, Carberp. О DarkComet RAT много пишут в Сети, Carberp — тоже известный троян. А SpyEye — это троян, разработанный Александром Паниным, который даже засветился в сводках ФБР<sup>1</sup>.

По роду своей деятельности мне иногда приходится исследовать информационную безопасность того или иного предприятия. Не так давно я использовал для этого модифицированную версию трояна Zeus. На момент создания его последние модификации не обнаруживал ни один антивирус (рис. 6.1), к тому же в нем присутствовала функция отключения процессов, в которых «замечен» Dr.Web. Однако на компьютере «жертвы» была установлена антивирусная система Comodo — так даже лучше.

---

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

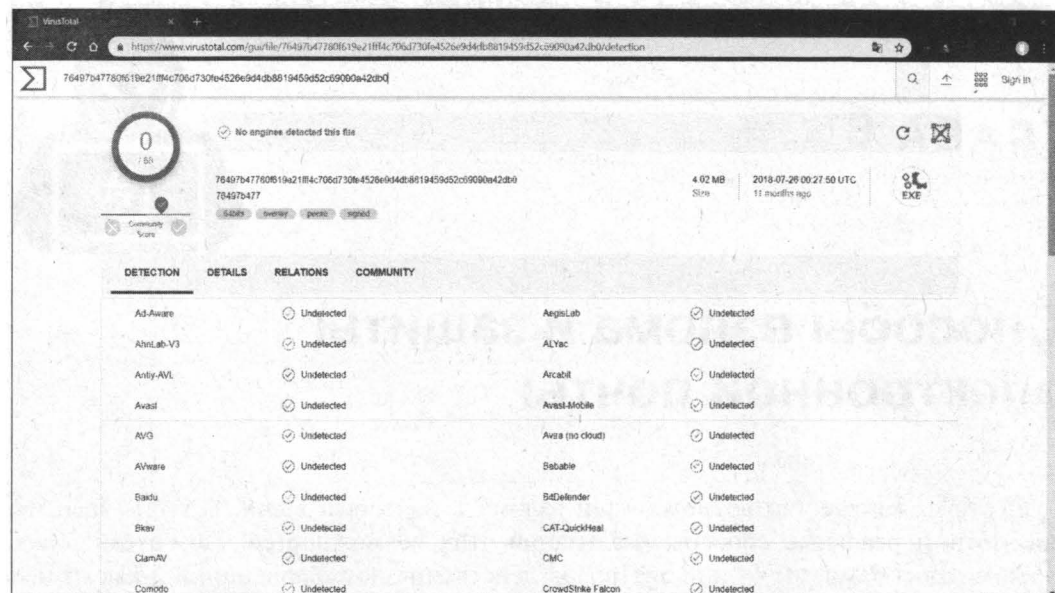


Рис. 6.1. Отчет VirusTotal

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

Итак, у нас есть модифицированный ZeusS, но как заставить бухгалтера запустить его? Если просто отправить ей ссылку, понятное дело, она переходить по ней не станет. Обещать в письме «золотые горы» — тоже прошлый век, на такое пользователи уже не реагируют.

Как бы там ни было, для внедрения трояна нужно написать «жертве» письмо, которое мотивирует ее запустить троян. Здесь надо проявить изобретательность. Конкретных рекомендаций я дать не могу — все зависит от того, кем является эта «жертва». 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 что-то типа **xaker134566788@gmail.com**, мы подделали заголовки письма. Это делается достаточно просто, а как именно, будет показано в разд. 6.1.5. Так что пока не будем на это отвлекаться.

После установки трояна на компьютер «жертвы» мы получили возможность полностью контролировать его (рис. 6.2).

Давайте, например, ради интереса посмотрим список процессов компьютера, в котором, ясное дело, не будет нашего трояна (рис. 6.3). Мы можем также просмотреть файловую систему (рис. 6.4).

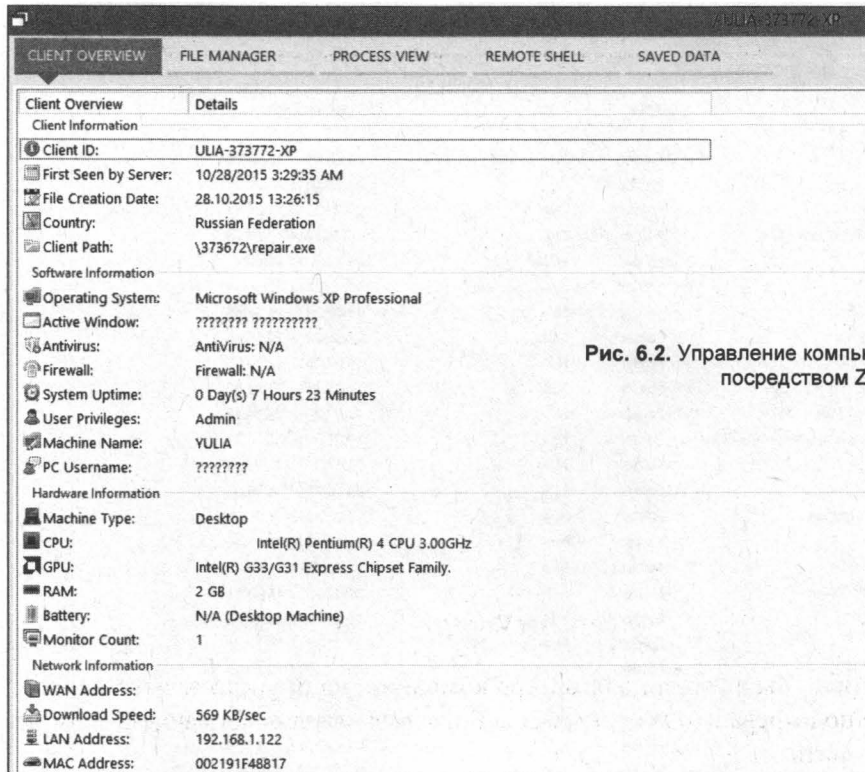


Рис. 6.2. Управление компьютером «жертвы» посредством Zeus

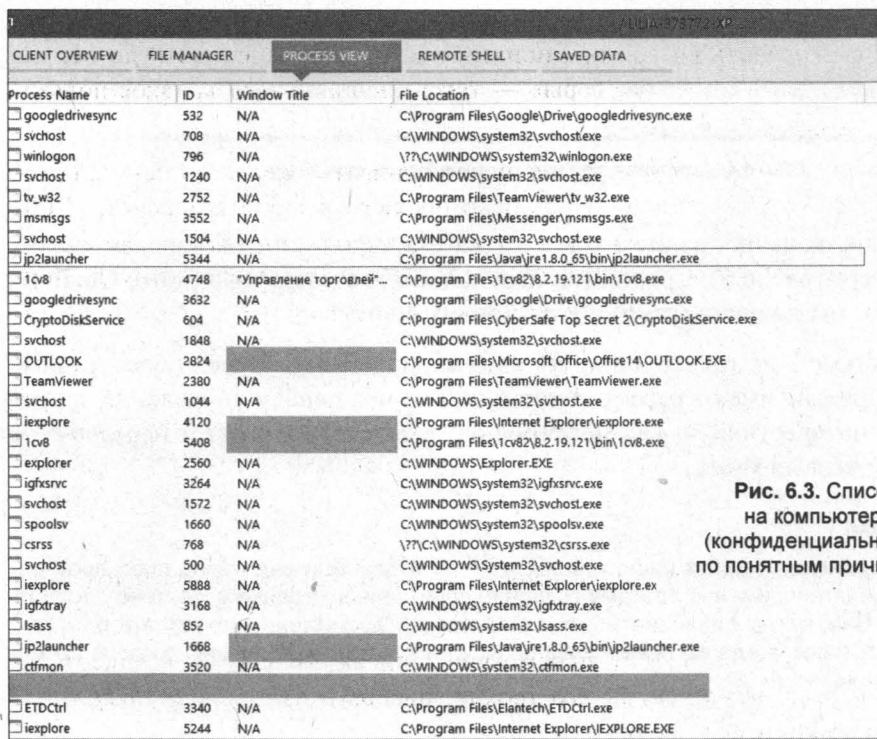


Рис. 6.3. Список процессов на компьютере «жертвы» (конфиденциальная информация по понятным причинам закрашена)

File Name	Type	Size	Creation Time
...			
IYUGBANK	Folder	N/A	20.03.2012 15:11:09
373672	Folder	N/A	28.10.2015 13:26:15
373772	Folder	N/A	28.10.2015 13:26:15
64ad34c5ec977c77d7299c2114	Folder	N/A	12.02.2014 17:26:03
AI_RecycleBin	Folder	N/A	09.12.2014 9:30:24
banks	Folder	N/A	19.02.2012 22:10:33
bcrshb_100844685	Folder	N/A	13.02.2013 11:53:39
bcrshb_magnatnovo	Folder	N/A	22.05.2013 10:10:43
BSCInt_3	Folder	N/A	19.02.2012 22:12:01
BSCInt_3.2	Folder	N/A	19.02.2012 22:13:00
BSCInt_3_B5PP (---) [100840029]	Folder	N/A	19.02.2012 22:24:48
BSCInt_3_Национальный Резервный Банк...	Folder	N/A	19.02.2012 22:25:29
BSCInt_RSHB	Folder	N/A	21.02.2012 12:49:23
Config.Msi	Folder	N/A	08.10.2013 15:39:45
Documents and Settings	Folder	N/A	17.01.2012 17:09:03
DrWeb Archive	Folder	N/A	25.02.2014 13:57:43
DrWeb Quarantine	Folder	N/A	25.02.2014 11:44:46
HP Universal Print Driver	Folder	N/A	20.02.2012 16:04:51
Intel	Folder	N/A	19.02.2012 23:48:18
keys	Folder	N/A	21.02.2012 15:12:36
ModemIte	Folder	N/A	05.03.2013 10:20:27
MSOCache	Folder	N/A	18.03.2015 13:45:42
Program Files	Folder	N/A	17.01.2012 17:10:11
RECYCLER	Folder	N/A	17.02.2012 14:34:26
Sun	Folder	N/A	03.02.2014 9:29:08
System Volume Information	Folder	N/A	17.01.2012 17:09:07
temp	Folder	N/A	17.02.2012 15:12:25
VBRR	Folder	N/A	19.02.2012 22:09:53
WINDOWS	Folder	N/A	17.01.2012 14:28:31

Рис. 6.4. Файловая система на компьютере «жертвы»

Но самое главное, конечно, ради чего все это затевалось — список паролей, сохраненных в браузере (рис. 6.5). Среди этих паролей имелся и пароль к почте Gmail — 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.

### **ВНИМАНИЕ!**

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

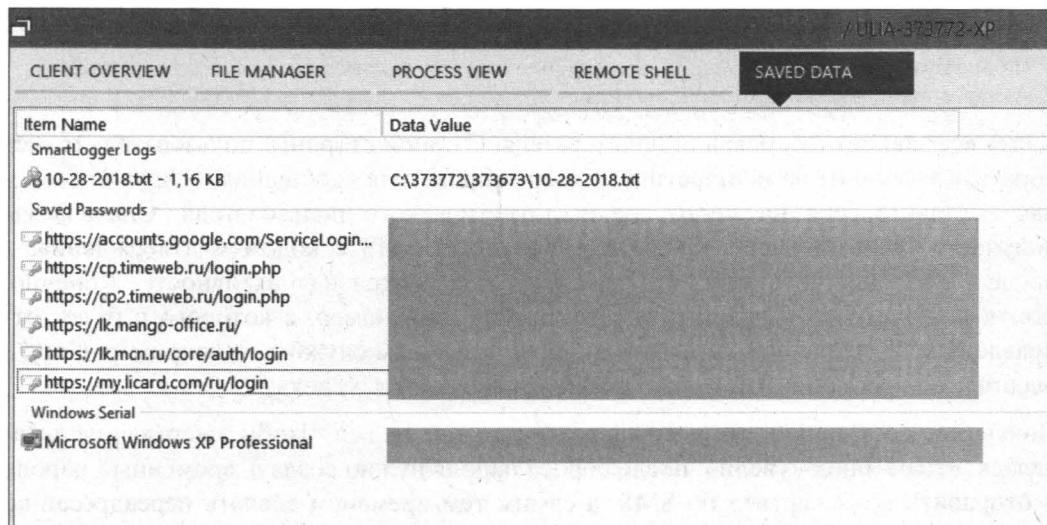


Рис. 6.5. А вот и пароли...

### 6.1.2. Взлом по номеру телефона

Суть этого способа заключается в следующем. Злоумышленнику нужно знать номер телефона «жертвы», указанный при регистрации почтового ящика. Дело в том, что при сбросе пароля почтовая служба требует ввести последние символы номера телефона (или выбрать номер телефона из списка). На этот номер будет отправлена SMS-ка с кодом подтверждения сброса пароля. Зная номер телефона «жертвы», злоумышленник отправляет ей SMS-ку с требованием указать код из предыдущей. Пользователь, ничего не подозревая, отправляет на номер, с которого пришла вторая SMS-ка, код из первой. Самый большой недостаток этого способа в том, что первая SMS-ка придет от Google, а вторая — с неизвестного «жертве» номера. Успех этого способа зависит от сообразительности «жертвы».

Последовательность действий здесь такая:

1. Нужно попытаться выполнить вход в аккаунт Google «жертвы».
2. Поскольку пароля мы не знаем, Google предложит нам его восстановить.
3. Далее, если у вашей «жертвы» был привязан к аккаунту Android-телефон, то Google предложит отправить оповещение на мобильный. Примечательно, но смартфон не издаст ни единого звука, а просто отобразит это предложение. Если смартфона не будет перед глазами у пользователя, есть вероятность, что он это предложение не заметит. Если же пользователь нажмет Нет, не отчаивайтесь — повторите этот процесс несколько раз — позже поймете зачем.
4. После отправки оповещения на смартфон пользователя поступит информация с инструкциями, содержащая ссылку на классическую страницу сброса пароля по SMS. Будем надеяться, что он выполнит предложенную процедуру и получит от системы SMS-ку с кодом подтверждения разблокировки.



## 5. С другого телефона отправьте примерно такое сообщение:

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

Далее все зависит от смекалки пользователя. С одной стороны, пользователь может обратить внимание на неизвестный номер отправителя сообщения. С другой стороны, поставьте себя на место среднестатистического пользователя. Сначала вы получаете 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 «жертве» по SMS, а самым тем временем сделать переадресацию всей почты на «хакерский» ящик. Так можно получить контроль над ящиком, не вызвав особых подозрений.

Этот способ придуман не мною, и было бы некрасиво приписывать его авторство себе. Изначально с нам я познакомился в блоге компании Symantec, в котором даже есть видео, демонстрирующее этот способ наглядно<sup>1</sup> — как говорится, лучше один раз увидеть, чем сто раз услышать.

### 6.1.3. 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.

#### Кейлоггер

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

К преимуществам кейлоггеров относится то, что они записывают 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.

---

<sup>1</sup> См. <http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access>.

Второй недостаток кейлоггера 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 сохранен в нем, 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 вам придется еще один раз подходить к компьютеру.

Вот пример кейлоггера: *SniperSpy*<sup>1</sup> — на случай, если вы захотите им воспользоваться.

## **Программы для «восстановления» паролей почтовых учетных записей**

Программы для «восстановления» паролей почтовых учетных записей позволяют сразу получить все интересующие вас пароли без необходимости чтения мегабайтов кейлоггерского текста в поиске нужного вам пароля. К тому же на них никак не реагирует антивирус. Одна из таких программ — это *Mail PassView*<sup>2</sup>. 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).

---

<sup>1</sup> См. <http://www.sniperspy.com/>.

<sup>2</sup> См. <http://www.nirsoft.net/utils/mailpv.html>.

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

- ❑ Outlook Password Decryptor<sup>1</sup> — позволяет восстановить пароли из Outlook, в том числе самых последних версий (Outlook 2016, работающей под управлением Windows 10);
- ❑ PstPassword<sup>2</sup> — еще одна программа для восстановления паролей, сохраненных в Outlook;
- ❑ WebBrowserPassView<sup>3</sup> — программа для восстановления паролей, хранящихся в браузере. Поддерживаются браузеры IE, Chrome, Opera, Safari, Firefox.

Все, что нужно, — это знать, каким почтовым клиентом пользуется «жертва». Тогда найти программу для «восстановления» пароля из этого почтового клиента — не проблема. Если же «жертва» читает свою почту через веб-интерфейс, 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. Она успешно «восстановила» все пароли, хранящиеся в браузерах IE, Firefox, Chrome и Opera (Safari не проверялся, но, думаю, и там будет полный порядок). Даже если вы не найдете среди полученного списка пароль от почтового ящика, все равно польза от него несомненна — 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.

### **6.1.4. Социальная инженерия, или просто обман**

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

Относительно недавно была взломана почта тогдашнего директора ЦРУ Джона Бреннана. Абсурдность ситуации в том, что почту взломал не «матерый» хакер, а обычный подросток, правильно собрав информацию о своей «жертве».

Подросток сначала связался с сотовым оператором и, представившись сотрудником технической поддержки, уточнил детали аккаунта Бреннана. После этого он позвонил 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.

---

<sup>1</sup> См. <http://securityxploded.com/outlookpassworddecryptor.php>.

<sup>2</sup> См. [http://www.nirsoft.net/utils/pst\\_password.html](http://www.nirsoft.net/utils/pst_password.html).

<sup>3</sup> См. [http://www.nirsoft.net/utils/web\\_browser\\_password.html](http://www.nirsoft.net/utils/web_browser_password.html).

Чуть позже Wikileaks опубликовал письма директора ЦРУ<sup>1</sup> (рис. 6.6).

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

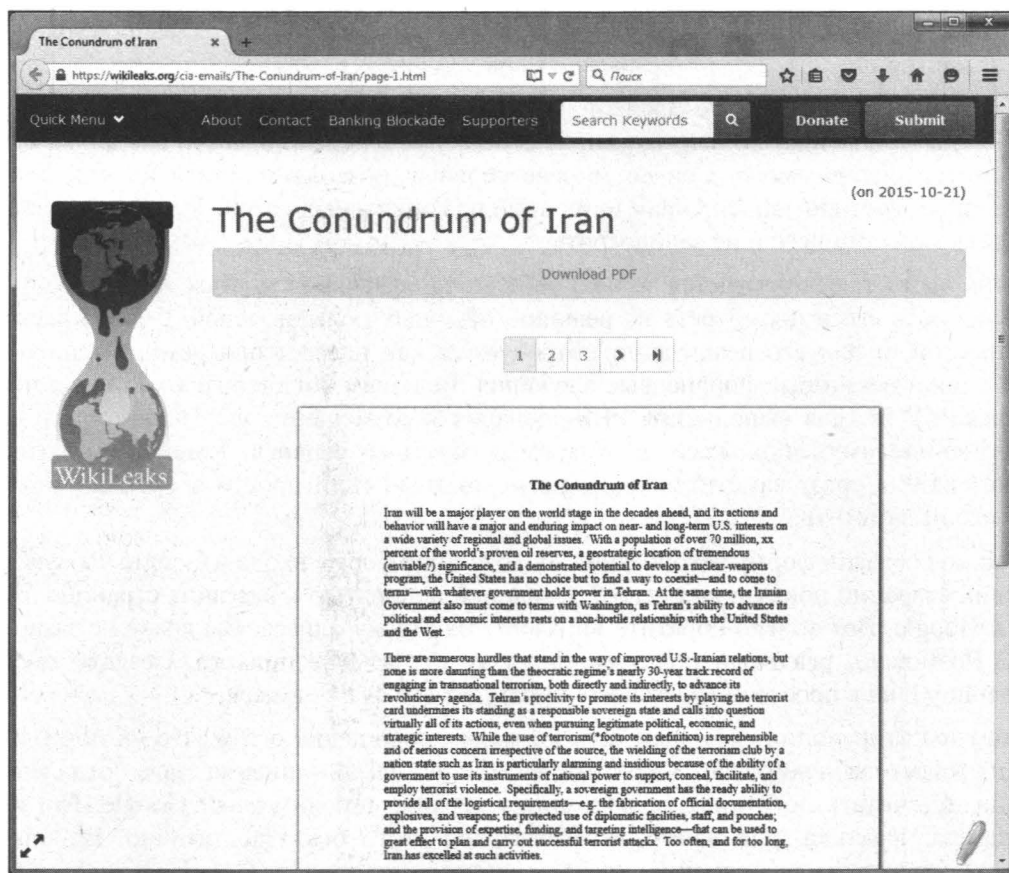


Рис. 6.6. Письма директора ЦРУ, опубликованные Wikileaks

### 6.1.5. Модное слово «фишинг»

Здесь мы просим пользователя самому 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 следует создать такую же страницу входа.

<sup>1</sup> См. <https://wikileaks.org/cia-emails/The-Conundrum-of-Iran/page-1.html>.

Затем надо заманить пользователя на поддельную страницу. Это можно сделать несколькими способами:

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

Очень часто так описывается только «общее направление». Сейчас мы попробуем реализовать его и посмотреть на реакцию обычных пользователей. Способ весьма непростой, и для его реализации потребуются 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 (или просто в спешке) может ничего не заметить.

Итак, мы создали форму авторизации, похожую на форму входа в Google. Результат наших стараний показан на рис. 6.7. 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.

Затем мы отправили некоторым пользователям сообщение о том, что их почтовый ящик будет заблокирован. Обратите внимание: дизайн письма даже отдаленно (если не считать логотипа) не напоминал дизайн, используемый Google. Но, как показала практика, для наших пользователей этого было достаточно. Впрочем, можно было взять исходный код письма, которое отправляет Google, и сделать все более качественно. В реальных условиях злоумышленник так и делает — будьте в этом уверены.

Что произошло дальше? Пользователи прочитали письмо, перешли по ссылке и наивно ввели свои 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 6.1.

#### Листинг 6.1. 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 пользователя на страницу входа в google, чтобы
// меньше было подозрений
header('Location:
https://accounts.google.com/ServiceLogin?service=mail&passive=true&np=
false&continue=https://mail.google.com/mail/&ss=1&sc=1&tmpl=
default&tmplcache=2&emr=1&osid=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.

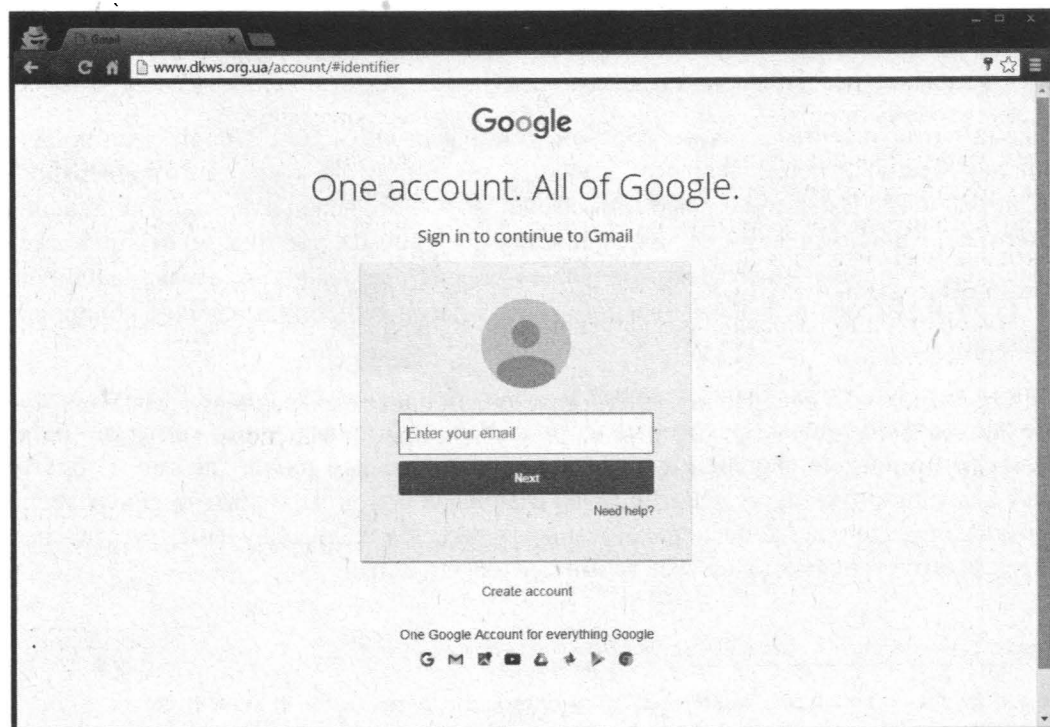


Рис. 6.7. Поддельная версия страницы входа в Gmail

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-нибудь небольшой организации. Списки таких серверов регулярно обновляются на специальных ресурсах. Думаю, не составит особого труда найти такой список<sup>1</sup>. Далее можно развернуть на локальном компьютере веб-сервер<sup>2</sup> с поддержкой PHP. Тогда у вас будет доступ к файлу `php.ini`, и можно будет указать SMTP-сервер, через который функция `mail()` будет отправлять письма.

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 наш хостинг и использовали. На нем функция `mail()` выполнялась без особых нареканий. Понятно, что если просмотреть все заголовки письма, «след» приведет к нам. Но для нас сейчас важно не это. Сейчас важно, чтобы в почтовом клиенте поле **From** содержало то, что нам нужно. В первом способе мы поступили именно так, т. е. для отправки сообщения использовали функцию `mail()`.

Стандартная PHP-функция `mail()`<sup>3</sup> позволяет с легкостью задать 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 возможный скептицизм.

<sup>1</sup> См. <https://www.arclab.com/en/kb/email/list-of-smtp-and-pop3-servers-mailserver-list.html>.

<sup>2</sup> См. <https://bitnami.com/stack/wamp/installer>.

<sup>3</sup> См. <http://php.net/manual/bg/function.mail.php>.

### 6.1.6. «Вспоминаем» пароль

Теперь попробуем «вспомнить» то, что никогда не знали, — пароль от почтового ящика «жертвы». Очень часто почтовые службы позволяют восстановить забытый вопрос. 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, т. е. вероятность, 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.

### 6.1.7. Кража Cookies

Еще один неплохой способ получения доступа к почтовому ящику — это кража Cookies. Конечно, он эффективен, если «жертва» хранит свои пароли в браузере. Впрочем, 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 или форуму), вы можете попытаться его использовать при входе в почтовый аккаунт. Есть вероятность, что он подойдет.

Как украсть «куки»? Существуют различные способы: от использования трояна (рис. 6.8) до банального копирования их 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 его на своем компьютере. Для анализа Cookies можно использовать самые разные утилиты, одна из которых CookieSpy<sup>1</sup>, которая поддерживает не только установленные, но и portable-браузеры, что позволяет «подсунуть» программе каталог с Cookies (рис. 6.9)

### 6.1.8. XSS-уязвимости

Еще 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 потребуются

---

<sup>1</sup> См. <http://www.cookiespy.com/>.



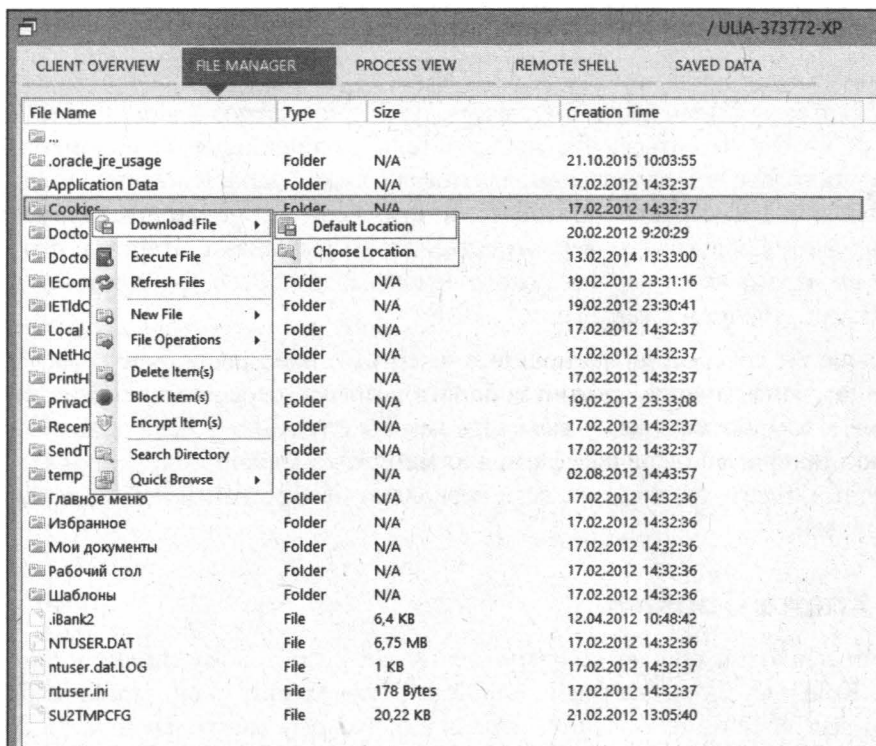


Рис. 6.8. Использование трояна для кражи Cookies

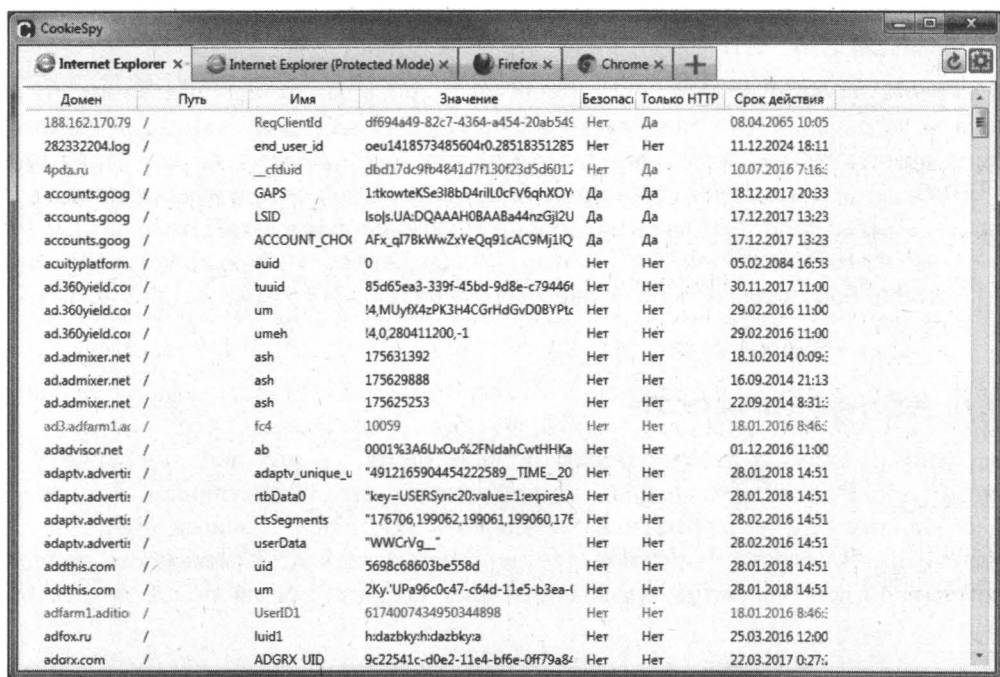


Рис. 6.9. Программа CookieSpy

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 инжиниринг окажется более эффективным.

### 6.1.9. Метод грубой силы

Самый неэффективный способ — он заключается в переборе паролей 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 так хочется попытаться, тогда можете попробовать воспользоваться утилитой Brutus, работа с которой обсуждается на [hackerthreads](http://hackerthreads.org)<sup>1</sup>.

Есть и еще одна весьма популярная утилита — THC-Hydra<sup>2</sup>, 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.

## 6.2. Защита почтового ящика

Итак, мы рассмотрели девять способов взлома почтового ящика. Уберечься от них просто:

- ❑ троянский конь — не переходить по ссылкам в письме, не запускать программы и другие объекты из письма. Антивирус тоже не помешает. Он не всегда помогает, но все же с ним лучше, чем без него;
- ❑ взлом по номеру — внимательно читать все входящие SMS и помнить, что Google и другие почтовые сервисы не требуют отправки им каких-либо кодов для восстановления доступа. Максимум, код нужно будет ввести на их сайте;
- ❑ физический доступ к компьютеру — настройте блокировку экрана, когда вы не за компьютером, и установите пароль посложнее для вашей учетной записи;
- ❑ обман — от этого никто не застрахован, но лучше проявляйте лишний раз бдительность;
- ❑ фишинг — просто будьте внимательны. Злоумышленник может создать домен вроде [gogle.com](http://gogle.com), [qoogle.com](http://qoogle.com) и пр. Это как с первыми китайскими подделками

<sup>1</sup> См. <http://www.hackerthreads.org/Topic-47150>.

<sup>2</sup> См. <https://www.thc.org/thc-hydra/>.

в 1990-е: были и Panasonic, и Sony, и другие «лейблы», написание которых было похоже на оригинал, но таковым не являлось;

- ☐ восстановление пароля — никому не сообщайте личную информацию о себе, особенно ту, которую вы используете для восстановления доступа к почтовому ящику;
- ☐ кража Cookies — украсть Cookies можно либо получив физический доступ к компьютеру, либо с помощью трояна. Значит, методы защиты такие же;
- ☐ XSS-уязвимости — способ используется редко; но от пользователя мало что зависит. Он же не знает, что в выбранном почтовом сервисе есть уязвимость...
- ☐ перебор пароля — здесь поможет только сложный пароль. Если для восстановления доступа вы указали второй почтовый ящик, то сложный пароль нужно установить и для него.

И еще — меньше доверяйте всем! Представим ситуацию: вы защищаетесь, защищаетесь, а потом предоставляете доступ (либо физически, либо удаленный через TeamViewer или другую подобную программу) малознакомому лицу для решения каких-либо проблем с компьютером. А где вероятность, что пока он «ремонтирует» компьютер, он не украдет пароли и другую важную информацию?

\* \* \*

Итак, почтовый ящик мы защитили. Теперь нужно позаботиться о защите содержимого, т. е. самих писем. Сразу нужно отметить — практически все почтовые сервисы используют HTTPS для доступа к веб-интерфейсу и TLS/SSL для шифрования POP/IMAP/SMTP, т. е. ваши письма отправляются по зашифрованному каналу. Если в них нет ничего особо секретного, то такой защиты вполне достаточно.

Однако вы можете также настроить шифрование писем при передаче. Сделать это можно двумя способами: правильным и неправильным. Далее, в следующем разделе, мы рассмотрим правильный способ шифрования с использованием открытого и закрытого ключей. А о неправильном поговорим прямо сейчас.

Вы можете зашифровать файл с текстом письма (есть много программ, позволяющих шифровать одиночные файлы) и прикрепить этот зашифрованный файл к письму, которое отправите другому человеку. При личной встрече или с использованием других защищенных каналов связи вы передадите ему ключ (пароль) от зашифрованного файла. Также можно использовать следующий лайфхак:

```
copy /b my_foto.jpg + file.rar my_foto2.jpg
```

Эта команда принимает два файла: my\_foto.jpg (ваша фотка с отпуска) и file.rar (архивный файл с паролем, в нем — секретная информация) и создает файл my\_foto2.jpg. К письму вы прикрепляете файл my\_foto2.jpg. Для всех — это обычная пляжная фотка. Но получатель знает, что можно открыть файл my\_foto2.jpg как обычный архив и получить доступ к секретной информации. Подробнее об этом способе мы поговорим в следующей главе.

А недостатки неправильного способа следующие:

- ☐ при создании зашифрованного файла не используется PKI (от англ. Public Key Infrastructure, инфраструктура открытых ключей) — такое шифрование проще

взломать. Да и пароль еще как-то передать нужно. Если кто-то перехватит пароль, то он сможет читать все ваши зашифрованные файлы;

- при использовании предложенного лайфхака нужно помнить, что размер файла `my_foto2.jpg` не должен превышать размера среднестатистической картинки, а это несколько мегабайтов. Иначе такие «картинки» будут привлекать лишнее внимание. Часто почтовые серверы устанавливают ограничение для одного письма на уровне порядка 20 Мбайт. Другими словами, много информации таким способом не передашь. Но если информация текстовая, и учитывая, что мы используем сжатие, то в целом получится неплохо.

## 6.3. Шифрование электронной почты

### 6.3.1. Немного теории: S/MIME, PKI и PGP

При подготовке 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.

Специалистам известно, что самым надежным способом защиты электронной почты является использование стандарта S/MIME. S/MIME (Secure/Multipurpose Internet Mail Extensions) — это 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 весьма гордо: «стандарт». Но на самом деле S/MIME — это всего лишь PKI-приложение, используемое для цифровой подписи, а также для шифрования почтовых и других сообщений.

«Погружаемся» глубже. У нас появился новый термин (правда, он был вскользь упомянут в конце предыдущего раздела) — PKI (Public Key Infrastructure), инфраструктура открытых ключей. Разберемся, что это такое. Шифрование информации основано на двух криптографических подходах — существует *симметричная* и *асимметричная* криптография. Классический метод криптографии — симметричный — 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 служит как для шифрования, так и для расшифровки сообщения.

Но есть и асимметричная криптография, которая базируется на использовании пары ключей: *закрытого* и *открытого*. Эти ключи с использованием специальных алгоритмов создаются вместе, парой. Любая информация, зашифрованная открытым ключом, может быть расшифрована только с помощью соответствующего закрытого ключа.

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

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

Дополнительную информацию (если, конечно, вы заинтересовались) о S/MIME и PKI<sup>1</sup> 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. В настоящее время используются обе технологии защиты электронной почты: PKI (в лице S/MIME) и PGP — и обе они основаны на принципе открытых ключей. Обе технологии также одинаково популярны. Посмотрим, какая между ними разница.

В основу PGP положен стандарт OpenPGP, который содержит:

- ☐ сведения о владельце сертификата;
- ☐ открытый ключ владельца сертификата;
- ☐ электронную цифровую подпись (ЭЦП) владельца сертификата;
- ☐ период действия сертификата;
- ☐ предпочтительный алгоритм шифрования.

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

- ☐ открытый ключ владельца сертификата;
- ☐ 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 же X.509 может быть как получен от центра сертификации, так и быть самоподписанным. Именно по этой причине я использую стандарт S/MIME — ведь он предусматривает третью сторону, которая выступает гарантом того, что

---

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

тот, с кем вы обмениваетесь корреспонденцией, и есть 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 почему-то нравится больше именно PGP). Но я не считаю, что на полемику нужно тратить время. Книга эта задумывалась практической, и поэтому должна содержать краткие и понятные инструкции, а не рассуждения о том, какая технология теоретически надежнее.

### 6.3.2. Как будем защищать почту?

Ранее было сказано, 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, включающий открытый (публичный) и закрытый (секретный, приватный) ключи, и настроить свой почтовый клиент. При этом нет разницы, какой это будет клиент, — главное, чтобы он поддерживал S/MIME. Какая операционная система стоит на компьютере, тоже не имеет значения. Вы можете сгенерировать сертификаты в Windows, а использовать их для настройки почтовых клиентов в macOS, Linux и Android (или наоборот — скажем, сгенерировать сертификат в Android и использовать их в любой другой ОС). При этом не будет его привязки к конкретной программе (типа 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 им по умолчанию. А вот Windows-пользователи могут скачать программу OpenSSL для Windows по адресу: <https://code.google.com/archive/p/openssl-for-windows/downloads>.

### 6.3.3. 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 битов), вторая — приватный (закрытый) ключ длиной 4096 битов. Третья команда генерирует по этому закрытому ключу публичный (открытый) ключ.

Позволю себе некоторые технические подробности относительно шифрования. Здесь мы сгенерировали пару RSA-ключей: открытый и закрытый. Но так уж устроен криптографический алгоритм RSA, что зашифровать данные длиной более 4 Кбайт не получится. Что делать? Есть способ обойти это — информация сначала шифруется симметричным алгоритмом с использованием одноразового ключа.

При симметричном шифровании зашифровать и расшифровать файл `file.txt` (кстати, сообщение электронной почты, по сути, тоже файл, формируемый почтовым клиентом) можно так:

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

А уже затем этот одноразовый ключ шифруется публичным ключом. И при расшифровке одноразовый ключ расшифровывается закрытым. Именно такой способ и используется в почтовых клиентах — ведь передаваемая с их помощью информация часто превышает 4 Кбайт.

Пользователям Linux для выполнения такого сценария могу предложить следующий Bash-скрипт `encrypt` (листинг 6.2).

#### Листинг 6.2. Bash-скрипт `encrypt` для шифрования файла

```
# !/bin/bash

FNAME="$1"
PUBLICKEY="$2"
SESSIONKEY="$3"
OUT="$4"

# Generate the random symmetric-key with length 50 chars
if [ -c /dev/urandom ] ; then
KEY=`head -c 50 /dev/urandom | openssl enc -base64`
else
KEY=`openssl rand -base64 50`
fi
export KEY

# Encrypt the symmetric key using the public key
openssl rsautl -encrypt -inkey "$PUBLICKEY" -out "$SESSIONKEY" -pubin <<EOF
$KEY
EOF

# Encrypt the file
openssl enc -aes-256-cbc -pass env:KEY -in "$FNAME" -out "$OUT"
```



Использовать сценарий `encrypt` нужно так:

```
./encrypt file.txt publicKey.pem session.key file.enc
```

В результате будет сгенерирован ключ `session.key` и зашифрованный файл `file.enc`. Для расшифровки файла `file.enc` служит скрипт `decrypt` (листинг 6.3).

#### Листинг 6.3. Сценарий `decrypt`

```
#!/bin/bash

PRIVATE="$1"
SESSION="$2"
ENCRYPTED="$3"
DECRYPTED="$4"

# Decrypt the symmetric key using the private key
KEY=`openssl rsautl -decrypt -inkey "$PRIVATE" -in "$SESSION" `
export KEY

# Decrypt the file
openssl enc -aes-256-cbc -d -pass'env:KEY' -in "$ENCRYPTED" -out "$DECRYPTED"
```

Использовать сценарий `decrypt` нужно так:

```
./decrypt privateKey.pem session.key file.enc file.zip
```

Linux-пользователи привыкли к командной строке. А вот Windows-пользователи — нет, и командная строка кажется для них страшным и непостижимым. Поэтому они могут задействовать любую оболочку для генерирования ключей. Одна из таких оболочек — программа *CyberSafe Top Secret*<sup>1</sup>. Программу можно использовать бесплатно, но с некоторыми ограничениями, которые вас не должны волновать, поскольку вы используете ее для личного применения, — бесплатная версия позволяет создать только одну ключевую пару: открытый и закрытый.

С помощью этой программы (рис. 6.10, а) легко можно сгенерировать пару ключей (открытый и закрытый) и экспортировать ее (рис. 6.10, б) в отдельную папку для того, чтобы далее привязать эти ключи к почтовым программам.

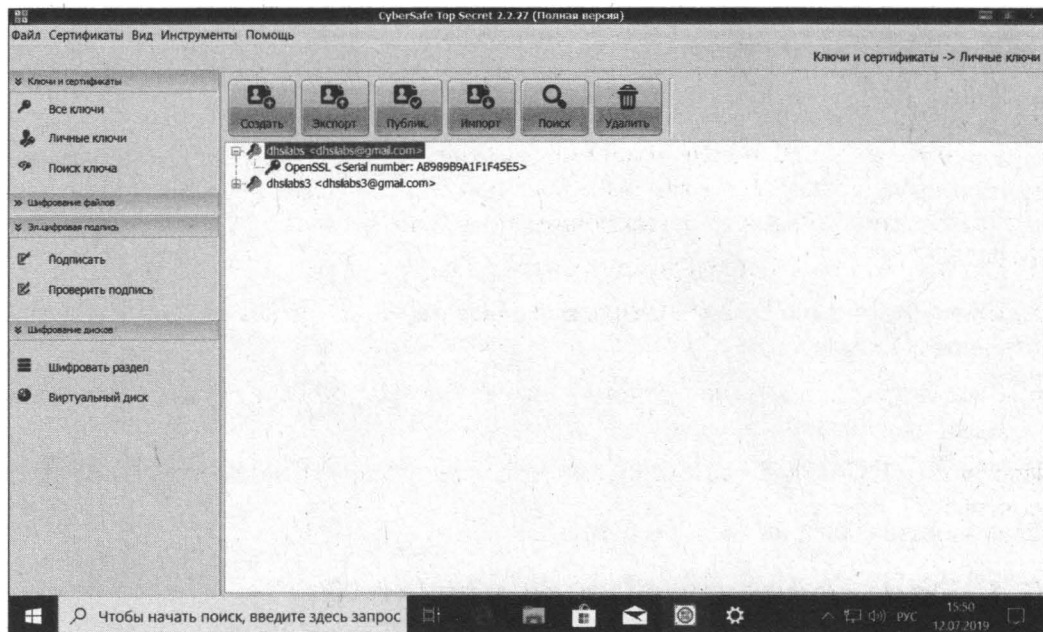
Для создания и экспорта ключевой пары выполните следующие действия:

1. Запустите *CyberSafe Top Secret* и перейдите в раздел **Ключи и сертификаты | Личные ключи**.
2. Нажмите кнопку **Создать**.
3. В открывшемся окне введите следующую информацию:
  - **Адрес эл. почты** — ваш электронный адрес.
  - **Пароль** — постарайтесь придумать для ключа надежный пароль. Если пароль слабый, программа сообщит вам об этом.

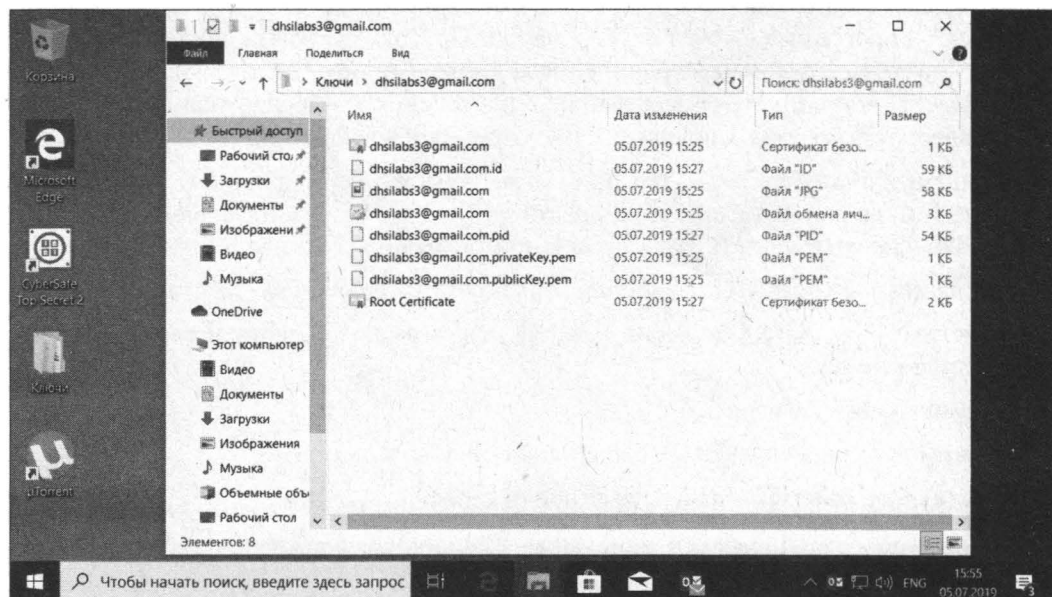
<sup>1</sup> См. <http://cybersafesoft.com/cstopsecret.zip>.



- **Наименование, Подразделение, Организация, Страна** — сугубо информационные поля, обязательным из которых является только **Наименование**. Можете ввести свое имя (настоящее или вымышленное) или название своей организации.



а



б

**Рис. 6.10.** Приложение CyberSafe Top Secret (а) и результат экспорта ключевой пары (б)

- **Срок действия сертификата** — по умолчанию используется срок действия 365 дней, но я бы рекомендовал увеличить этот срок. Ведь старым сертификатом вы не сможете зашифровать новые письма, а новым — расшифровать старые. Если же письма потеряют для вас актуальность за год, можно оставить все как есть.
  - **Длина ключа, бит** — на сегодняшний день вполне достаточной является длина ключа 4096 битов, но для максимальной защиты можно установить 8192 бита.
  - **Опубликовать, после создания** — открытый ключ будет опубликован на сервере CyberSafe, а вам на e-mail придет код подтверждения публикации. Если вам это не нужно, выключите этот флажок.
4. Нажмите кнопку **Далее** и дождитесь создания ключа.
  5. Ключ будет отображен в разделе **Личные ключи**. Выделите его и нажмите кнопку **Экспорт**.
  6. Введите пароль, указанный при создании ключа, и выберите папку, в которую будет экспортирован ключ.

Программу CyberSafe Top Secret на этом можно закрыть и перейти к настройке почтового клиента.

## 6.4. Настройка почтовых клиентов на шифрование

Представим, что у нас сгенерировано два сертификата: один — для пользователя `dhsilabs3@gmail.com`, другой — для `dhsilabs@gmail.com`. 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 `dhsilabs@gmail.com`, а на компьютере Б — публичный ключ для `dhsilabs3@gmail.com`, чтобы пользователи на компьютерах А и Б могли зашифровывать сообщения, адресованные друг другу.

Далее мы рассмотрим настройку почтовых клиентов MS Outlook 2013/2016/2019 и Mozilla Thunderbird. Первый входит в состав MS Office, поэтому многие пользователи не заморачиваются, а выбирают то, что есть. Второй — программа OpenSource, которую выбирают пользователи, заботящиеся об отсутствии всяких «черных» ходов.

### 6.4.1. Настройка Microsoft Outlook

Итак, настроим шифрование в почтовом клиенте Microsoft Outlook 2013/2016/2019. В более старых версиях Microsoft Outlook шифрование настраивается аналогично, но несколько иначе. Принцип будет тем же, но команды интерфейса и их расположение — другим. Подробные инструкции вы без проблем найдете в Интернете.

### ПРИМЕЧАНИЕ

Перед настройкой шифрования писем убедитесь, что ваш почтовый клиент уже настроен на обычную работу и нормально функционирует. В книге не описываются создание учетной записи и ее настройка — за этим обратитесь в службу поддержки своего почтового ящика. Далее мы будем считать, что вы уже можете отправлять и принимать обычные, незашифрованные письма (рис. 6.11).

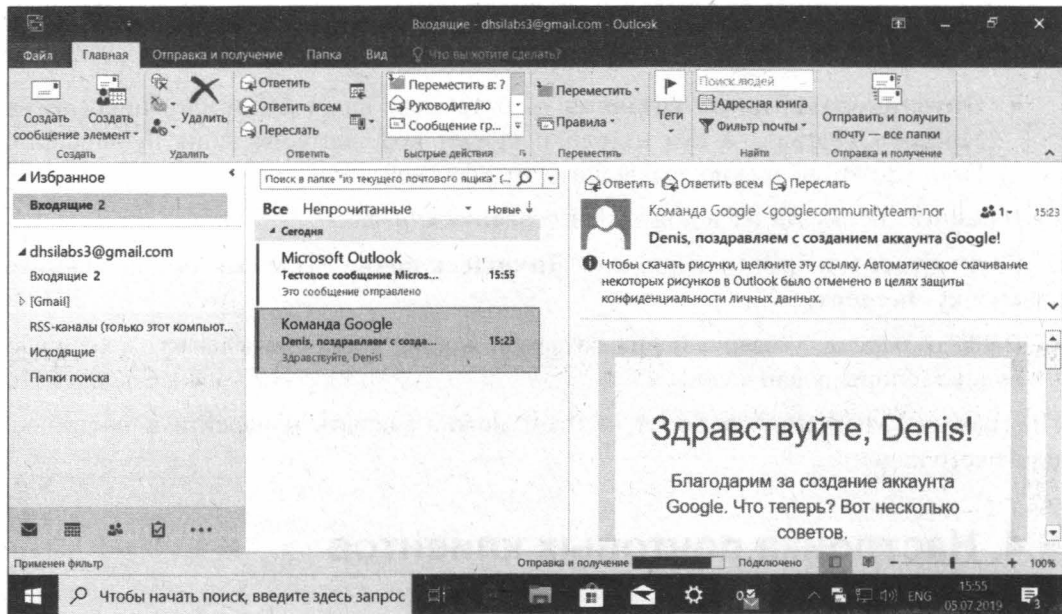


Рис. 6.11. Почтовый клиент настроен и работает

Прежде всего нужно установить экспортированный сертификат в формате PKCS#12 в хранилище Windows. Для этого щелкаем на PFX-файле сертификата двойным щелчком 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** (рис. 6.12). В открывшемся окне перейдите в раздел **Защита электронных писем** (рис. 6.13).

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. Впрочем, если цифровая подпись вам не нужна, этот параметр можно не включать. Однако с помощью цифровой подписи получатели ваших писем смогут убедиться, что вы — это вы.

Затем нажмите кнопку **Импорт/экспорт**, в открывшемся окне выберите свой закрытый ключ (диалоговое окно открытия файла, впрочем, не позволит выбрать

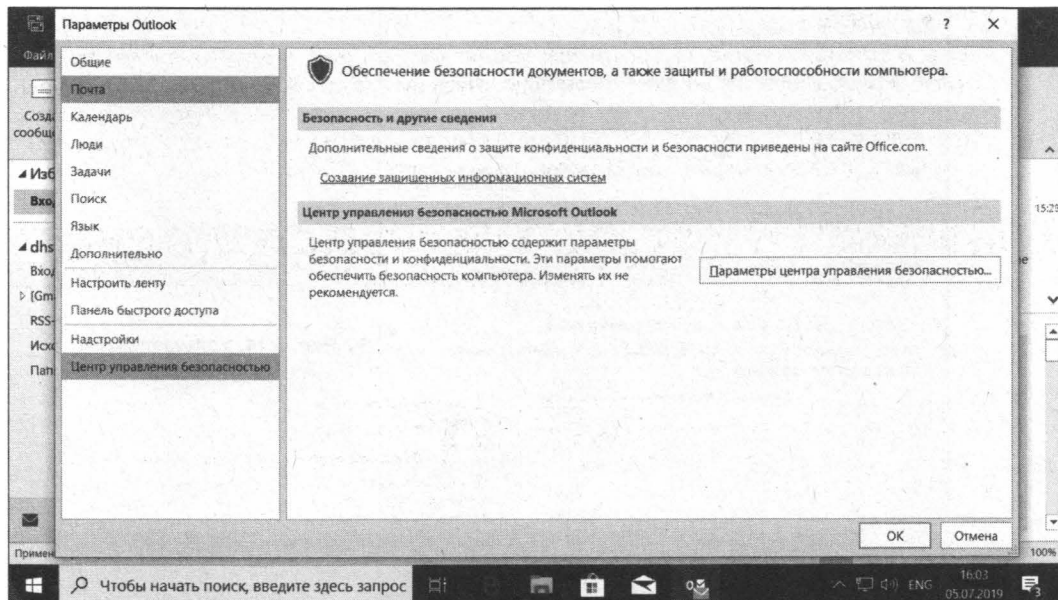


Рис. 6.12. Параметры центра управления безопасностью Microsoft Outlook

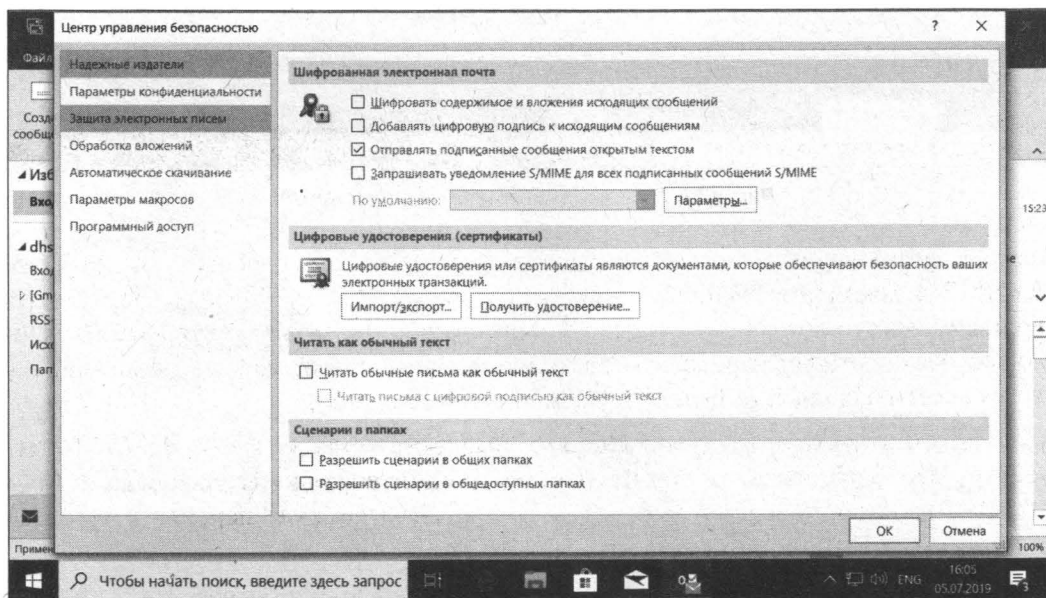


Рис. 6.13. Раздел Защита электронных писем параметров центра управления безопасностью Microsoft Outlook

какой-либо другой) и введите пароль от него (рис. 6.14). После чего просто нажмите кнопку ОК.

Закройте окна параметров, дважды последовательно нажав кнопки ОК. Собственно, Outlook вы уже настроили. Попробуйте создать письмо и отправить его (я прекрасно помню о втором сертификате) — просто попробуйте отправить пробное

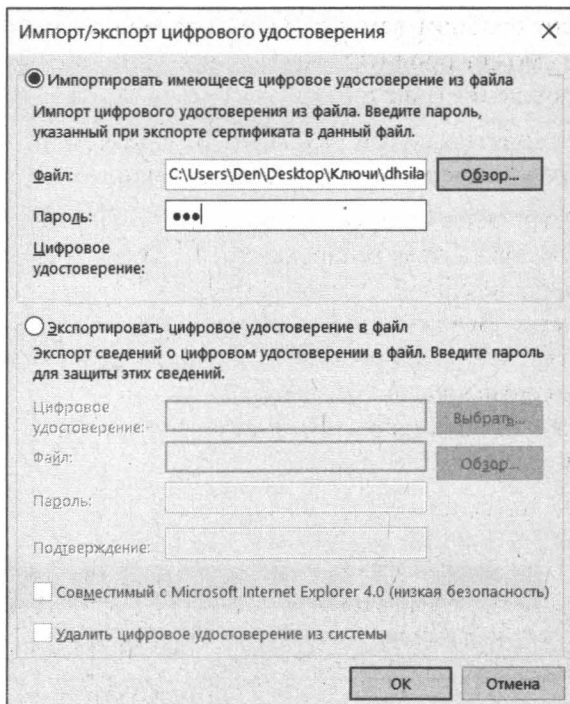


Рис. 6.14. Устанавливаем сертификат

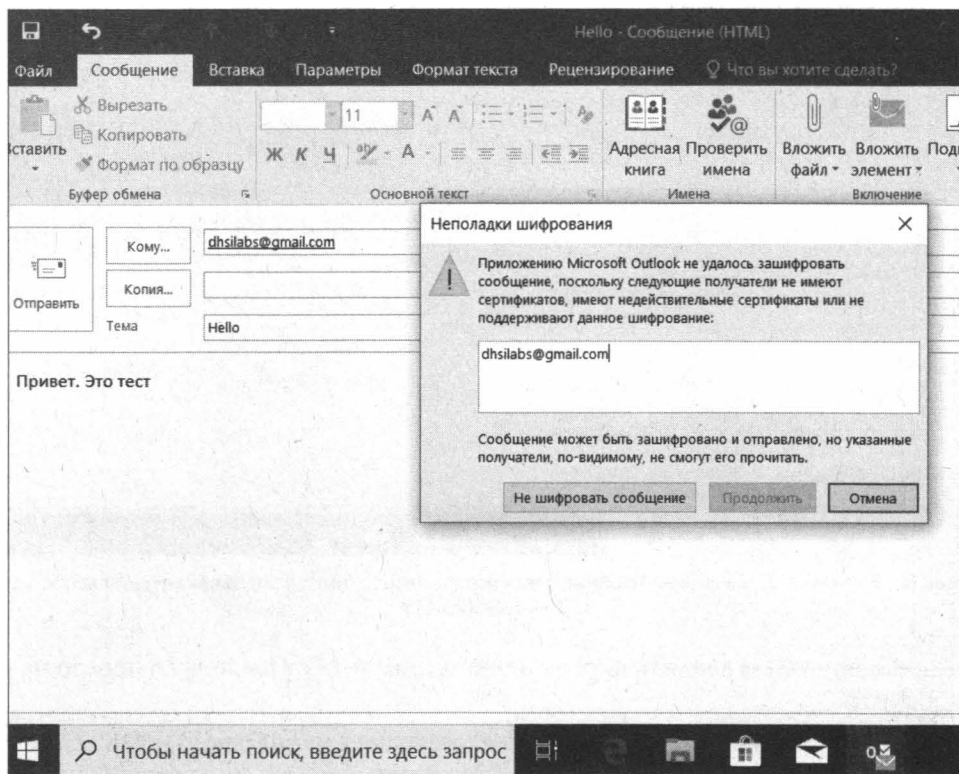


Рис. 6.15. Предложение не шифровать сообщение..

письмо. И тут почтовый клиент сообщит вам, что не установлен сертификат получателя письма, поэтому он не сможет прочитать написанное вами письмо. Поэтому и предложит не шифровать сообщение (рис. 6.15).

Именно такое окно вы будете видеть каждый раз, когда отправляете письма получателям, сертификаты которых не импортированы в адресной книге.

Теперь разберемся, как импортировать сертификат получателя. Первым делом попросите своего знакомого отправить вам его публичный ключ. После этого на вкладке **Главная** основного окна Microsoft Outlook (см. рис. 6.11) выберите команду **Создать элемент | Контакты**. Введите имя контакта и его электронный адрес. После этого нажмите кнопку **Сертификаты** — она скрыта в меню **Показ** (рис. 6.16). Откроется список сертификатов — он будет пуст (рис. 6.17). Нажмите кнопку **Импорт** и выберите публичный ключ пользователя (рис. 6.18). После чего нажмите кнопку **Сохранить и закрыть**.

Снова попытайтесь отправить этому пользователю письмо. На этот раз оно будет отправлено зашифрованным.

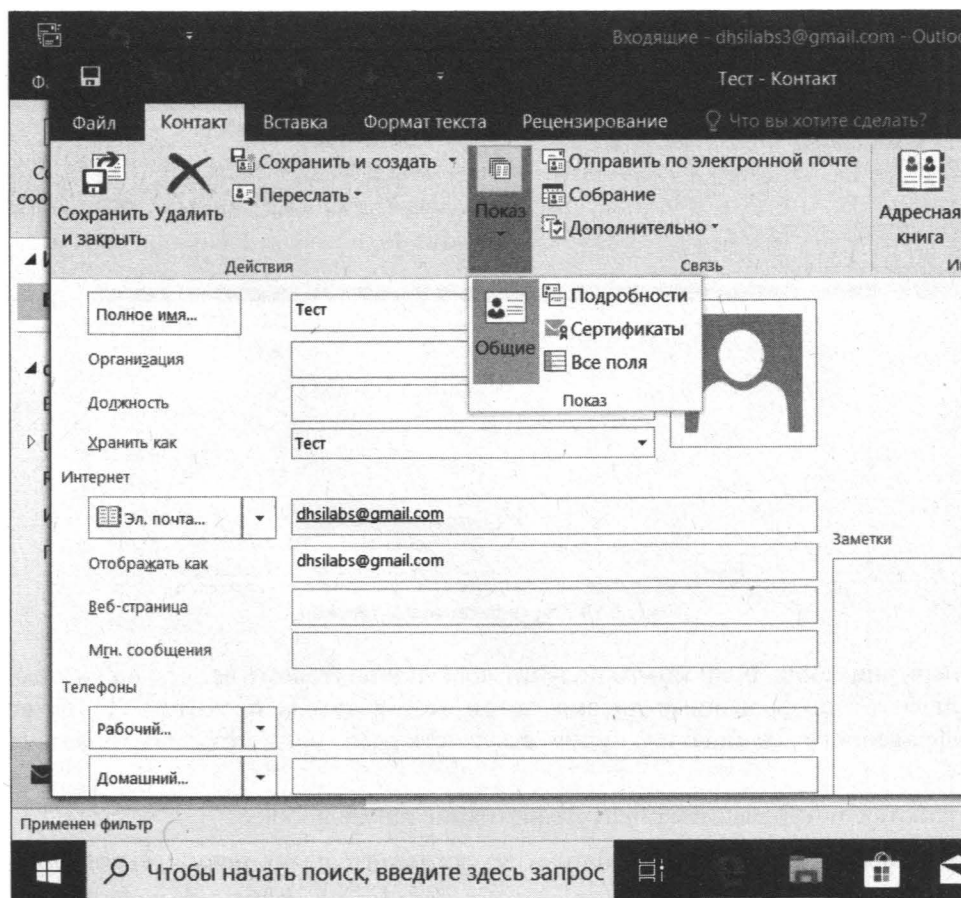
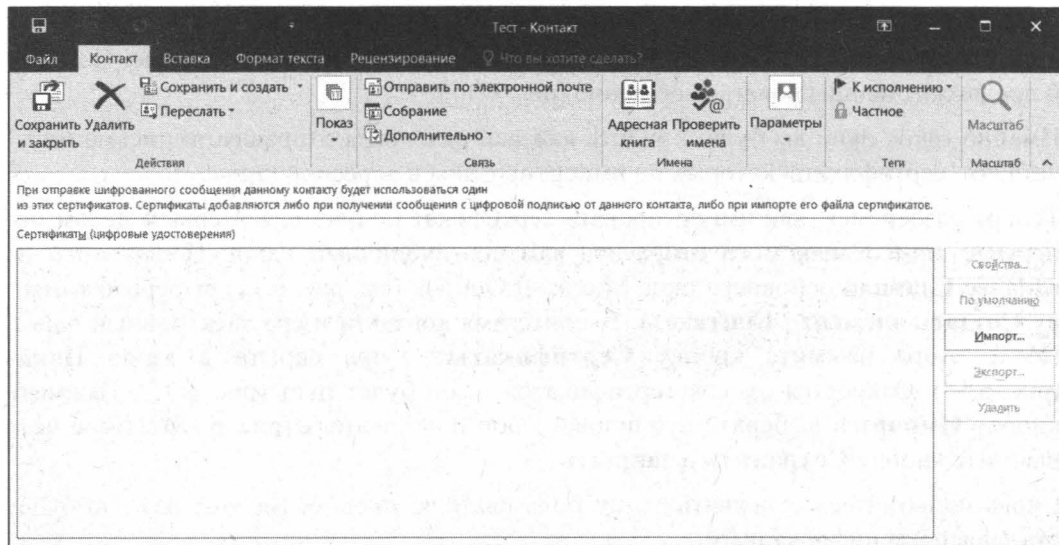
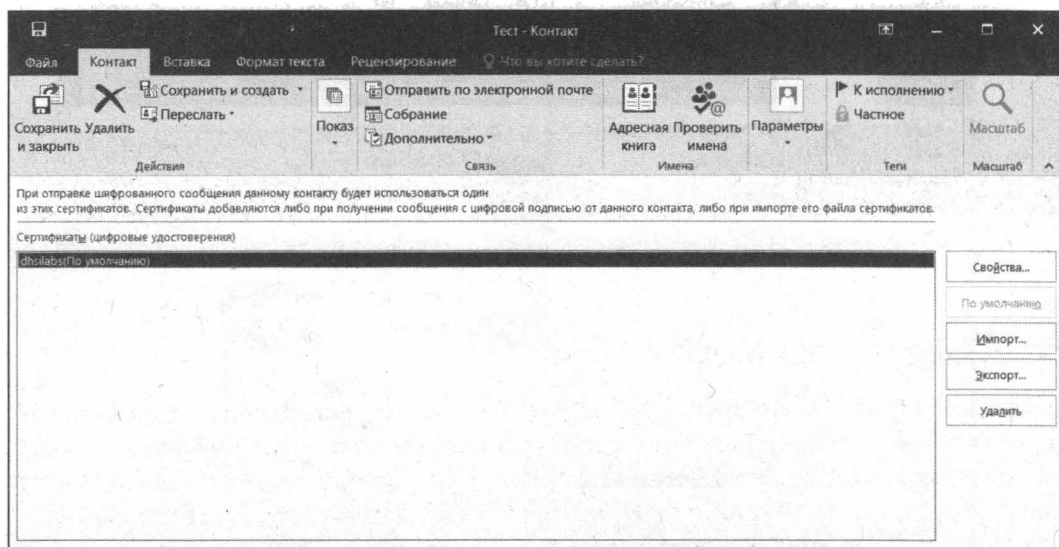


Рис. 6.16. Создание нового элемента адресной книги





**Рис. 6.17. Список сертификатов пуст**



**Рис. 6.18. Сертификат импортирован**

А теперь внимание. Если кто-то получит доступ к почтовому ящику, на который вы отправляли зашифрованные письма, то он не сможет их прочитать. Содержимое зашифрованного сообщения будет выглядеть для него так, как показано на рис. 6.19.

При работе с шифрованием обратите внимание на следующее:

- ☐ тема письма не шифруется, поэтому не указывайте в ней ничего секретного;
- ☐ при создании ключа вы указываете срок его действия. Некоторые почтовые клиенты, в том числе Outlook, не позволяют использовать старые сертификаты.

Казалось бы, что тут такого — сгенерировал новый и заново установил. Так-то оно так, но вы не сможете расшифровать сообщения, зашифрованные ключами старого сертификата. Поэтому или устанавливайте продолжительный срок действия сертификата (10 лет вместо 1 года), или же просто помните об этом, чтобы через год такое поведение почтовой программы не стало для вас сюрпризом.

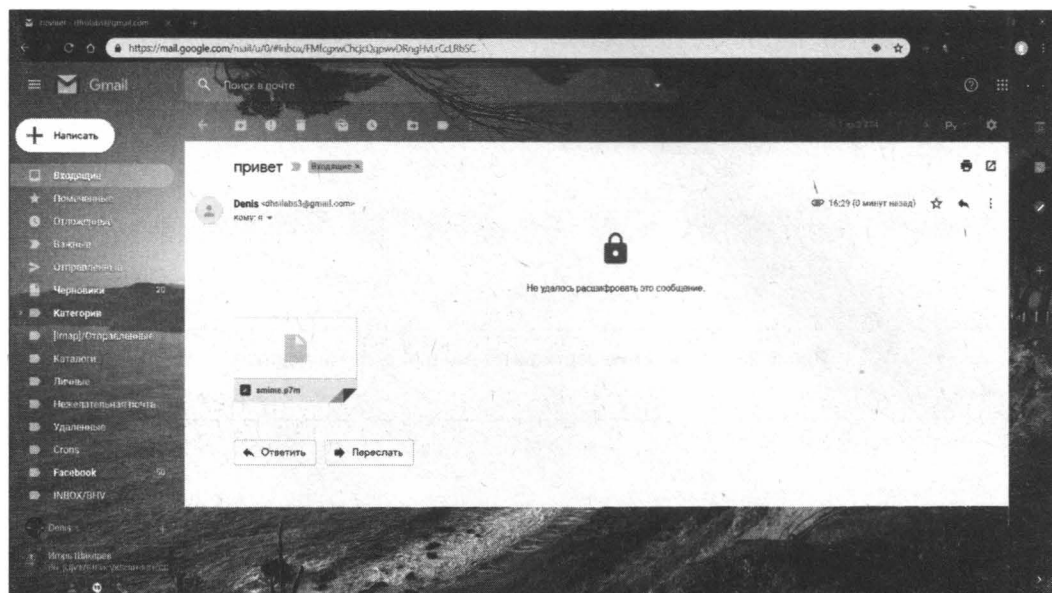


Рис. 6.19. Так увидит зашифрованное сообщение взломщик

## 6.4.2. Настройка Mozilla Thunderbird

Настройка других почтовых клиентов осуществляется аналогично. Принцип тот же — сначала нужно установить свой сертификат, потом сертификаты других пользователей. В Thunderbird нужно открыть окно **Управление сертификатами** (рис. 6.20). Для этого откройте окно настроек, перейдите на вкладку **Дополнительные**, а затем на вкладку **Сертификаты** и нажмите кнопку **Управление сертификатами**.

Перейдите на вкладку **Ваши сертификаты** и нажмите кнопку **Импортировать**. Выберите ваш сертификат. При установке сертификата программа запросит пароль сертификата — введите его. После этого сертификат появится в списке (рис. 6.21).

Как говорится, «не отходя» от кассы — пока вы еще не закрыли окно **Управление сертификатами** — перейдите на вкладку **Люди** и нажмите кнопку **Импортировать** для импорта публичных ключей других людей.

По умолчанию Thunderbird отправляет письма не зашифрованными, для шифрования нужно включить переключатель (рис. 6.22).



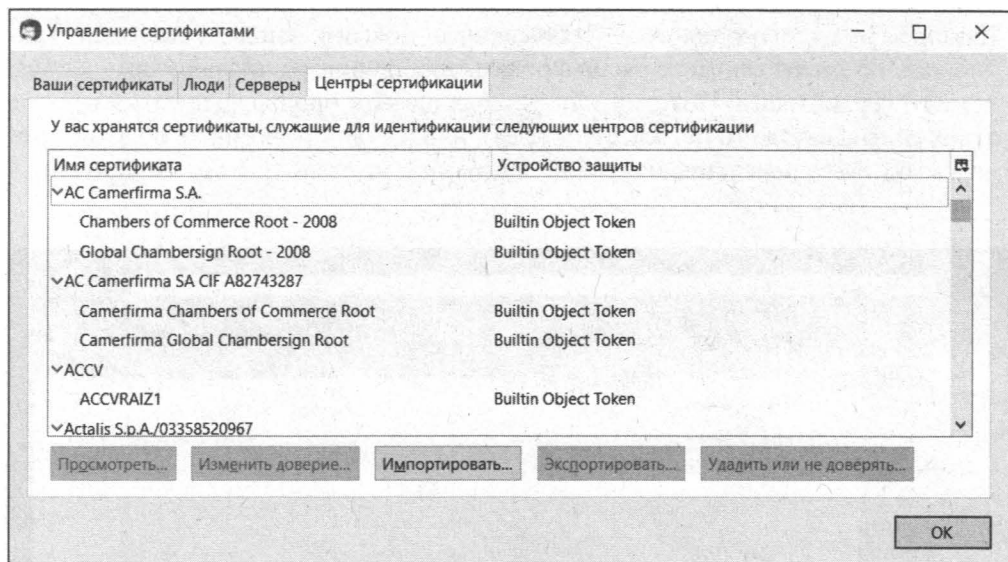


Рис. 6.20. Управление сертификатами в Mozilla Thunderbird

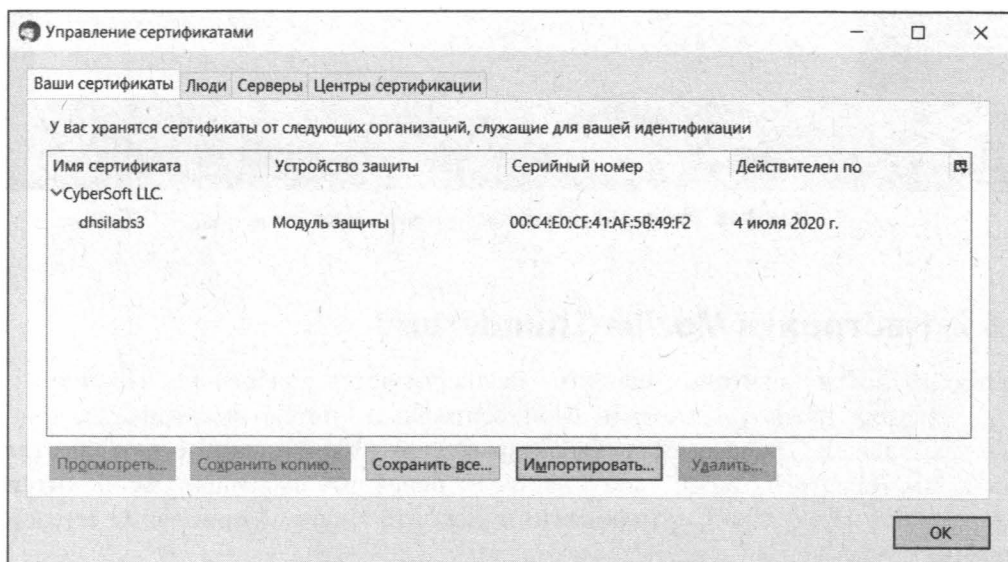


Рис. 6.21. Сертификат добавлен в список Mozilla Thunderbird

**ПРИМЕЧАНИЕ**

В почтовый клиент The Bat! встроены средства создания PGP-ключей. То есть ключи можно создать прямо из The Bat!, и никакие другие программы не нужны. Только это будет сертификат не PKI (S/MIME), 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.rtlabs.com/en/support/help/75/>.

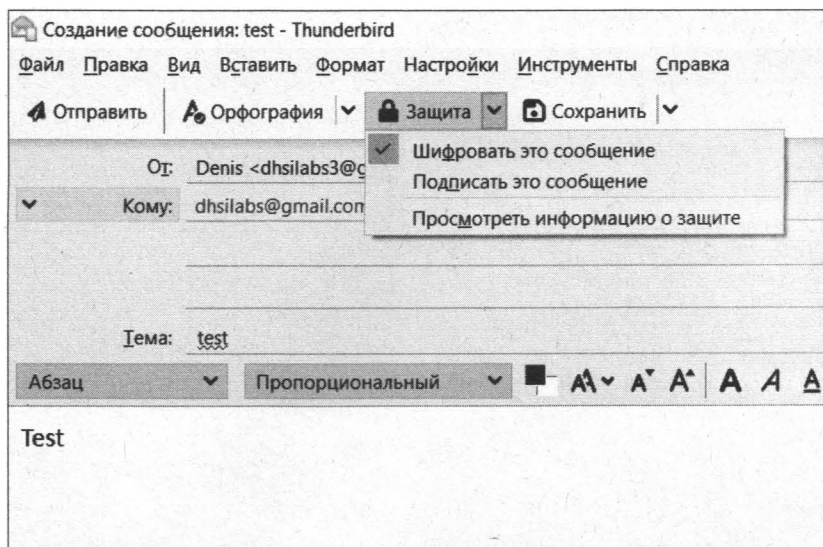


Рис. 6.22. Включаем шифрование/подпись документа в Mozilla Thunderbird



## ГЛАВА 7



# Шифрование 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 радикальное средство — 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 и еще прозрачное шифрование, когда шифруется одна из папок на жестком диске. Все файлы, помещенные в эту папку, автоматически шифруются. В этой главе мы рассмотрим все эти способы. Однако сначала нужно поговорить о выборе оптимального для вас средства защиты данных.

## 7.1. Выбор средства защиты данных

### 7.1.1. Шифрование всего диска

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

Но шифрование всего диска — далеко не самый оптимальный способ защиты данных. Во-первых, вы должны понимать, что любое шифрование данных — это, прежде всего, их преобразование, видоизменение. То есть при записи данных на диск их нужно сначала зашифровать, а для чтения — 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? Впрочем, если вы — настоящий параноик, то можете возразить: операционная система и приложения могут хранить конфиденциальные данные не только в пользовательских файлах, но и во временных файлах, в Cookies, в реестре, в файлах программ (каталог AppData).

Поэтому, когда нет времени, желания или возможности выяснить, что нужно шифровать, а что нет, часто шифруют весь жесткий диск, жертвуя производительностью.

В-третьих, нужно понимать, что даже если вы зашифровали весь жесткий диск, то зашифрованным он остается только тогда, когда компьютер выключен. Если внутри операционной системы есть источник утечки информации — т. е. программа, которая «сливает» третьим лицам ваши данные, то шифрование диска вас не спасет. После ввода пароля компьютер загрузится как обычно, и ничто не мешает этой программе «работать».

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.

### 7.1.2. Шифрование одного из разделов диска

Менее радикальный способ — шифрование одного из разделов диска. Вы можете выделить для своих секретных документов один из разделов и зашифровать его. Тогда все ваши секретные данные (и приложения — при желании) вы сможете перенести на этот раздел. Однако перенести на зашифрованный раздел пользовательский профиль, увы, не получится, т. к. далеко не все программы шифрования могут монтировать диск до входа пользователя в систему. Так что если вы опасаетесь, что кто-то сможет прочесть данные из каталога AppData вашего компьютера, лучше перестраховаться и зашифровать весь жесткий диск.

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

Если у вас на диске только один раздел, не беда. Существуют программы, которые могут «отрезать» свободное дисковое пространство и на его месте создать новый раздел. Пусть у вас есть один раздел (диск C:) размером 500 Гбайт. Из этих 500 Гбайт свободно, например, 250 Гбайт. Часть этого свободного дискового пространства можно использовать, чтобы создать новый раздел. Вы можете «отрезать», к примеру, 50 Гбайт — для секретных документов, думаю, этого более чем достаточно, после чего этот раздел можно зашифровать и использовать для хранения секретных файлов.

В качестве программы для изменения таблицы разделов я рекомендую использовать AOMEI Partition Assistant<sup>1</sup>. Эта программа гораздо компактнее всем известной платной Acronis, а работает не хуже, и ее версия Standard Edition распространяется бесплатно.

---

<sup>1</sup> См. <https://www.aomeitech.com/aomei-partition-assistant.html>.

Изменение таблицы разделов происходит без перезагрузки компьютера (если, конечно, изменяется не системный раздел).

На рис. 7.1 показана таблица разделов моего сервера (прошу прощения за «доисторические» скриншоты — они сделаны на реальной машине, а какая машина, такие и скриншоты). Для изменения размера раздела нужно щелкнуть на нем и выбрать команду меню **Partition | Resize Partition**. После этого откроется окно, в котором можно будет установить новый размер раздела (на рис. 7.2 видно, что я собираюсь «отрезать» 5,6 Гбайт дискового пространства от диска H:).

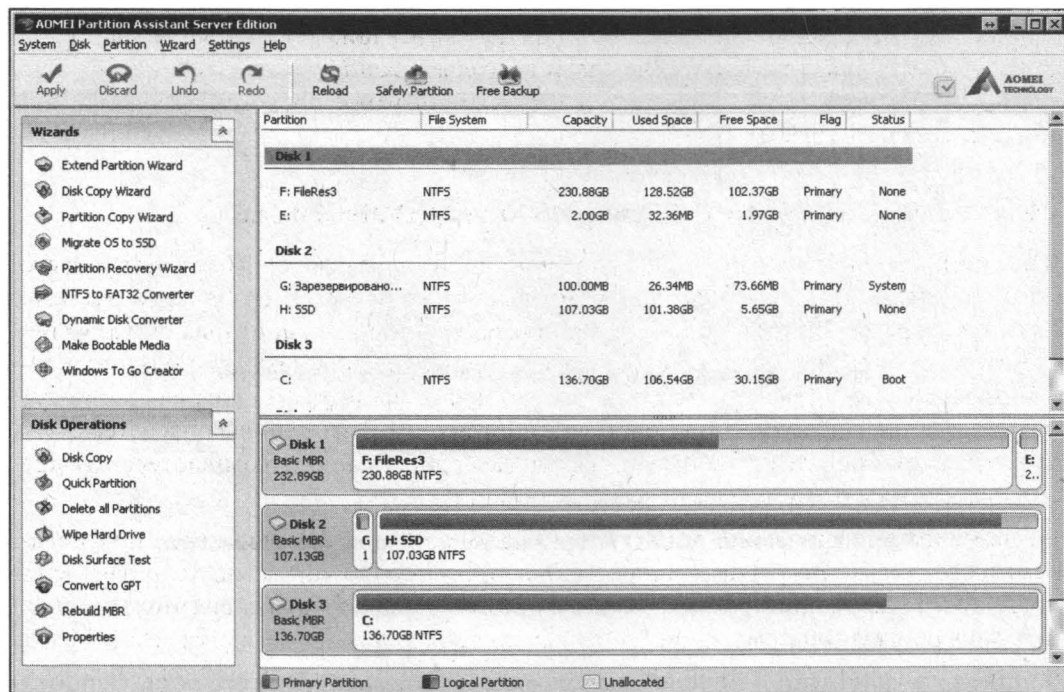


Рис. 7.1. Программа AOMEI Partition Assistant (серверная версия)

### ВНИМАНИЕ!

После шифрования изменить размер раздела будет невозможно. Поэтому сразу установите необходимый размер, возможно, с небольшим запасом (20–30%).

Когда программа уменьшит размер раздела, на жестком диске появится нераспределенная область. Далее все просто — нужно создать в ней новый раздел, для чего щелкнуть на этой области, выбрать команду меню **Partition | Create Partition**, а потом отформатировать созданный раздел как NTFS командой **Partition | Format Partition**.

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

Типичный сценарий, требующий шифрования раздела, — это совместное использование компьютера. Допустим, трое пользователей периодически работают с ком-

пьютером, жесткий диск которого имеет объем 500 Гбайт. Несмотря на то, что файловая система NTFS поддерживает права доступа и позволяет ограничить доступ одного пользователя к файлам другого, ее защиты недостаточно. Ведь у кого-то из этих трех пользователей будут права администратора, и он сможет получить доступ к файлам оставшихся двух.

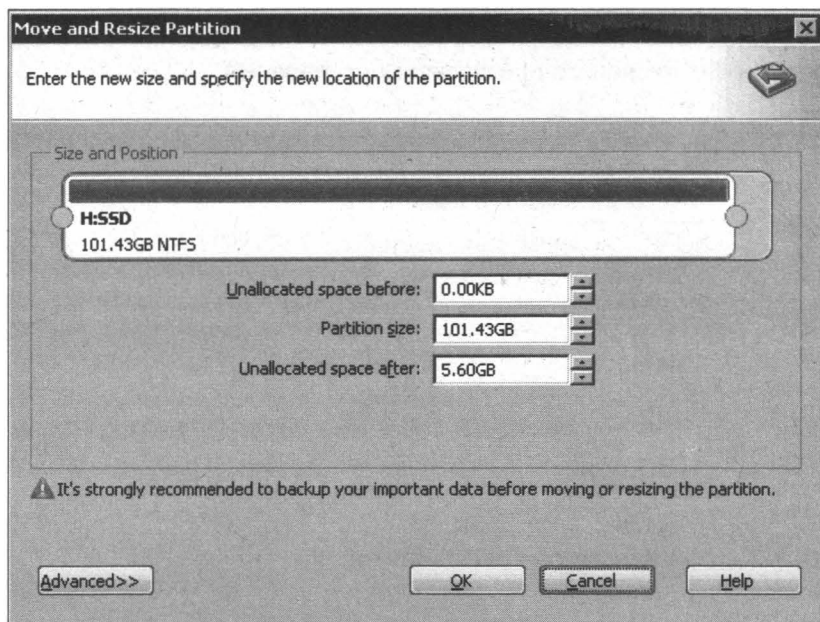


Рис. 7.2. Программа AOMEI Partition Assistant: изменение размера раздела

Поэтому дисковое пространство жесткого диска такого компьютера можно разделить следующим образом:

- ☐ примерно 200 Гбайт — общий раздел, он же системный. На него устанавливается операционная система, программы, и на нем могут храниться общие файлы всех трех пользователей;
- ☐ три раздела примерно по 100 Гбайт — думаю, 100 гигабайт вполне достаточно для хранения личных файлов каждого пользователя. Каждый из этих разделов шифруется, а пароль доступа к своему зашифрованному разделу будет знать только тот пользователь, который этот раздел и зашифровал.

И никакой администратор при всем своем желании не сможет расшифровать разделы других пользователей и получить доступ к их файлам. Да, при желании администратор может отформатировать шифрованный раздел и даже удалить его, но получить доступ к нему он сможет 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.

### 7.1.3. Криптоконтейнеры, или виртуальные диски

Далеко не всегда можно зашифровать весь жесткий диск или даже какой-либо его раздел. Типичный пример — офисный компьютер. Вы хотите скрыть свои данные от других коллег, которые, возможно, работают за этим же компьютером (общее рабочее место), но в то же время у вас нет прав администратора, которые необходимы для шифрования диска или раздела.

В этом случае на помощь придут виртуальные диски, или криптоконтейнеры. Виртуальный диск представляет собой зашифрованный файл, внутри которого находятся ваши данные: файлы и каталоги. Такой виртуальный диск можно подмонтировать к какой-нибудь букве — хоть к Z:, и работать с ним как с обычным диском. Шифрование виртуального диска так же надежно, как и шифрование разделов.

Что лучше: шифровать разделы или использовать виртуальные зашифрованные диски? Здесь каждый решает сам, поскольку у каждого способа есть свои преимущества и свои недостатки.

Преимущество виртуального диска в том, что его можно без проблем хранить на другом жестком диске или на флешке соответствующего размера. То есть вы можете создать виртуальный диск и при необходимости скопировать его файл на флешку или на внешний жесткий диск, вообще удалив его с «исходного» компьютера. 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 программа TrueCrypt. Следовательно, перенести контейнер с компьютера на смартфон — проще простого (лишь бы на SD-карте хватило места). С зашифрованным разделом у вас такое сделать 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. И когда у вас возникнет подобная потребность, рекомендую программу Clonezilla — надежное и проверенное решение. Перенос зашифрованного раздела на другой компьютер — это более сложная затея, чем перенос виртуального диска. И если есть такая необходимость, то проще использовать виртуальные диски.

Какой способ выбрать? Если вы можете себе это позволить — воспользуйтесь шифрованием раздела. Этот способ также удобен, если размер ваших секретных документов достаточно большой.

Но есть ситуации, когда создать зашифрованный раздел диска нельзя или нет смысла. Например, когда на жестком диске компьютера имеется единственный раздел (диск C:), и по тем или иным причинам (нет прав, например, поскольку компьютер не ваш) вы не можете или не хотите изменять его разметку. Что ж, тогда нужно использовать виртуальные диски. Нет также смысла шифровать целый раздел, если размер документов (файлов), которые вам нужно зашифровать, небольшой — несколько гигабайт.



### 7.1.4. 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, файлы криптоконтейнеров (виртуальных дисков), как правило, занимают сотни мегабайт дискового пространства, и их наличие весьма просто обнаружить злоумышленнику. Да, есть методы сокрытия данных, но побеждает человеческая лень. В-третьих, зашифрованная папка внутри криптоконтейнера может постоянно расти, а размер криптоконтейнера ограничен величиной, указанной при его создании. Конечно, есть программы, позволяющие изменять размер криптоконтейнеров после их создания, но на это нужно обращать внимание еще 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 таким способом папку C:\Documents и поместили в нее свои документы, то при открытии документа из этой папки запускается соответствующее приложение (Word или Excel), и оно даже не подозревает, что документ является зашифрованным. Вы работаете с зашифрованными файлами, как с самыми обычными, совершенно не задумываясь о шифровании, монтировании, виртуальных дисках и т. п.

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 придется подмонтировать весь криптоконтейнер. В результате становятся уязвимыми все остальные содержащиеся в нем файлы. Конечно, можно создать множество небольших криптоконтейнеров, присвоить каждому отдельный пароль, но это не очень удобно.

А вот в случае прозрачного шифрования можно создать столько зашифрованных папок, сколько вам нужно, и поместить в каждую из них различные группы файлов: документы, личные фото и т. п. При этом расшифровываются только те файлы, к которым осуществляется доступ, а не все файлы зашифрованной папки сразу.

Организовать прозрачное шифрование папки можно как с помощью стандартных средств Windows (Encrypted File System), так и с помощью ряда сторонних программ. В следующем разделе мы поговорим о стандартных средствах шифрования в операционных системах Windows и Linux: EFS, BitLocker и eCryptfs. Мы также разберемся, как злоумышленник может расшифровать файлы, зашифрованные EFS.

## 7.2. Шифрование стандартными средствами операционной системы

### 7.2.1. Прозрачное шифрование с помощью EFS

#### Преимущества и недостатки EFS

В Windows (начиная с Windows 2000 и кроме Home-выпусков) для организации прозрачного шифрования традиционно 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 для того, 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 достаточно безопасной файловой системой, но со временем появились различные утилиты (одной из первых была NTFSDDOS, позволяющая читать файлы, находящиеся на NTFS-разделе, из DOS-окружения), игнорирующие права доступа NTFS. Поэтому 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 требуется какое-либо дополнительное программное обеспечение, — все необходимое уже есть в Windows. И чтобы пользоваться шифрованием файлов, нет необходимости совершать какие-либо предварительные действия, поскольку при первом шифровании файла для пользователя автоматически создается сертификат шифрования и закрытый ключ.

Преимуществом EFS является и то, что при перемещении файла из зашифрованной папки в любую другую он остается зашифрованным, а при копировании файла в зашифрованную папку он автоматически шифруется. Ничего специально для этого предпринимать не надо.

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, из-за сбоя жесткого диска повреждены системные файлы (bad sectors). Конечно, чтобы скопировать с жесткого диска хранящиеся на нем файлы, можно его извлечь и подключить к другому компьютеру, но если эти файлы 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. Впрочем, 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 к недостаткам отнести сей факт, — такое ПО позволяет восстановить доступ к данным, но оно же может использоваться злоумышленником для получения несанкционированного доступа к зашифрованным файлам.

Казалось бы, данные с помощью EFS зашифрованы очень надежно. Сами файлы на диске шифруются с помощью ключа FEK (File Encryption Key), который хранится в атрибутах файлов. Ключ 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 утилитой SYSKEY<sup>1</sup>.

Казалось бы, такая цепочка шифрования должна 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) — т. е. 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 (например, Advanced EFS Data Recovery<sup>2</sup>), 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

---

<sup>1</sup> SYSKEY — утилита, которая шифрует информацию хэшированного пароля в базе данных SAM в системе Windows, используя 128-битный ключ шифрования.

<sup>2</sup> См. <http://www.elcomsoft.ru/aefedr.html>.

файловых систем. Если вы скопируете зашифрованный файл на файловую систему, которая не поддерживает шифрование — например, на FAT/FAT32, файл будет дешифрован, и его смогут просмотреть все желающие. Ничего удивительного в этом нет, EFS — всего лишь надстройка над NTFS.

Получается, что от EFS вреда больше, чем пользы. Использовать или не использовать EFS — решать вам. С одной стороны, это удобно. С другой — не всегда безопасно. Далее будет показано, как включить EFS.

## Шифрование с помощью EFS

Приступая к шифрованию файлов с помощью EFS, нужно учитывать несколько моментов. Так, зашифрованные ею файлы открыть на другом компьютере невозможно: ни вы их не откроете, не откроет их и никто иной, — пусть он как-либо скопирует зашифрованную вами папку или даже украдет весь жесткий диск. Не сможете вы добраться до своих зашифрованных файлов и после переустановки Windows — если только не выполнили предварительно резервное копирование сертификатов.

Лучше всего шифровать не отдельные файлы, а создать папку, поместить туда все файлы, которые вы хотите зашифровать, и зашифровать эту папку. Но помните, что

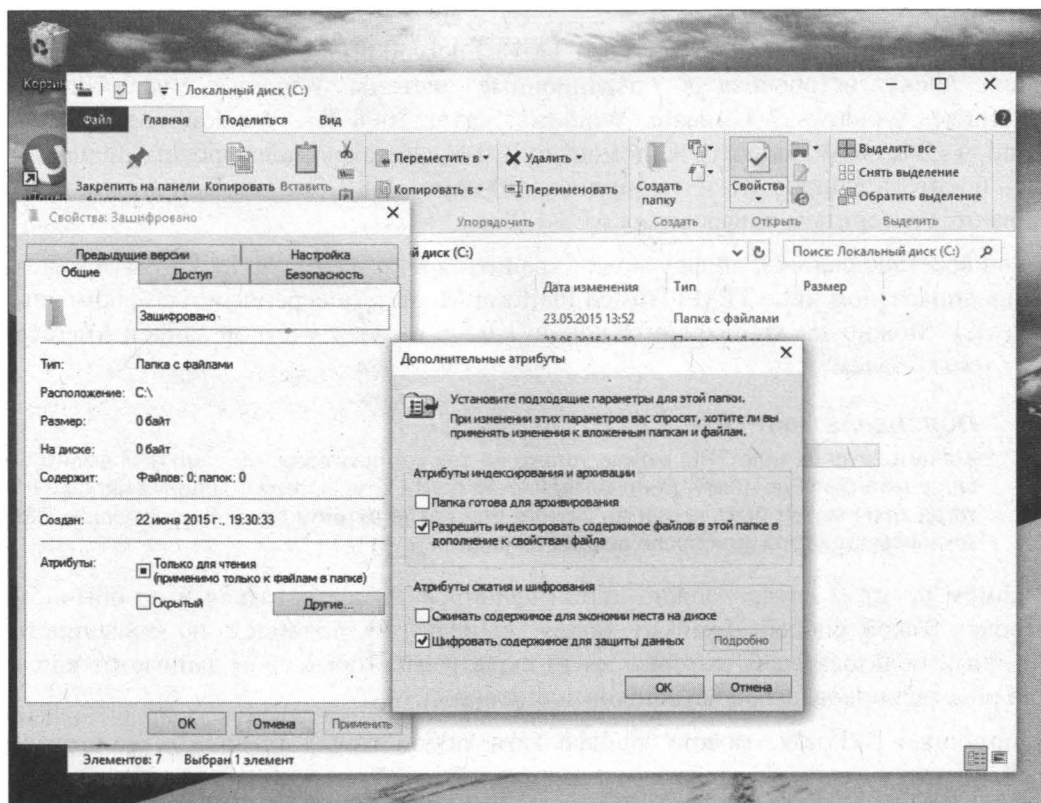


Рис. 7.3. Включение шифрования EFS

при копировании зашифрованных объектов на диски, которые не поддерживают шифрование, — например, на раздел FAT32 или на флешку, объекты эти окажутся автоматически расшифрованы. Не следует и шифровать все файлы подряд, иначе система будет изрядно «подтормаживать», — ведь ей тогда придется все файлы расшифровывать «на лету».

Для шифрования объекта (папки или файла — последовательность действий будет той же) щелкните на нем правой кнопкой мыши, выберите из контекстного меню команду **Свойства**, в области **Атрибуты** открывшегося окна свойств нажмите кнопку **Другие**, включите атрибут **Шифровать содержимое для защиты данных** (рис. 7.3) и нажмите кнопку **ОК**, а затем еще раз кнопку **ОК** в окне свойств папки.

Система спросит, нужно ли шифровать только эту папку или все вложенные папки и файлы. Лучше выбрать второй вариант — **К данной папке и ко всем вложенным папкам и файлам**.

Все, осталось только подождать, пока файлы будут зашифрованы. Название зашифрованной папки в Проводнике будет выделено зеленым шрифтом.

## 7.2.2. Шифрование диска с помощью BitLocker

### 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, Windows 8/8.1 и Windows 10. С помощью BitLocker можно зашифровать полностью весь носитель данных: логический диск, SD-карту, USB-брелок. При этом поддерживаются алгоритмы шифрования AES-128 и AES-256.

Ключ восстановления к шифру может храниться в компьютере, на USB-устройстве или в аппаратном чипе TPM (Trusted Platform Module, доверенный платформенный модуль). Можно также сохранить копию ключа в своей учетной записи Microsoft (вот только зачем?).

#### **Пояснение: чип TPM**

Хранить ключ в чипе TPM можно только на тех компьютерах, где чип TPM смонтирован в материнскую плату. Если материнская плата компьютера оснащена чипом TPM, тогда ключ может быть прочитан из него или после аутентификации с помощью USB-ключа/смарт-карты, или после ввода PIN-кода.

В самом простом случае можно аутентифицировать пользователя и по обычному паролю. Такой способ Джеймсу Бонду, конечно, не подойдет, но большинству обычных пользователей, которые хотят скрыть некоторые свои данные от коллег или родственников, его будет вполне достаточно.

С помощью BitLocker можно зашифровать любой том, в том числе и загрузочный, — тот, с которого происходит загрузка Windows. Тогда пароль нужно будет вводить при загрузке (или использовать другие средства аутентификации — например, тот же TPM).

**СОВЕТ**

Я настоятельно не рекомендую вам шифровать загрузочный том. Во-первых, снижается производительность. На сайте <http://technet.microsoft.com> сообщают, что обычно снижение производительности составляет в этом случае 10%, однако в вашем конкретном случае можно ожидать большего «торможения» компьютера — все зависит от его конфигурации. Да и шифровать, по сути, нужно далеко не все данные. Зачем шифровать те же программные файлы? — в них нет ничего конфиденциального. Во-вторых, если что-то случится с Windows, боюсь, все может закончиться плачевно — форматированием тома и потерей данных.

Поэтому лучше всего зашифровать один какой-то том — отдельный логический диск, внешний USB-диск и т. п., а затем на этот зашифрованный диск поместить все ваши секретные файлы, в том числе и установить программы, требующие защиты, — например, ту же «1С:Бухгалтерию». Такой диск вы будете подключать только при необходимости: щелкнул двойным щелчком на значке диска, ввел пароль — и получил доступ к данным.

**Что можно зашифровать, а что — нет?**

Можно зашифровать любой диск, кроме сетевого и оптического. Вот список поддерживаемых типов подключения дисков: USB, Firewire, SATA, SAS, ATA, IDE, SCSI, eSATA, iSCSI, Fiber Channel.

Не поддерживается шифрование томов, подключенных по Bluetooth. И пусть карта памяти мобильного телефона, подключенного к компьютеру по Bluetooth, выглядит как отдельный носитель данных, зашифровать ее нельзя.

Поддерживаются файловые системы: NTFS, FAT32, FAT16, ExFAT. Не поддерживаются прочие файловые системы, в том числе: CDFS, NFS, DFS, LFS, программные RAID-массивы (аппаратные RAID-массивы поддерживаются).

Можно зашифровать твердотельные накопители: (SSD-накопители, флешки, SD-карты), жесткие диски (в том числе, подключаемые по USB). Шифрование других типов дисков не поддерживается.

**СОВЕТ**

Перед тем как приступить непосредственно к самому процессу шифрования, настоятельно рекомендую ознакомиться со следующей ссылкой, где приведены часто задаваемые вопросы (и ответы на них) других пользователей: <http://technet.microsoft.com/ru-ru/library/hh831507.aspx>.

**Шифруем диск с помощью BitLocker**

Перейдите на рабочий стол, запустите Проводник и щелкните правой кнопкой мыши на диске, который хотите зашифровать. Напомню, что это может быть логический том, SD-карта, флешка, USB-диск, SSD-накопитель. Из открывшегося контекстного меню выберите команду **Включить BitLocker** (рис. 7.4).

Вас, прежде всего, спросят, 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. 7.5).

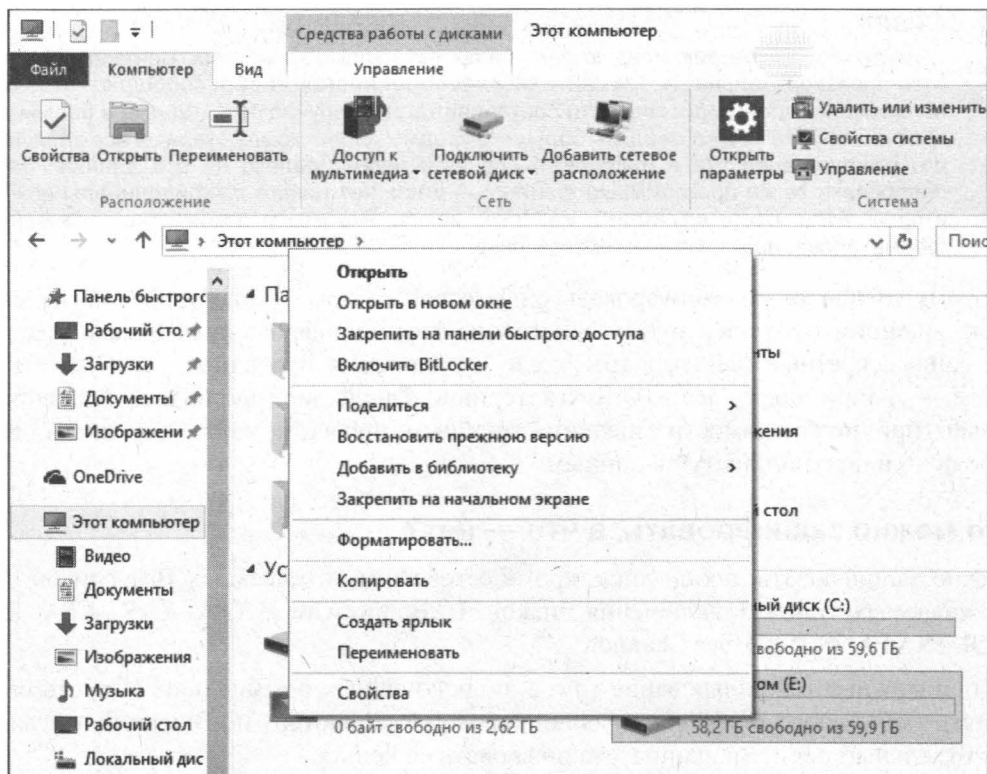


Рис. 7.4. Команда включения BitLocker

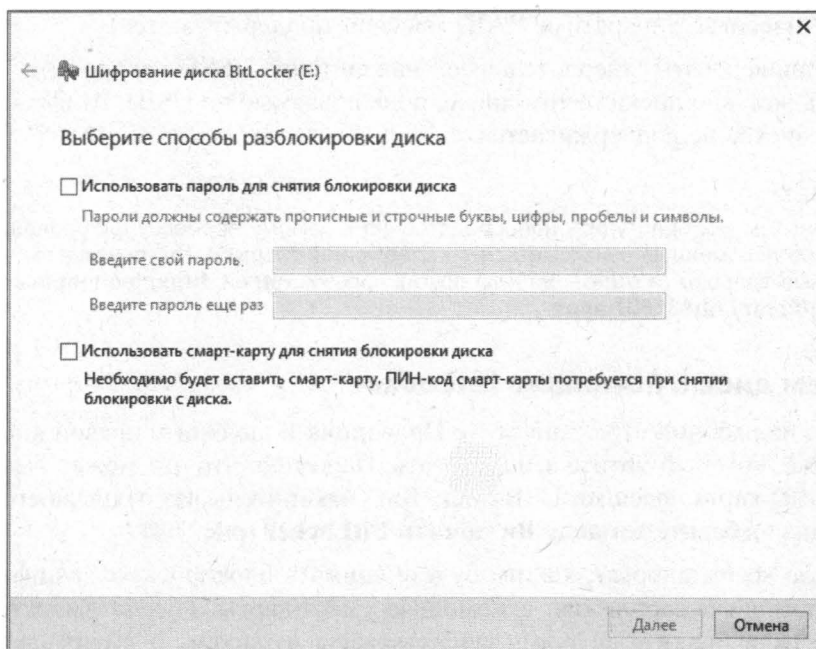


Рис. 7.5. Как будем снимать блокировку?



На следующем шаге вам будет предложено создать резервную копию ключа восстановления (рис. 7.6, а):

#### **ПОЯСНЕНИЕ: КЛЮЧ ВОССТАНОВЛЕНИЯ**

Ключ восстановления используется для разблокировки диска в случае, когда вы забыли пароль или потеряли смарт-карту. Отказаться от создания ключа восстановления нельзя. И это правильно — ситуации бывают разные. Например, вернувшись как-то из отпуска, я обнаружил, что забыл свой пароль к зашифрованному диску. Подобная же ситуация может повториться и у вас. Поэтому выбираем один из предложенных способов архивирования ключа восстановления.

- ☐ сохранение ключа в учетную запись Майкрософт. Этот способ я не рекомендую: нет соединения с Интернетом — получить свой ключ не удастся;
- ☐ сохранение в файл — оптимальный способ: файл с ключом восстановления будет записан на рабочий стол (рис. 7.6, б).

Сами понимаете, его оттуда следует перенести в более надежное место, — например, на флешку. Также желательно его переименовать, чтобы по имени файла не было сразу понятно, что это как раз тот самый ключ. Можно открыть этот файл (позже вы увидите, как он выглядит) и скопировать сам ключ восстановления в какой-либо другой файл — чтобы только вы знали, что это за строка и в каком файле она находится. Оригинальный файл с ключом восстановления лучше потом удалить — так будет надежнее;

- ☐ распечатка ключа восстановления — идея довольно дикая, разве что потом вы поместите этот лист бумаги в сейф и закроете на семь замков.

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

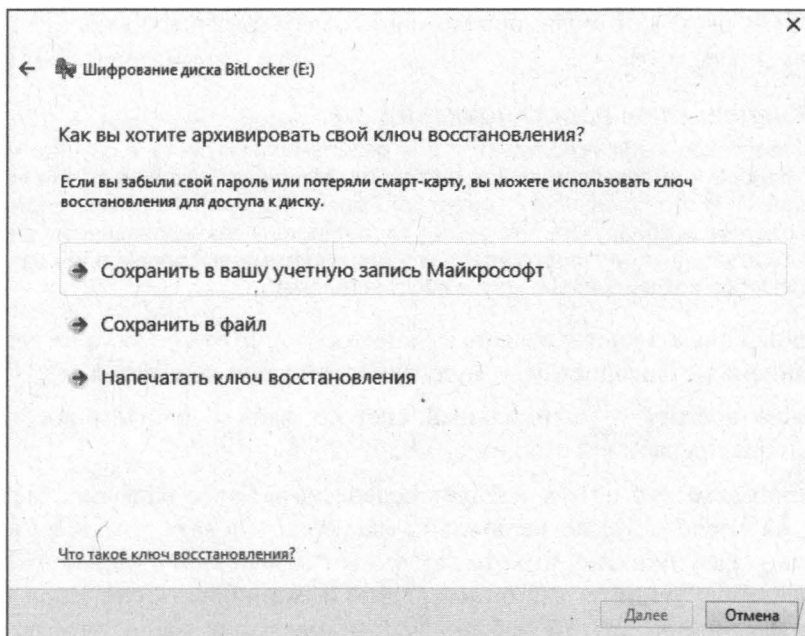
Здесь нужно определить, какую часть диска требуется шифровать (рис. 7.7). Можно зашифровать только занятое место, а можно — сразу весь диск. Если ваш диск практически пуст, то намного быстрее зашифровать только занятое место. Рассмотрим варианты:

- ☐ пусть на флешке в 16 Гбайт имеется всего 10 Мбайт данных — выберите первый вариант, и диск будет зашифрован мгновенно. Новые же файлы, записываемые на флешку, будут шифроваться «на лету», т. е. автоматически;
- ☐ второй вариант подойдет, если на диске много файлов, и он почти полностью заполнен. Впрочем, для той же 16-гигабайтной флешки, но заполненной до 15 Гбайт, разница во времени шифрования по первому или второму вариантам будет практически неразличима (что 15 Гбайт, что 16 — будут шифроваться практически в одно и то же время);
- ☐ однако если на диске мало данных, а вы выбрали второй вариант, то шифрование будет длиться по сравнению с первым способом мучительно долго.

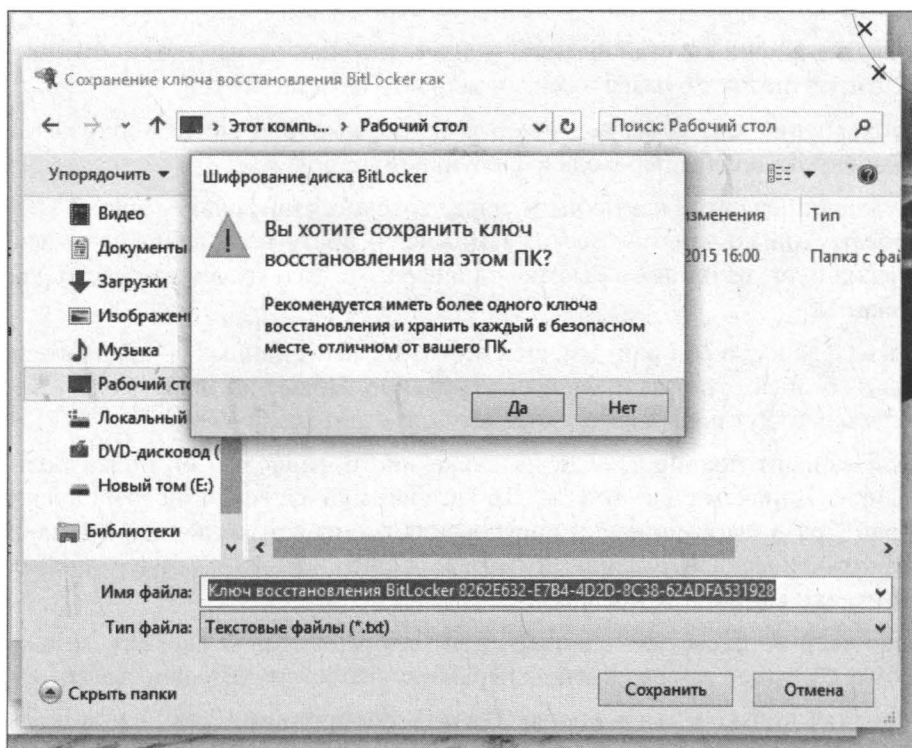
Итак, осталось только нажать кнопку **Начать шифрование** (рис. 7.8) и дождаться, пока диск будет зашифрован.

Не выключайте питание компьютера и не перезагружайте его до тех пор, пока шифрование не завершится — об этом вы получите соответствующее сообщение.





а



б

Рис. 7.6. Создание резервной копии ключа восстановления: а — архивация ключа восстановления; б — сохранение ключа восстановления на рабочем столе

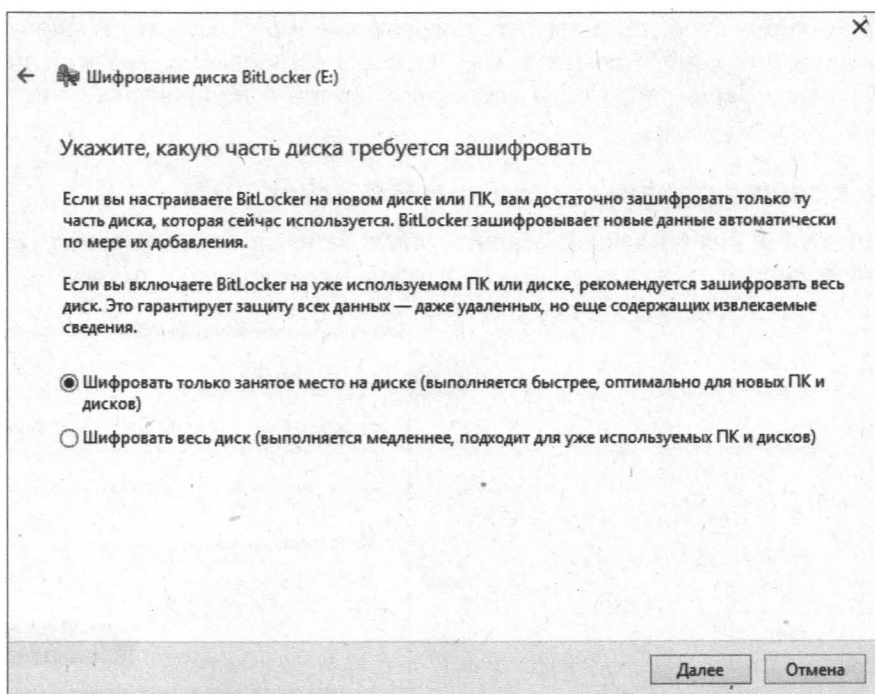


Рис. 7.7. Какую часть диска нужно зашифровать?

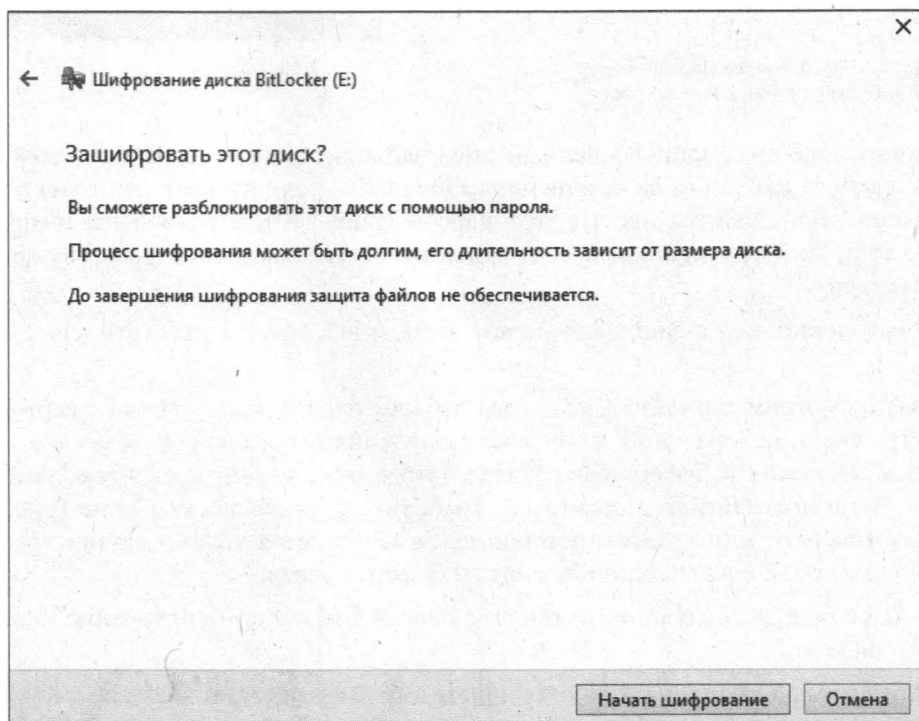


Рис. 7.8. Нажмите кнопку Начать шифрование

Если произойдет сбой питания, то шифрование при запуске Windows будет продолжено с того самого момента, где оно было остановлено, — так написано на сайте Microsoft. Верно ли это для системного диска, я не проверял — не захотел рисковать.

## Работа с зашифрованным диском BitLocker

В Проводнике Windows зашифрованный диск помечен значком замка (рис. 7.9): у заблокированного диска замок закрыт, у разблокированного — открыт.

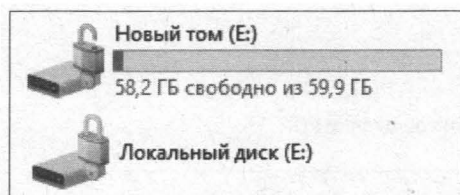


Рис. 7.9. Разблокированный (вверху) и заблокированный (внизу) диски

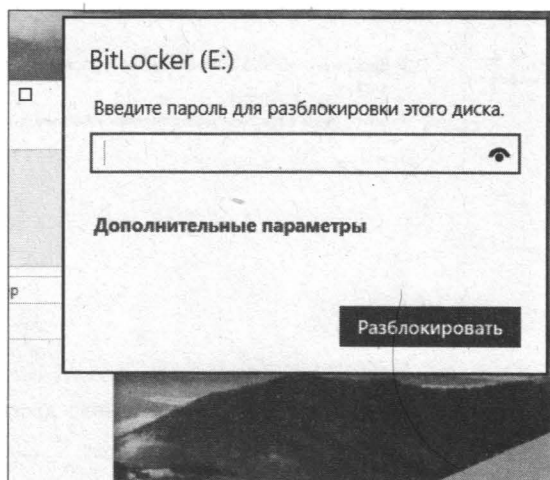


Рис. 7.10. Разблокировка диска

Свежеподключенный зашифрованный диск заблокирован, и, чтобы его разблокировать, следует щелкнуть на нем двойным щелчком. Если вы выбрали только защиту паролем, понадобится ввести этот пароль (рис. 7.10), 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.

Теперь рассмотрим ситуацию, когда вы забыли пароль или утеряли смарт-карту. Откройте файл, содержащий ключ восстановления (рис. 7.11), и возьмите содержащийся там ключ в буфер обмена. Нажмите в окне ввода пароля (см. рис. 7.10) кнопку **Дополнительные параметры**. Выберите в открывшемся окне (рис. 7.12) команду **Введите ключ восстановления**. Вам останется только вставить в соответствующее поле ключ восстановления из буфера обмена.

Рассмотрим еще две ситуации: изменение пароля BitLocker и управление зашифрованным диском.

Щелкните правой кнопкой на разблокированном зашифрованном диске и найдите в открывшемся контекстном меню (рис. 7.13) команды: **Изменить пароль BitLocker** и **Управление BitLocker**.

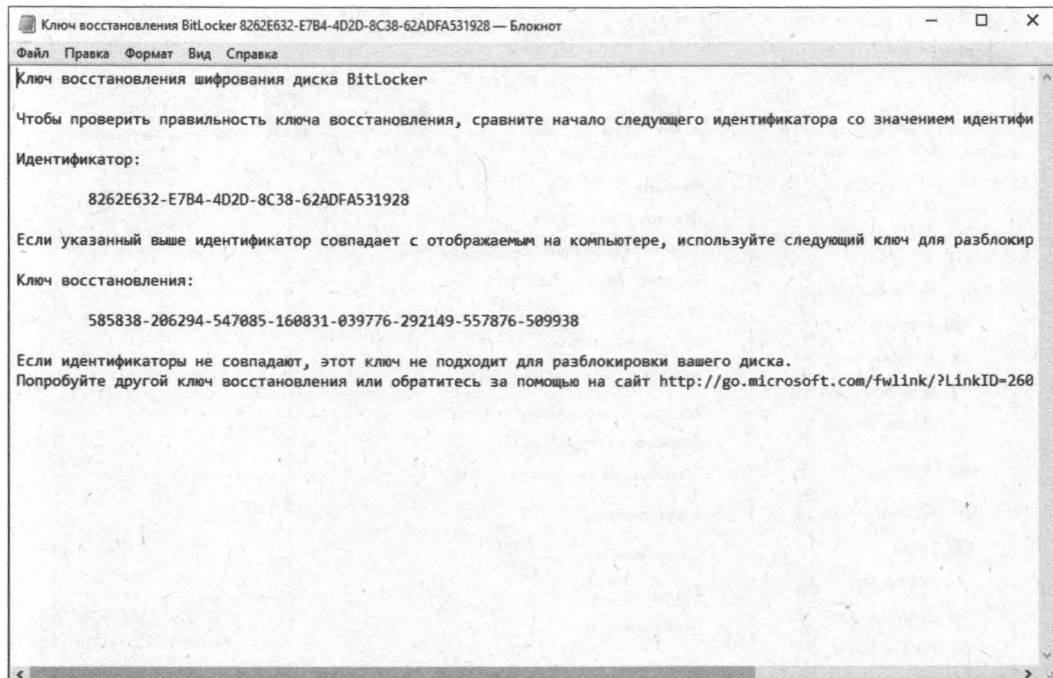


Рис. 7.11. Файл с ключом восстановления

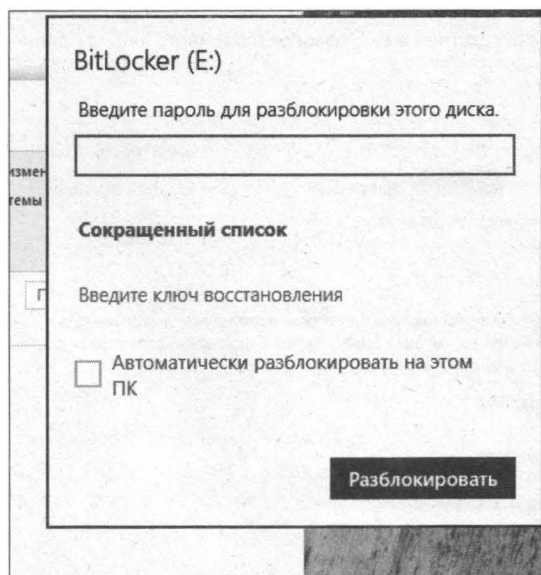


Рис. 7.12. Окно дополнительных параметров разблокировки диска

Первая команда, как вы уже догадались, позволяет изменить пароль для разблокировки зашифрованного диска. Процедура смены пароля обычная: нужно ввести старый пароль, новый пароль и его подтверждение (рис. 7.14).

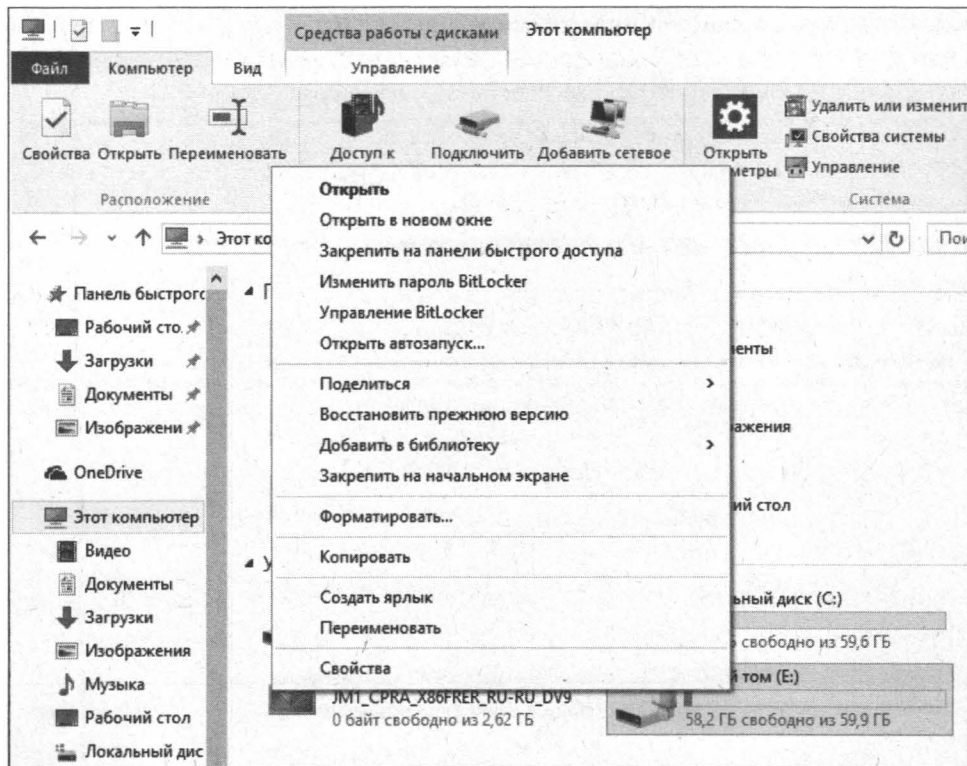


Рис. 7.13. Контекстное меню разблокированного зашифрованного диска

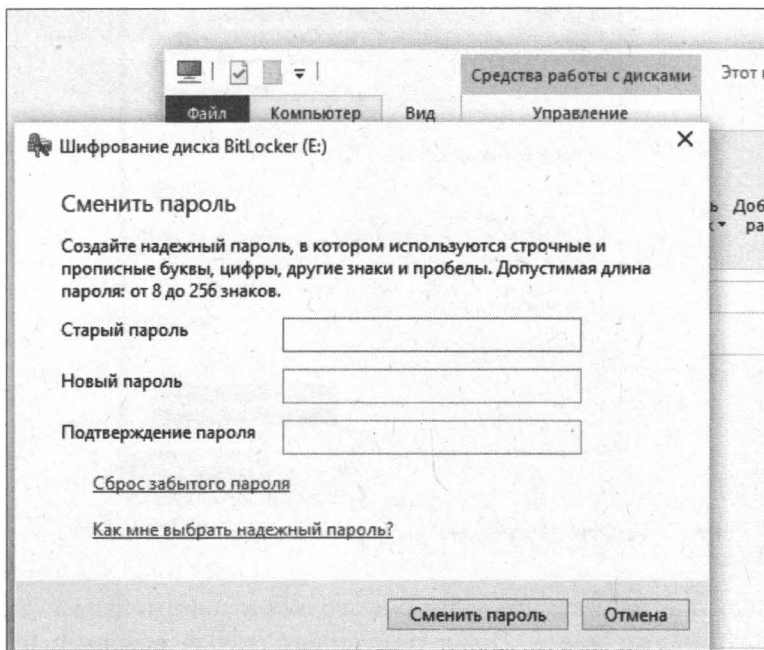


Рис. 7.14. Смена пароля для разблокировки зашифрованного диска

Выберите теперь команду **Управление BitLocker** (см. рис. 7.13). В открывшемся окне (рис. 7.15) вы увидите список как незашифрованных, так и зашифрованных дисков. Для зашифрованного диска доступны следующие команды:

- ☐ **Архивировать ключ восстановления** — если вы потеряли файл с ключом восстановления, вы можете сделать его копию в любой момент (естественно, пока вы еще помните пароль разблокировки);
- ☐ **Сменить пароль** — с этой командой вы уже знакомы;
- ☐ **Удалить пароль** — удаляет пароль, но перед этим нужно выполнить команду **Добавить смарт-карту**. Иначе, если удалить пароль, то как потом будет осуществляться доступ к зашифрованному диску;
- ☐ **Добавить смарт-карту** — добавляет смарт-карту, которая будет использоваться для разблокировки диска. Если раньше был добавлен пароль, то для разблокировки диска теперь понадобятся и смарт-карта, и пароль.

Если хотите использовать только лишь смарт-карту, тогда добавьте ее, а потом удалите пароль;

- ☐ **Включить автоматическую разблокировку** — позволяет включить автоматическую разблокировку диска на этом компьютере;

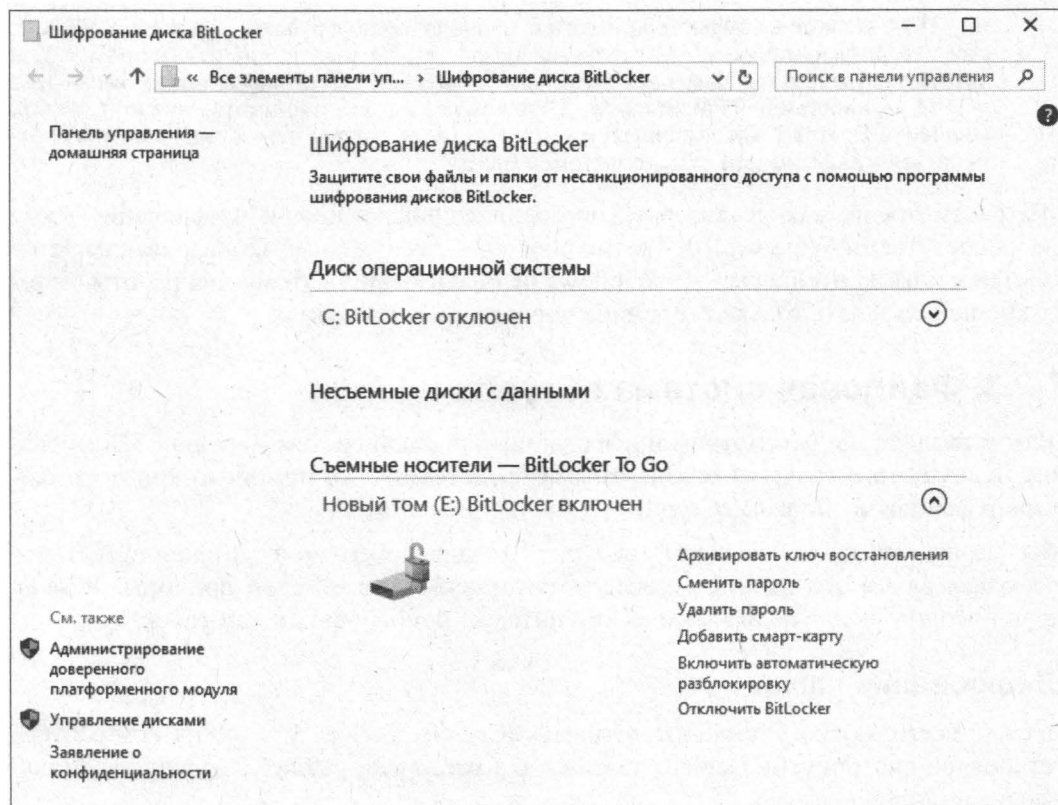


Рис. 7.15. Управление зашифрованным диском

- ❑ **Отключить BitLocker** — отключает шифрование. После этого данные на диске перестанут быть зашифрованными, и вводить пароль для разблокирования диска более не понадобится.

Команда **Администрирование доверенного платформенного модуля** позволяет управлять TPM-чипом, если таковой имеется в вашем компьютере. У меня его не оказалось, поэтому вместо консоли управления я увидел сообщение о том, что TPM-чип не найден (рис. 7.16).

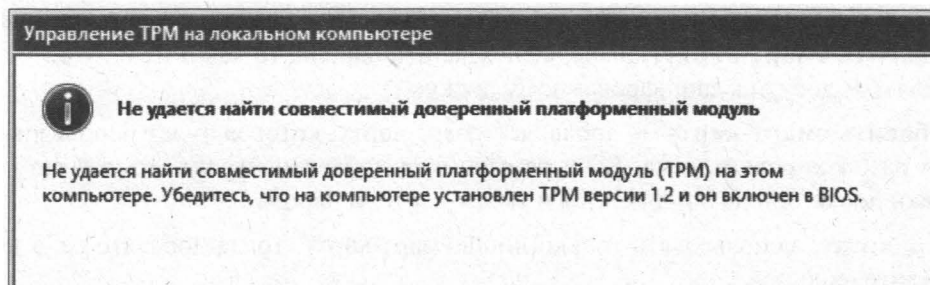


Рис. 7.16. TPM-чип не найден

### **ВНИМАНИЕ! ВКЛЮЧЕНИЕ ЧИПА TPM**

Чип TPM, если он в компьютере имеется, сначала нужно включить через BIOS SETUP. Изучите документацию по материнской плате, чтобы узнать, как это сделать. Если читать документацию вам не с руки, ищите в BIOS SETUP параметры, связанные с TPM, — например: **TPM Security**, **TPM Activation**. Эти параметры нужно включить (значения **Enabled**, **On**, **Activated** и т. п.). Названия параметров и значений могут отличаться в зависимости от используемой BIOS.

Мы рассмотрели, как реализовать прозрачное шифрование и шифрование всего диска средствами Windows 10. Третий способ — виртуальные зашифрованные диски, или криптоконтейнеры — в Windows не реализован, поэтому для работы с ним нужно использовать только сторонние программные продукты.

## **7.2.3. Файловая система eCryptfs в Linux**

В этом разделе мы рассмотрим шифровании файловой системы в Linux. Шифрование будет осуществляться стандартными средствами — с помощью криптографической файловой системы eCryptfs.

Мы познакомимся с системой eCryptfs и зашифруем мой домашний каталог `/home/den`. Зачем это делать, объяснять не стану — у всех свои причины. У меня причина одна — сугубо академический интерес: попробовать и вам рассказать.

### **Шифрование папки**

Прежде всего нужно установить утилиты eCryptfs. Сейчас у меня на компьютере установлен дистрибутив Debian, поэтому для установки утилит eCryptfs я воспользуюсь командой `apt-get`:

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



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

```
sudo cp -pfr /home/den /tmp
```

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

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

Вывод будет таким (полужирным шрифтом выделено то, что нужно ввести или сделать вам):

Passphrase: **<секретная фраза>**

Select cipher:

- 1) aes: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
- 2) blowfish: blocksize = 16; min keysize = 16; max keysize = 56 (not loaded)
- 3) des3\_ede: blocksize = 8; min keysize = 24; max keysize = 24 (not loaded)
- 4) twofish: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
- 5) cast6: blocksize = 16; min keysize = 16; max keysize = 32 (not loaded)
- 6) cast5: blocksize = 8; min keysize = 5; max keysize = 16 (not loaded)

Selection [aes]: просто нажмите Enter (aes по умолчанию)

Select key bytes:

- 1) 16
- 2) 32
- 3) 24

Selection [16]: **нажмите Enter**

Enable plaintext passthrough (y/n) [n]: n

Enable filename encryption (y/n) [n]: n

Attempting to mount with the following options:

```
ecryptfs_unlink_sigs
ecryptfs_key_bytes=16
ecryptfs_cipher=aes
ecryptfs_sig=bd28c38da9fc938b
```

WARNING: Based on the contents of [/root/.ecryptfs/sig-cache.txt], it looks like you have never mounted with this key before. This could mean that you have typed your passphrase wrong.

Would you like to proceed with the mount (yes/no)? : **yes**

Would you like to append sig [bd28c38da9fc938b] to  
[/root/.ecryptfs/sig-cache.txt]

in order to avoid this warning in the future (yes/no)? : **yes**

Successfully appended new sig to user sig cache file

Mounted eCryptfs

Теперь разберемся, какие опции здесь указаны. Мы согласились на использование алгоритма по умолчанию: AES. Если вы считаете, что другой алгоритм лучше, можете выбрать его. Также мы отказались от шифрования имен файлов (Enable



filename encryption): если что-то случится с зашифрованным каталогом, то разобраться, где и какой файл, будет сложно.

Итак, каталог `/home/den` зашифрован. Восстановим наш бэкап и удалим его (чтобы никто не смог его прочитать):

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

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/den
```

Размонтируем зашифрованный каталог:

```
sudo umount /home/den
```

Теперь пробуем прочитать `/home/den/motd`:

```
cat /home/den/motd
```

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

## Храним пароль на флешке

Шифрование работает, но каждый день (точнее, после каждой перезагрузки/загрузки системы) вам надоест вводить секретную фразу. Нужно позаботиться об автоматическом монтировании. Но где при этом будет храниться пароль? На жестком диске? Но тогда нет смысла в самом шифровании. Это все равно, что установить пароль и написать его на желтой бумажке, приклеенной к монитору.

Мы, как обычно, найдем рациональное решение и станем хранить секретную фразу на флешке с файловой системой FAT32. Секретная фраза будет храниться на ней в незашифрованном виде, поэтому постарайтесь, чтобы флешка не попала к врагу. Двойное шифрование (т. е. и домашнего каталога, и флешки) возможно, но оно выходит за рамки этой книги.

Первым делом нужно подмонтировать флешку:

```
sudo mkdir /mnt/usb  
sudo mount /dev/sdb1 /mnt/usb
```

Затем нужно заглянуть в файл `/root/.ecryptfs/sig-cache.txt`. Найдите там кэш подписи — он выглядит примерно так: `da51c78bc1fc726d`. Запишите это значение.

Откройте файл `/root/.ecryptfsrc` и добавьте в него следующие строки:

```
key=passphrase:passphrase_passwd_file=/mnt/usb/secret.txt  
ecryptfs_sig=da51c78bc1fc726d  
ecryptfs_cipher=aes  
ecryptfs_key_bytes=16  
ecryptfs_passthrough=n  
ecryptfs_enable_filename_crypto=n
```

Параметр `key` задает имя файла с паролем, второй параметр — подпись из файла `sig-cache.txt`. Остальные параметры задают тип шифрования, размер ключа и устанавливают прочие режимы `ecryptfs`.

Создайте файл `/mnt/usb/secret.txt` и добавьте в него строку:

```
passphrase_passwd=<секретная фраза>
```

Осталось совсем немного — обеспечить автоматическое монтирование флешки и зашифрованной файловой системы. Откройте файл `/etc/fstab` и добавьте в него строки:

<code>/dev/sdb1</code>	<code>/mnt/usb</code>	<code>vfat</code>	<code>ro</code>	<code>0 0</code>
<code>/home/den</code>	<code>/home/den</code>	<code>ecryptfs</code>	<code>defaults</code>	<code>0 0</code>

Первая строка монтирует флешку к `/mnt/usb`, а вторая — монтирует зашифрованную файловую систему. Понятно, что флешка должна быть смонтирована до монтирования зашифрованной файловой системы.

Перезагружаемся (команда `reboot`). В идеале все должно работать нормально — после перезагрузки автоматически подмонтируется зашифрованная файловая система.

Однако в моем Debian все пошло не так. Флешка не была автоматически подмонтирована, в результате не смонтировалась и `ecryptfs`. Вылечить удалось редактированием файла `/etc/rc.local`, в который я добавил строку `/bin/mount -a` перед `exit 0`:

```
...  
/bin/mount -a  
exit 0
```

Теперь вы можете комфортно использовать `ecryptfs`.

## 7.2.4. Можно ли доверять стандартному шифрованию?

Только что были рассмотрены три стандартных способа шифрования данных: EFS, BitLocker и `ecryptfs` (Linux). Все три способа достаточно надежны. Нарекание вызывает лишь EFS — 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 данным, зашифрованным 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. Так что если вы не агент МИ-6, 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 и здесь — 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 далее.

## 7.3. Сторонние программные продукты

### 7.3.1. Выбор сторонней программы для шифрования

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

Составьте список необходимых вам характеристик, например:

- ☐ шифрование разделов;
- ☐ шифрование всего диска (системного диска);
- ☐ двухфакторная аутентификация;
- ☐ поддержка виртуальных дисков (криптоконтейнеров);
- ☐ формат виртуальных дисков, совместимый с мобильными приложениями.

Затем для подбора программы, соответствующей вашим требованиям, посетите страницу сравнения программ для шифрования данных: [https://en.wikipedia.org/wiki/Comparison\\_of\\_disk\\_encryption\\_software](https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software).

В книге подобную таблицу приводить не хочется по двум причинам. Во-первых, список программ обновляется, и со временем появляются новые приложения. Например, на момент подготовки книги просто могло не быть приложения, которое соответствует всем вашим пожеланиям. Но оно может появиться месяц спустя. И велика вероятность, что его появление будет отражено 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 требований. Если просмотреть таблицу функций, то всем известная TrueCrypt соответствует всем требованиям, кроме последнего. Да, нет версии программы TrueCrypt для Android, но есть приложение EDS Lite, которое поддерживает формат дисков TrueCrypt.

### 7.3.2. История TrueCrypt, и что случилось с проектом

Первая версия TrueCrypt вышла 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 с 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. И 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 программы произошел с выходом четвертой версии ее в 2005 году: тогда программа стала кроссплатформенной — появилась ее Linux-версия. Но, кроме этого, была также добавлена поддержка x86-x64, хэш-алгоритм Whirlpool и многое другое. В том же 2005 году (в версии 4.1) существенно увеличилась стабильность работы программы 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 ассемблера (ранее она была написана на языке C) — в результате производительность шифрования диска существенно выросла.

В шестой версии тоже появились весьма интересные возможности:

- ☐ параллельное шифрование/дешифрование, что повышало производительность на многоядерных и многопроцессорных системах;
- ☐ возможность создания скрытых разделов при работе с Linux и macOS;
- ☐ 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-либо причине вам 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 байтов, а также TrueCrypt придали умение шифровать файл подкачки Windows, который может содержать конфиденциальную информацию.

Но 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 скомпро-

метирована. Даже был проведен ее независимый аудит, который не нашел в этой программе каких-либо слабых сторон, закладок и прочих не очень хороших моментов. 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 кто был этой третьей стороной, и какие условия были предложены разработчикам проекта, никто не знает (кроме, понятное дело, самих участников событий).

Тогда же, 28 мая 2014 года, вышла финальная версия 7.2. Эта версия не может шифровать данные — ее можно использовать только для расшифровки. Таким образом, последняя полноценная версия программы — 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, что версия старовата и давно не обновлялась (хотя даже в 2016 году в TrueCrypt не было найдено никаких уязвимостей), вы можете использовать программы VeraCrypt (см. *разд. 7.3.4*) или CipherShed (см. *разд. 7.3.5*). Обе эти программы являются форками (человеческим языком — потомками) программы TrueCrypt. Их возможности примерно такие же, как и у TrueCrypt. Да и интерфейс практически такой же — ведь эти программы делали «по образу и подобию» TrueCrypt. Настоящих параноиков может насторожить то, что сейчас нет возможности загрузить TrueCrypt из официальных источников. Да это так. Или загрузите ее с моего сайта (это последняя официальная версия, скачанная с сайта разработчиков), или же используйте VeraCrypt. Программы в других местах могут быть с «сюрпризом» — исходный код доступен всем, поэтому есть вероятность, что кто-то его изменит в своих целях, откомпилирует программу и опубликует где-то на торрентах или на очередной «файлопомойке».

Что же касается Windows 10, то версия 7.1a нормально в ней работает, что подтверждают скриншоты, которые вы далее увидите.

### 7.3.3. Использование TrueCrypt

#### 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 в подробности не вдаваться — примите лицензию и нажмите кнопку **Next**. А вот дальше вы увидите два режима установки (рис. 7.17):

- ☐ **Install** — обычная установка, для выбора этого варианта 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. Этот вариант не требует установки, следовательно, для него не нужны права администратора.

Вы можете вообще извлечь программу на флешку и на этой же флешке создать зашифрованный файл, в котором и станете хранить все ваши конфиденциальные данные. Для запуска программы нужно будет запустить исполнимый файл TrueCrypt.exe непосредственно из каталога установки. У этого способа есть один

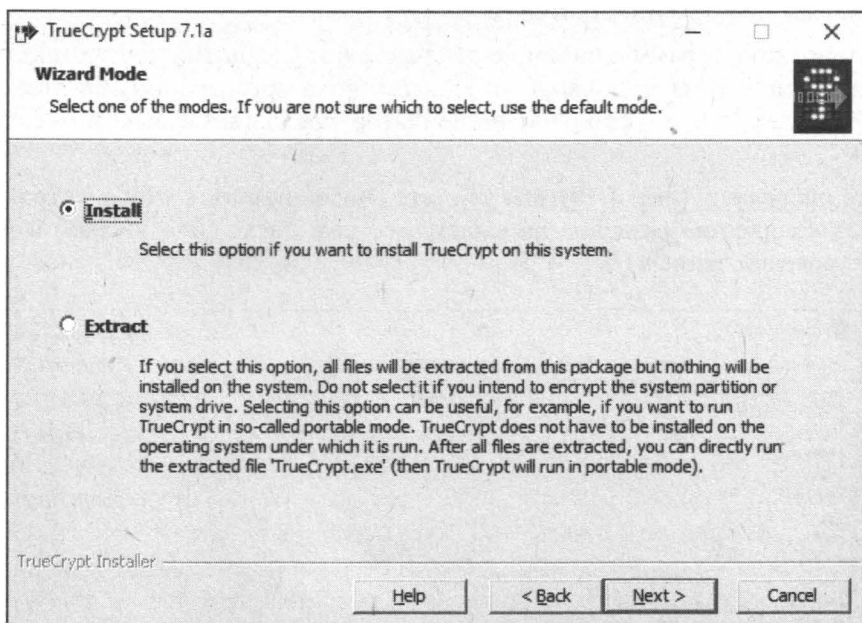


Рис. 7.17. Выбор варианта установки программы TrueCrypt

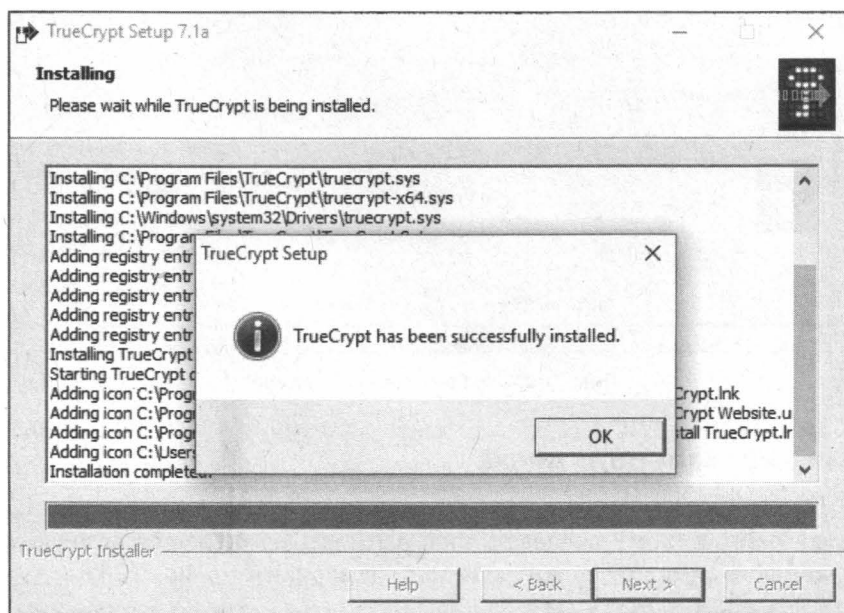


Рис. 7.18. Программа TrueCrypt успешно установлена

недостаток, иначе все бы только и работали с TrueCrypt в portable-режиме. Система UAC будет каждый раз при запуске TrueCrypt ругаться, что очень неудобно, когда работаешь с зашифрованным томом ежедневно. Другое дело, когда действительно нужно записать на флешку что-то такое, и чтобы были гарантии, что никто не прочитает записанную на нее информацию. Или когда нет другого выхода (нет прав администратора).

Далее установка программы ничем не отличается от установки других программ — нажимаем кнопку **Next** несколько раз и ждем, пока программа будет установлена (рис. 7.18). Сразу после установки инсталлятор предлагает ознакомиться с руководством.

Запустите программу (рис. 7.19). Вы увидите список незанятых букв устройств. Он зависит от количества разделов на вашем жестком диске (или дисках) и подключенных носителей данных.

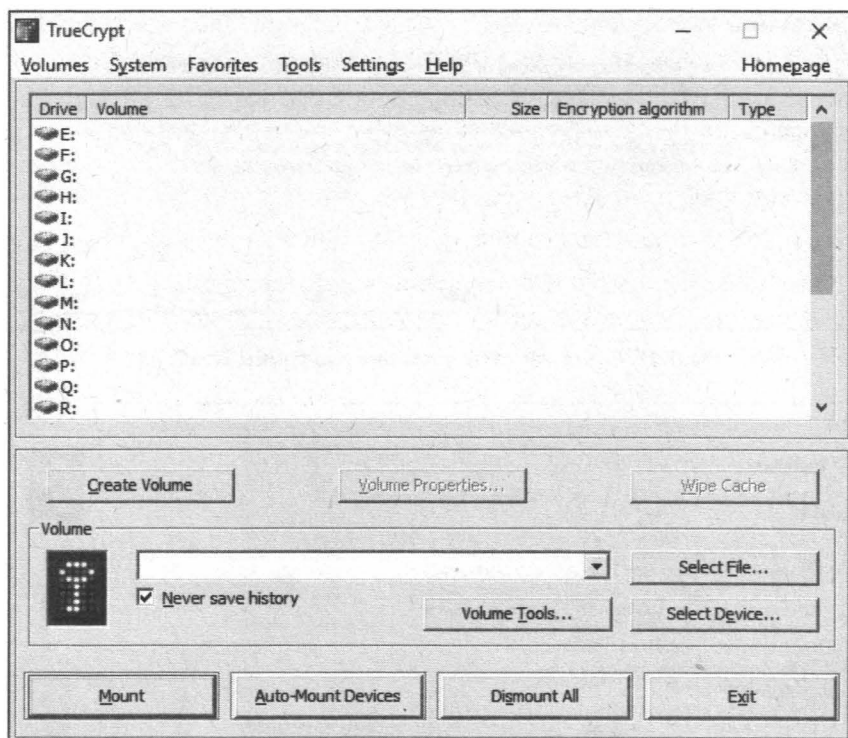


Рис. 7.19. Окно программы TrueCrypt

## Создание виртуального диска

Нажмите кнопку **Create Volume**. Не беспокойтесь — хотя в названии этой кнопки и есть слово **Volume** (том), создавать еще один раздел на жестком диске никто не будет. Далее программа предложит вам один из вариантов (рис. 7.20):

- ☐ **Create an encrypted file container** — создать виртуальный зашифрованный диск (криптоконтейнер), который 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;

- ☐ **Encrypt a non-system partition/drive** — зашифровать несистемный раздел или диск. Вы можете зашифровать раздел вашего 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** — зашифровать системный раздел или весь системный диск. Будьте осторожны: программа вносит изменения в процесс загрузки системы — ведь ей нужно запросить пароль до запуска Windows. Этот же вариант можно использовать для создания скрытой операционной системы. Неопытным пользователям не рекомендуется связываться с шифрованием системного диска, т. к. в случае малейшего сбоя все может закончиться переформатированием жесткого диска и потерей данных.

Какой вариант выбрать? 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 двух 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.

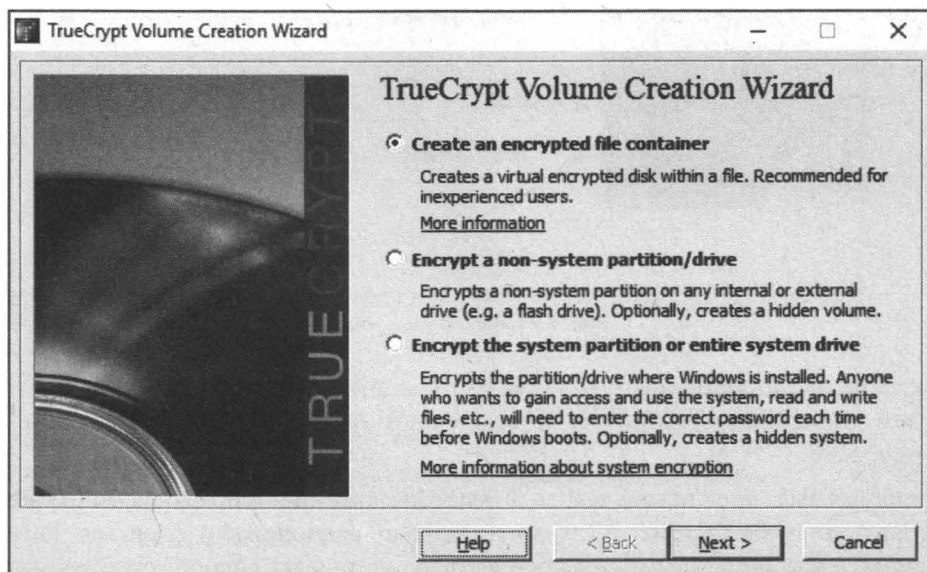


Рис. 7.20. Мастер создания зашифрованного тома



Думаю, прочитав предыдущий раздел, 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. 7.21):

- ☐ **Standard TrueCrypt volume** — обычный зашифрованный том. Он будет виден в системе как обычный диск;
- ☐ **Hidden TrueCrypt volume** — скрытый том. Недостаток обычного тома заключается в том, что он будет виден всем, следовательно, кто-то может попытаться подобрать к нему пароль. А вдруг у него получится? Скрытый том не будет виден в списке дисков, и о его существовании будете знать только вы.

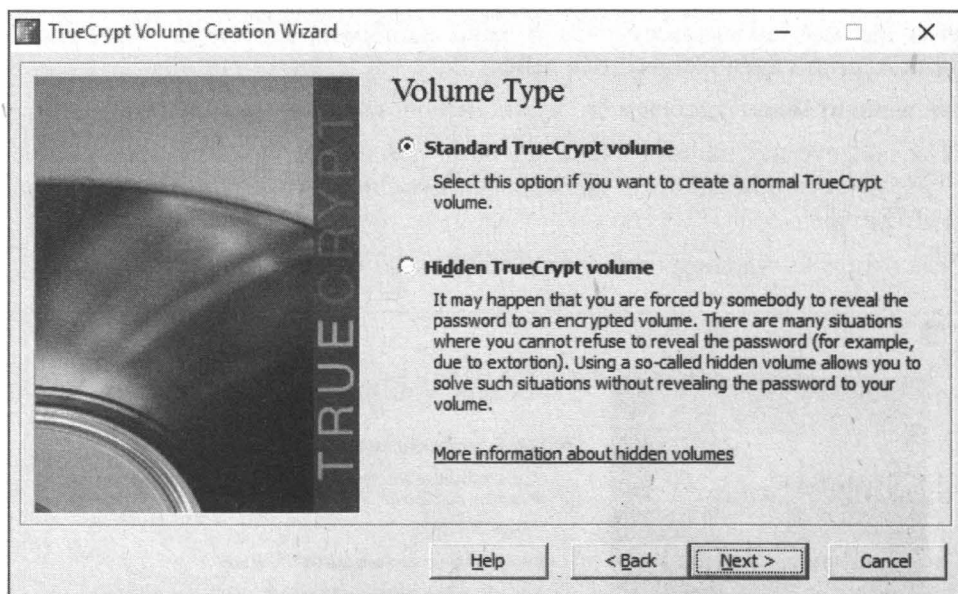


Рис. 7.21. Выбор типа тома

Пока выберите стандартный том — для начинающего пользователя TrueCrypt этого более чем достаточно. Тем более, при надежном пароле «вскрыть» ваш том будет очень непросто.

Далее программа предложит выбрать местоположение для файла виртуального зашифрованного диска (рис. 7.22). Файл можно расположить в любом каталоге, к которому у вас есть доступ, а также на флешке или на внешнем жестком диске. Нажмите кнопку **Select File** для выбора файла.

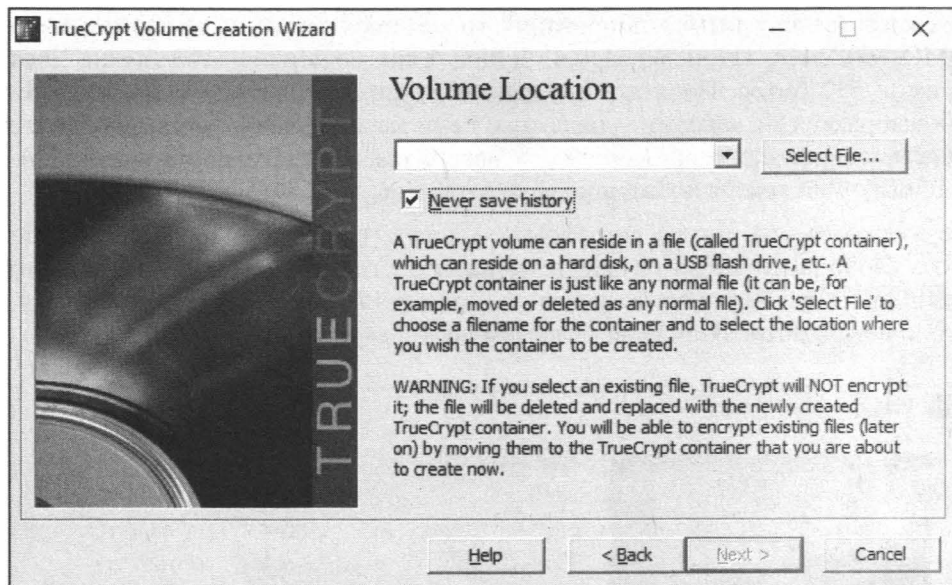


Рис. 7.22. Выбор местоположения для файла зашифрованного диска

Далее нужно выбрать алгоритм шифрования и алгоритм хэширования (рис. 7.23). Вы можете выбрать алгоритмы AES, Serpent, Twofish или же их комбинации AES-Twofish или Serpent-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. Тут уж решать вам.

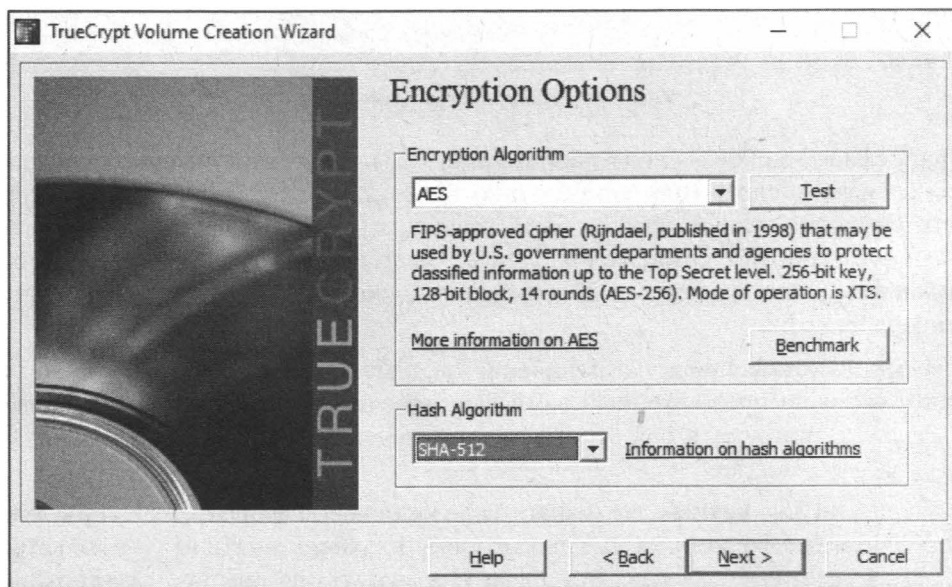


Рис. 7.23. Выбор алгоритмов шифрования и хэширования

Что же касается алгоритма хэширования, то вам предлагают на выбор три варианта: RIPEMD-160, SHA-512 и Whirlpool. Длина хэша первого — 160 битов, двух последних — 512 битов. Понятно, что два последних алгоритма — надежнее. Какой из них выбрать? Оба алгоритма надежны. Если вы когда-нибудь имели дело с шифрованием, точнее с хэшированием, то наверняка выберете привычный SHA-512, хотя Whirlpool появился позже и должен быть надежнее SHA-512.

Далее нужно ввести размер виртуального диска (рис. 7.24). Программа сообщает, сколько свободного места осталось на разделе, где хранится файл виртуального диска. Если же вы планируете хранить на зашифрованном диске, скажем, базу почтового клиента, потребуется как минимум несколько гигабайт.

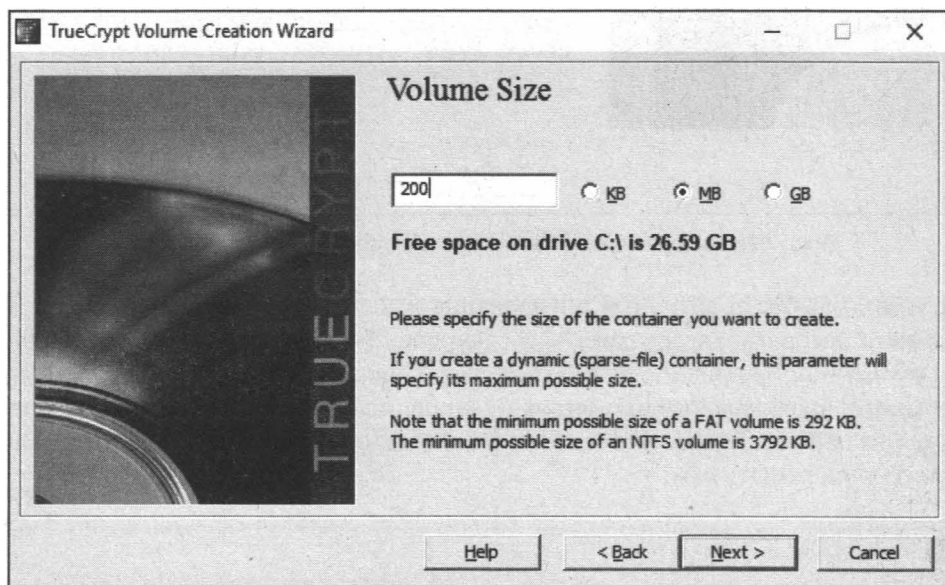


Рис. 7.24. Размер виртуального диска

А теперь самое важное — ввод пароля (рис. 7.25). Не нужно выбирать в качестве пароля словарное слово (или комбинацию таких слов) или дату вашего рождения. Регистр символов пароля должен быть разный, в пароле должны присутствовать цифры и неалфавитные символы (@, ^, =, \$, \* и др.). Рекомендуемая разработчиком минимальная длина пароля — 20 символов, максимальная возможная длина — 64 символа.

Программа не устанавливает ограничение на длину пароля, но обязательно сообщит вам, что если предложенный вами ваш пароль будет по ее мнению ненадежным. Решение принимать вам — или указать надежный пароль, или оставить как есть.

Включив режим **Use keyfiles**, вы можете задать ключевые файлы для доступа к тому. Указать ключевые файлы можно, нажав кнопку **Keyfiles**.

Следующий шаг — форматирование тома (рис. 7.26). Для небольших виртуальных дисков нужно выбрать файловую систему FAT. А вот если размер диска составляет

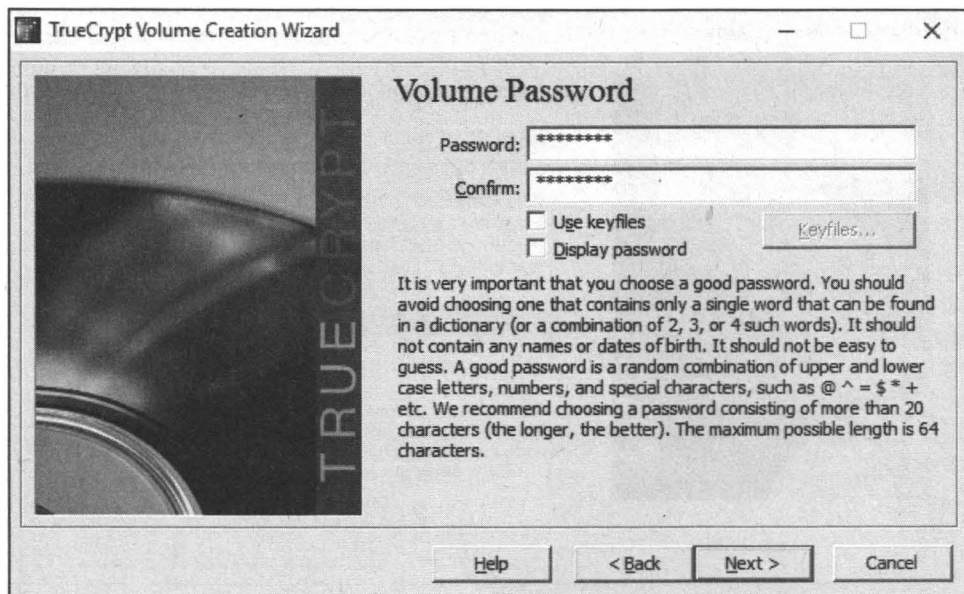


Рис. 7.25. Установка пароля

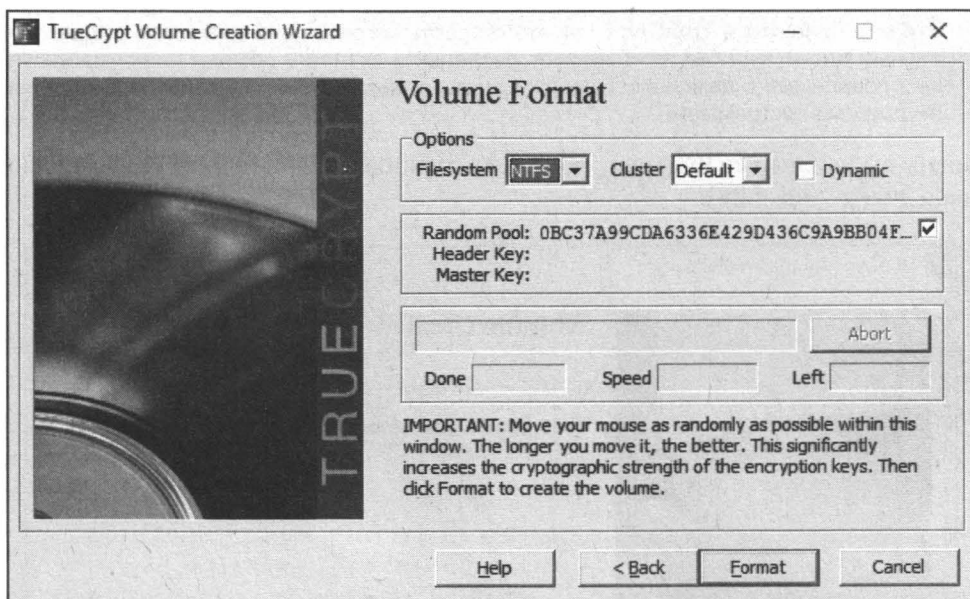


Рис. 7.26. Выбор файловой системы для виртуального тома

более 4 Гбайт, и вы планируете хранить на нем большие файлы (размером тоже более 4 Гбайт) — например, размер диска 100 Гбайт и размер файлов от 4 Гбайт, тогда нужно выбрать файловую систему NTFS. Нажмите кнопку **Format** и подождите, пока форматирование будет завершено (рис. 7.27). Время ожидания зависит от выбранного размера диска.

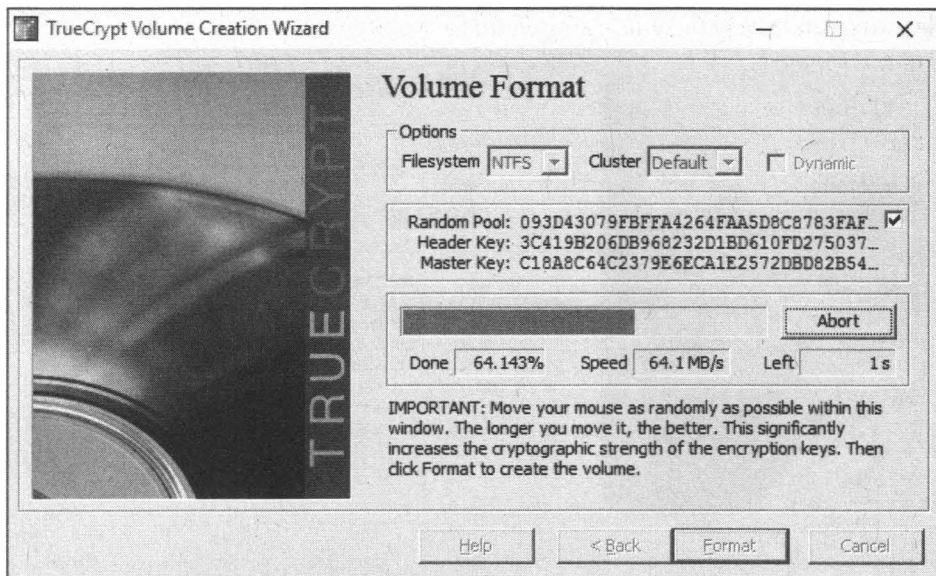


Рис. 7.27. Процесс форматирования виртуального диска

#### 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, вы увидите сообщение, свидетельствующее об успешном создании виртуального диска (рис. 7.28).

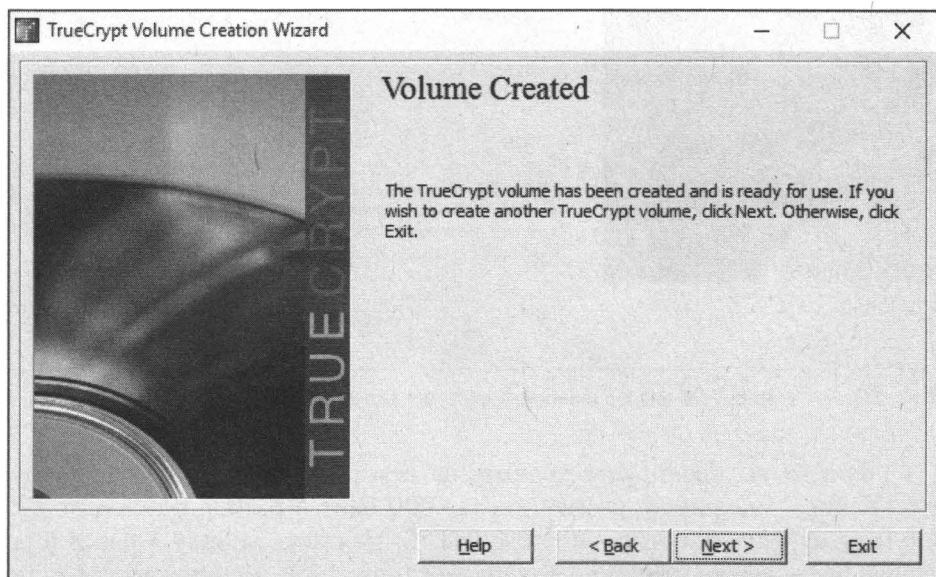


Рис. 7.28. Виртуальный диск успешно создан



Если вы желаете создать еще один зашифрованный диск, нажмите кнопку **Next**, в противном случае — нажмите кнопку **Exit**.

После создания виртуального жесткого диска его нужно подмонтировать. Для этого 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. 7.29).

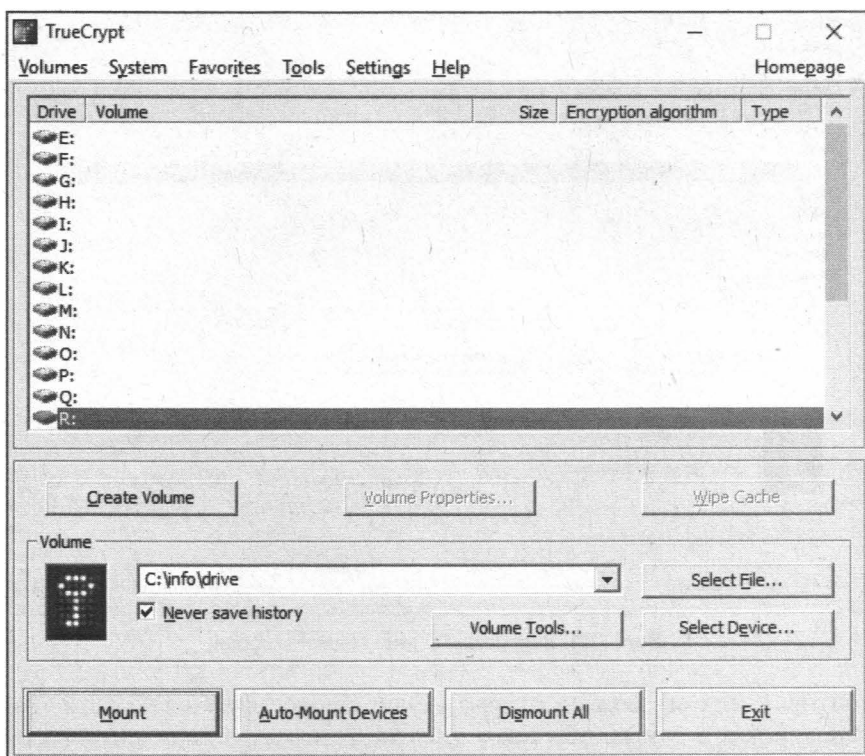


Рис. 7.29. Выбор и монтирование файла виртуального диска

Программа попросит указать пароль для доступа к тому. Если при создании тома вы выбрали доступ к нему по паролю, введите в соответствующее поле пароль, если использовали ключевые файлы, включите переключатель **Use keyfiles** и нажмите кнопку **Keyfiles** для выбора ключевого файла (рис. 7.30).

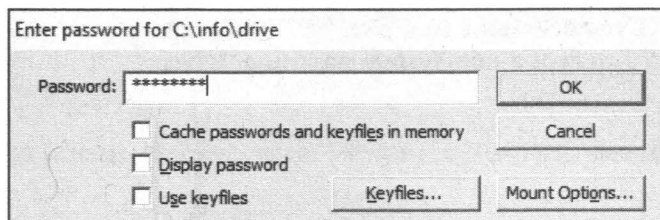


Рис. 7.30. Ввод пароля при монтировании тома

В основном окне программы вы увидите, что том подмонтирован (конечно, при условии, правильного ввода пароля). В нашем случае том подмонтирован как диск R:, размер тома — 199 MB, алгоритм — AES (рис. 7.31).

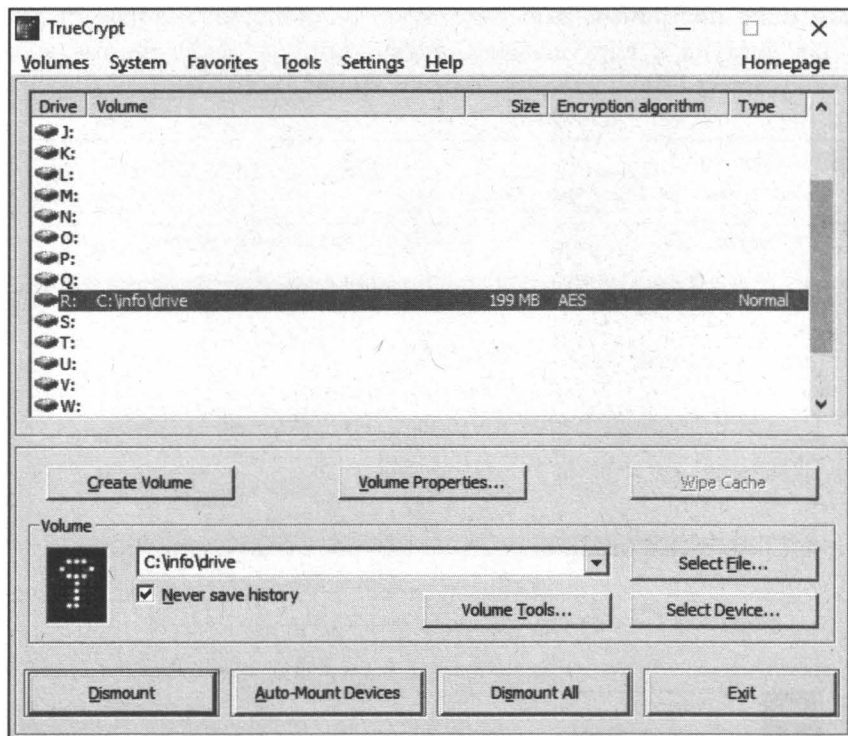


Рис. 7.31. Виртуальный диск подмонтирован

После монтирования вы можете открыть окно Проводника и работать с зашифрованным диском как с самым обычным диском. Никаких ограничений на использование виртуального диска нет.

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

## Шифрование раздела

Шифрование раздела аналогично созданию виртуального диска. Поэтому, если вы не читали предыдущий раздел, самое время это сделать.

Нажмите кнопку **Create Volume** (см. рис. 7.19) и в открывшемся окне (см. рис. 7.20) выберите вариант **Encrypt a non-system partition/drive**.

### СОВЕТ

Для шифрования системного раздела (если вам это нужно) лучше используйте BitLocker.

После этого в окне, показанном на рис. 7.21, выберите, какой это будет том: скрытый (**Hidden TrueCrypt volume**) или стандартный (**Standard TrueCrypt volume**).



Далее необходимо выбрать том, который вы хотите зашифровать. Нажмите кнопку **Select Device** (рис. 7.32), чтобы выбрать раздел диска. Выберите раздел, нажмите кнопку **OK**, а затем кнопку **Next** (рис. 7.33).

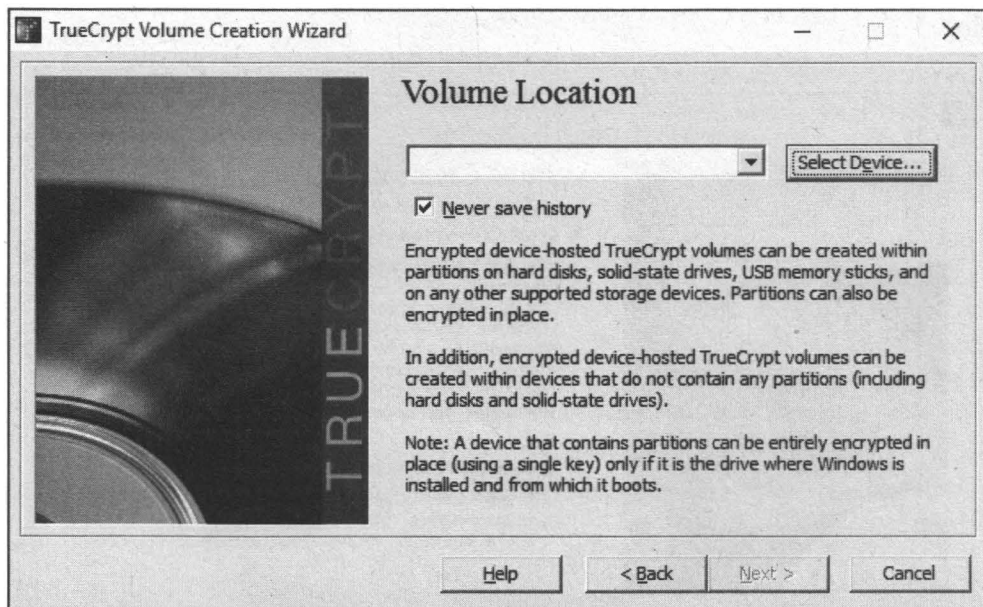


Рис. 7.32. Нажмите кнопку **Select Device**

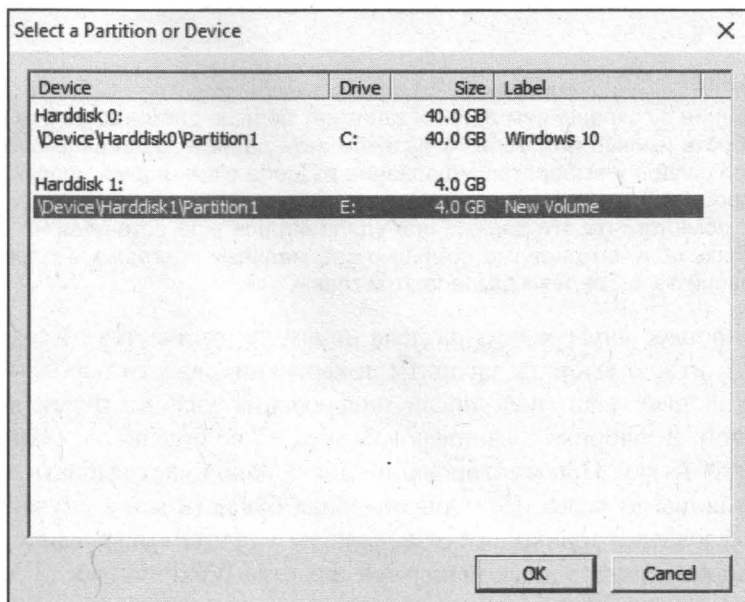


Рис. 7.33. Выберите устройство для шифрования

С помощью опций следующего окна (рис. 7.34) 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**). Первый вариант предпочтительнее для пустых дисков или дисков, где нет важной информации. Второй вариант позволяет сохранить имеющиеся на диске данные.

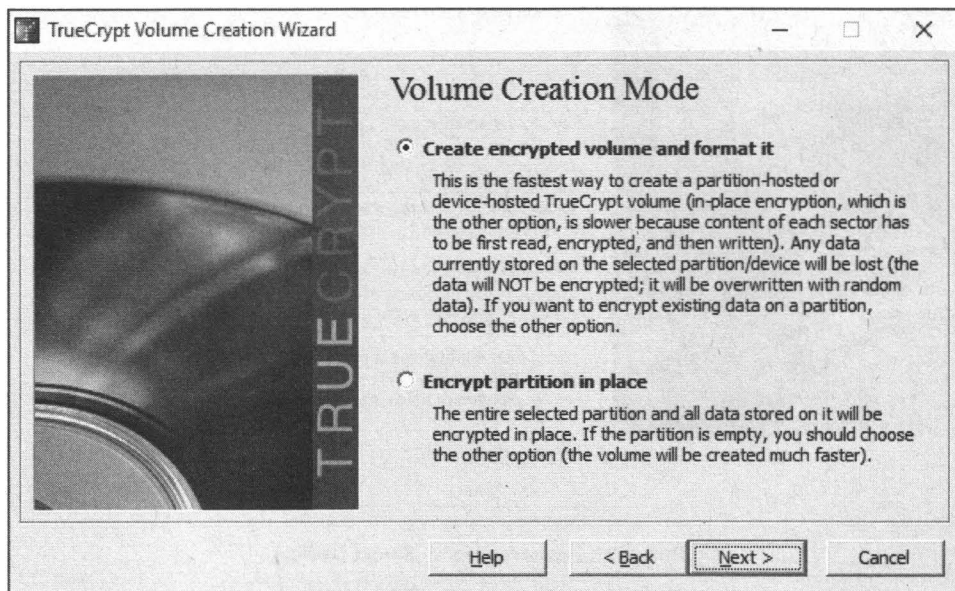


Рис. 7.34. Выбор типа шифрования

### **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 выберете 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.

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 уже не будет доступен под прежней буквой. Я, например, зашифровал диск E:, но больше не смогу обратиться к нему через эту букву. При монтировании диска надо будет выбрать другую букву и работать с данными через нее. Оригинальная буква (в моем случае — E:) снова сможет использоваться только в случае, если вы удалите шифрование. А для этого придется отформатировать диск, используя средства Windows (рис. 7.35).

Теперь разберемся, как получить доступ к зашифрованному диску. В окне TrueCrypt (см. рис. 7.19) нажмите кнопку **Select Device** и выберите зашифрованный

диск. Затем выберите букву, через которую будет осуществляться доступ к данным, и нажмите кнопку **Mount** (рис. 7.36). Как обычно, придется ввести указанный при шифровании пароль. Программа отобразит, к какой букве подмонтирован диск, его физическое расположение, размер и алгоритм шифрования (рис. 7.37).

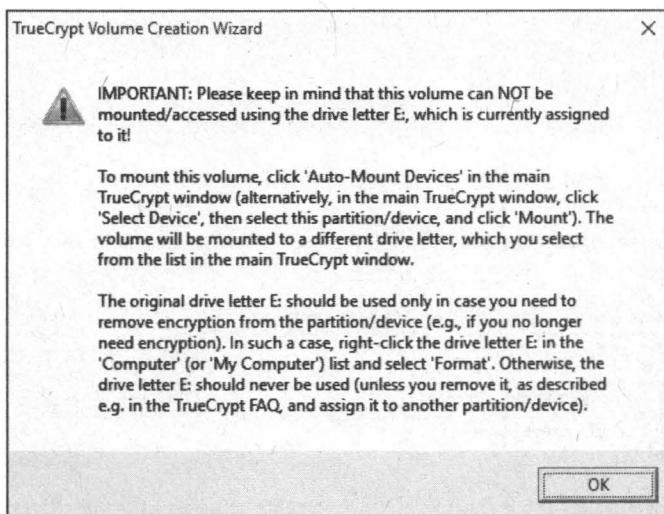


Рис. 7.35. Важное предупреждение

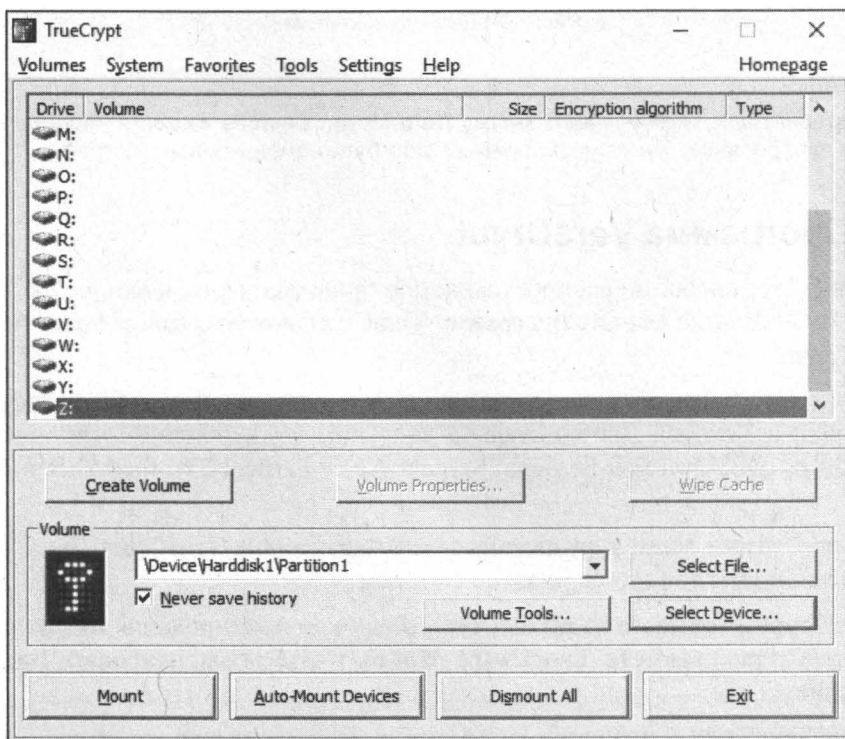


Рис. 7.36. Подготовка к монтированию диска

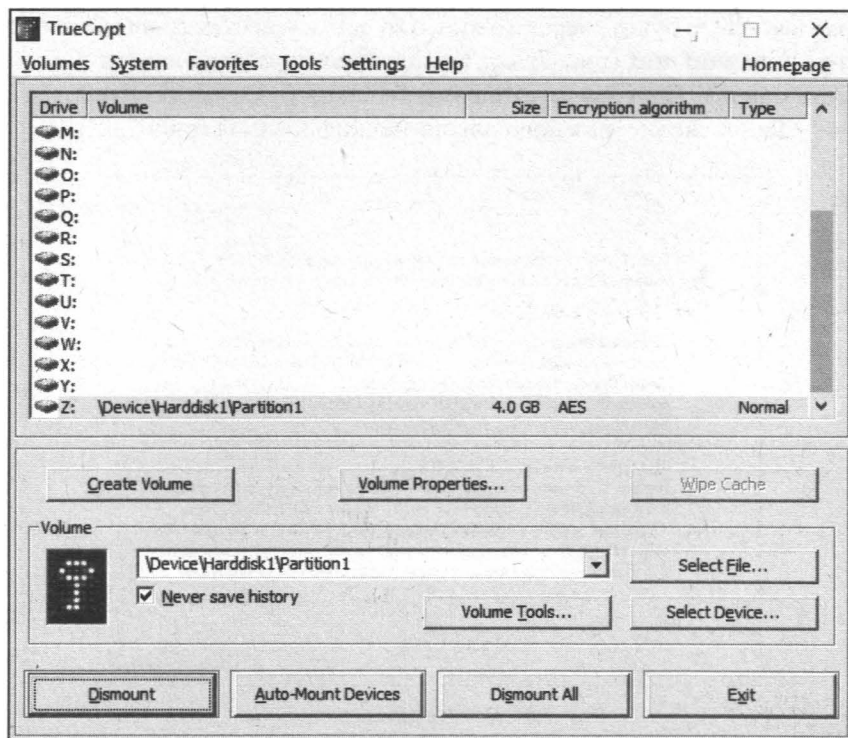


Рис. 7.37. Диск подмонтирован

**СОВЕТ**

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

### 7.3.4. Программа VeraCrypt

VeraCrypt — это свободно распространяемое приложение, основанное на TrueCrypt версии 7.1a. Бесплатно скачать программу 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 (рис. 7.38), поэтому подробно мы ее рассматривать не станем.

Хоть VeraCrypt и совместима с TrueCrypt, но в окне монтирования нужно включать режим TrueCrypt (параметр **TrueCrypt Mode**), иначе подмонтировать диск не получится (рис. 7.39).

Что лучше TrueCrypt или VeraCrypt? Разработчики VeraCrypt уверяют, что их продукт лучше и приводят неоспоримые факты: TrueCrypt использует 1000 итераций

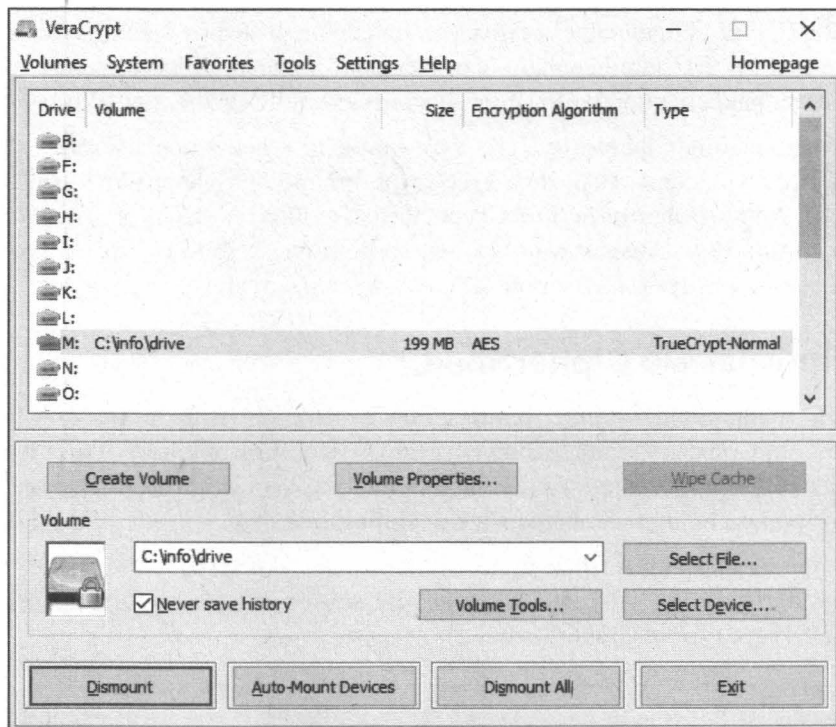


Рис. 7.38. Программа VeraCrypt с подмонтированным криптоконтейнером

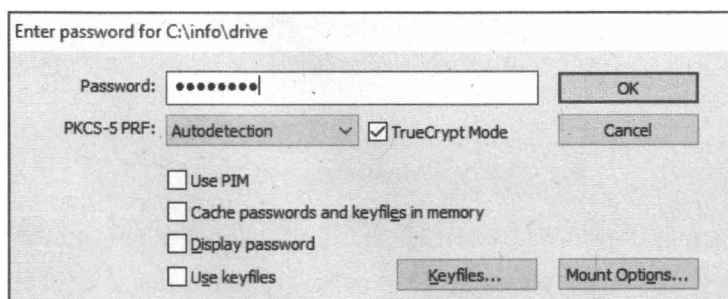


Рис. 7.39. Включаем режим TrueCrypt

при генерации ключа, которым шифруется системный раздел при использовании алгоритма PBKDF2-RIPEMD-160, а VeraCrypt — 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 было интересно, насколько медленнее окажется VeraCrypt, и я решил это проверить, — о результатах тестирования производительности будет рассказано далее (см. разд. 7.3.7).

Также в VeraCrypt исправлена уязвимость начального загрузчика для Windows, 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.

### 7.3.5. 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 (рис. 7.40). А вот VeraCrypt может спокойно жить на одном компьютере и с TrueCrypt, и CipherShed.

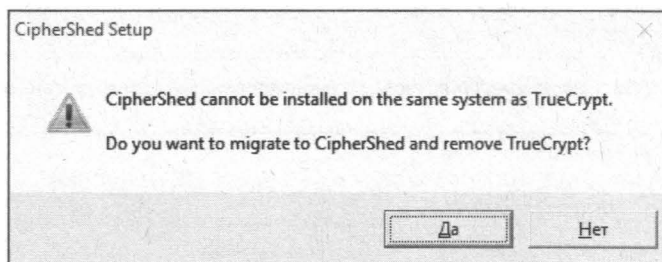


Рис. 7.40. Предложение удалить TrueCrypt

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 (на момент написания этих строк — 3 июля 2019 года — доступна версия 0.7.4). На мой взгляд, 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.

### 7.3.6. Шифрование файла для передачи

Иногда нужно зашифровать файл для передачи другому пользователю. Если файл небольшой, то можно просто отправить зашифрованное электронное сообщение,



приложив этот файл. Но вся беда в том, что большинство почтовых серверов имеют ограничения на максимальный размер письма. Часто это 20–40 Мбайт.

Что делать, если нужно передать файл большего размера? Есть несколько способов:

- ☐ создать виртуальный диск примерно такого же размера, что и передаваемые файлы (диск нужно создавать с небольшим запасом). Поместите на него секретные файлы, размонтируйте и опубликуйте в облаке — скажем, на Google Drive, файл виртуального диска. Его получателю нужно будет безопасным способом (например, в зашифрованном e-mail) сообщить пароль и ссылку на файл. Он скачает его и откроет на своем компьютере;
- ☐ создать самораспаковывающийся архив, защищенный паролем. Такие архивы могут создавать различные архиваторы вроде WinRAR, но все же лучше его создать в специальных программах, которые изначально предназначены для шифрования. Дело в том, что существует много программ, позволяющих «вспомнить» пароль WinRAR, поэтому такую защиту нельзя назвать надежной;
- ☐ использовать мобильное приложение для облачного шифрования. Оно позволяет безопасно передавать файлы через Google Drive (файлы передаются в зашифрованном виде).

Самый безопасный способ — первый. Главное, чтобы не было утечки пароля, который вы отправите получателю файла.

### 7.3.7. Производительность зашифрованных дисков

Очевидно, что шифрование и расшифровка требуют дополнительных системных ресурсов. Но насколько медленнее становится работа с зашифрованным диском? Ответ на этот вопрос — здесь.

В качестве тестовой машины использовался компьютер-динозавр — AMD Athlon 2.2 ГГц, 2 ядра, 8 Гбайт оперативной памяти и жесткий диск (не SSD) на 500 Гбайт. Операционная система — Windows 7 SP1, 64-битная. При использовании SSD-диска результаты будут лучше. Но нам важна не столько «чистая» производительность, сколько разница в производительности при использовании разных программ.

Мы зашифруем раздел жесткого диска, затем сравним производительность диска в CrystalDiskMark. Никаких антивирусов, да и прочих программ во время теста запущено не будет, чтобы ничто не смогло повлиять на результаты.

Результаты CrystalDiskMark нужно трактовать так:

- ☐ Seq Q32T1 — тест последовательной записи/последовательного чтения, количество очередей — 32, потоков — 1;
- ☐ 4K Q32T1 — тест случайной записи/случайного чтения, размер блока 4 Кбайт, количество очередей — 32, потоков — 1;
- ☐ Seq — тест последовательной записи/последовательного чтения;
- ☐ 4K — тест случайной записи/случайного чтения, размер блока 4 Кбайт.



На эти тесты далее я буду ссылаться по их порядку в программе CrystalDiskMark, т. е. Seq Q32T1 — это первый тест, 4K Q32T1 — второй и т. д.

Результаты тестирования производительности дисков, зашифрованные различными программами шифрования, приведены в табл 7.1.

*Таблица 7.1. Результаты тестирования*

Приложение	Seq Q32T1		4K Q32T1		Seq		4K	
	Чтение	Запись	Чтение	Запись	Чтение	Запись	Чтение	Запись
Без шифрования	79.88	80.66	0.679	1.195	79.89	78.43	0.548	1.101
BitLocker	79.65	79.80	0.688	1.226	66.85	77.15	0.534	1.115
TrueCrypt	79.81	80.65	0.551	1.151	79.65	71.51	0.539	1.133
VeraCrypt	79.69	76.56	0.562	1.262	79.89	68.15	0.542	1.154
CipherShed	73.52	77.05	0.551	1.096	74.04	65.84	0.536	1.139
Symantec EE	79.86	80.13	0.666	1.134	58.93	51.80	0.507	1.115

При использовании BitLocker снижение производительности наблюдается только в третьем тесте. В случае с TrueCrypt ощутимое снижение производительности наблюдается тоже в третьем тесте и то только при записи. Во всех остальных случаях снижение производительности вряд ли будет замечено пользователем.

Производительность VeraCrypt, как и ожидалось, ниже, чем производительность TrueCrypt. Снижение производительности наблюдается в первом и третьем тестах. А вот CipherShed оказался даже медленнее, чем VeraCrypt, — тоже в первом и третьем тестах.

Symantec Endpoint Encryption (SEE)<sup>1</sup> не выглядел бы аутсайдером, если бы не третий тест, который он провалил вчистую. Последовательный I/O с блоками небольшого размера — явно не его конек.

В целом, все рассмотренные приложения весьма известные и обеспечивают высокий уровень производительности, даже SEE с его провалом в третьем тесте.

Первое место по производительности разделяют TrueCrypt и BitLocker. На втором месте — VeraCrypt, она не намного медленнее, чем TrueCrypt. Третье место — CipherShed, а четвертое — Symantec EE, но только из-за провала в третьем тесте.

Если нужна поддержка GPT, то я бы выбрал BitLocker. Как и SEE, BitLocker — решение с закрытым кодом. Но если выбирать между платным и бесплатным (стоимость BitLocker уже включена в стоимость Windows) решением, то выбор очевиден.

<sup>1</sup> В книге не рассматривался, поскольку является коммерческим решением. Книга же адресована обычным пользователям, которые скорее выберут бесплатные программные продукты, чем коммерческое решение корпоративного уровня. Однако у меня была возможность, и я включил этот продукт в сравнение.

Однако если нужно зашифровать несистемный диск, то можно смело выбирать VeraCrypt. Да, она чуть медленнее, чем TrueCrypt, но зато проект развивается и есть надежда, что и поддержка GPT появится в обозримом будущем.

## 7.4. Соккрытие файлов

Иногда файл нужно скрыть. Само по себе соккрытие файлов не гарантирует, что никто не сможет получить к ним доступ. Поэтому для файлов с секретной информацией рекомендуется сначала их зашифровать, а затем — скрыть, чтобы убрать подальше от посторонних глаз.

Традиционно операционная система Windows позволяет скрывать файлы путем установки атрибута **Скрытый**. Но в этом случае файл просто перестанет быть виден в Проводнике, но если в его настройках включено отображение скрытых файлов, то все они будут видны.

Поэтому нужно использовать сторонние программы, которые будут перехватывать вывод таблицы каталога и удалять нужные вам файлы из этой таблицы при выводе содержимого каталога. Одна из таких программ — Folder Lock. Со своей задачей она справляется, но учтите, что она не блокирует доступ к скрытым файлам, поэтому, если злоумышленник знает точное расположение файла, он его откроет. Вот поэтому я и рекомендовал шифровать файлы с важной информацией.

Программа Folder Lock — далеко не единственная подобная программа. Есть много других — например: File Lock, WinMend Folder Hidden, Wise Folder Hider, Free Hide Folder.

Есть и другой, более «продвинутый» способ соккрытия файлов. Пусть у нас есть архив с секретными документами (файл `secret.rar`) и файл с изображением, например, машины (`car.jpg`). Откройте командную строку комбинацией клавиш `<Win>+<R>`, выполните команду `cmd` и введите команду:

```
copy /B car.jpg + secret.rar secret-car.jpg
```

В результате будет создан файл `secret-car.jpg`, состоящий из файлов `secret.rar` и `car.jpg`. Для постороннего файл `secret-car.jpg` — обычная картинка. Но вы, зная, что этот файл особенный, сможете извлечь из него файлы. Если открыть этот файл в архиваторе, то можно будет работать с ним, как с обычным архивом.

Посмотрите на рис. 7.41, *а* — это фрагмент окна Проводника Windows. Поверх него открыто окно командной строки, в котором показано, какая команда была введена для создания скрытого файла. И также видно, что в Проводнике файл `secret-car.jpg` отображается как обычная картинка, и если на нем щелкнуть, то откроется изображение. Однако если этот файл открыть в архиваторе (рис. 7.41, *б*), то вы получите содержимое архива. Только открывать файл нужно не двойным щелчком, как обычно, а командой **Show archive contents** (Показать содержимое архива), которая появится в контекстном меню архиватора при щелчке на новой картинке правой кнопкой мыши.

Такой способ подходит для сокрытия небольших архивов, размер которых не превышает размера среднестатистического изображения (до 10 Мбайт). В противном случае это привлечет лишнее внимание тех, кому эти документы видеть не нужно. Вы только вдумайтесь — картинка размером 500 Мбайт? Зато способ действительно работает и он, на мой взгляд, надежнее использования сторонних программ, которые часто бывают платными (например, тот же Folder Lock). Да и наличие на компьютере программ сокрытия уже привлекают внимание — значит, что-то скрывается. А такой способ работает всегда и везде — команда `copy` встроена в Windows, и нет надобности устанавливать что-то еще.

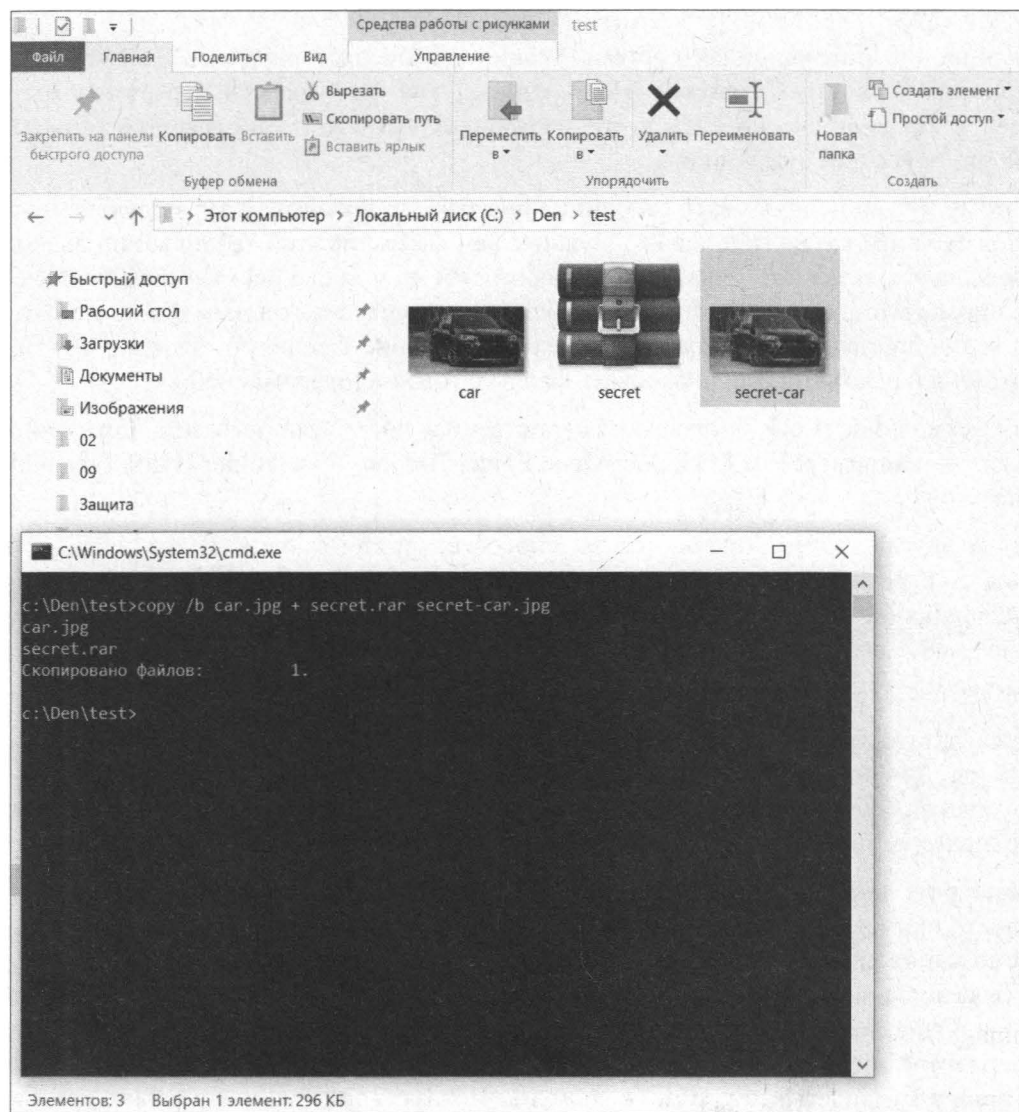


Рис. 7.41. (Часть 1 из 2) Прячем файл: а — открыто окно командной строки с командой, введенной для создания скрытого файла

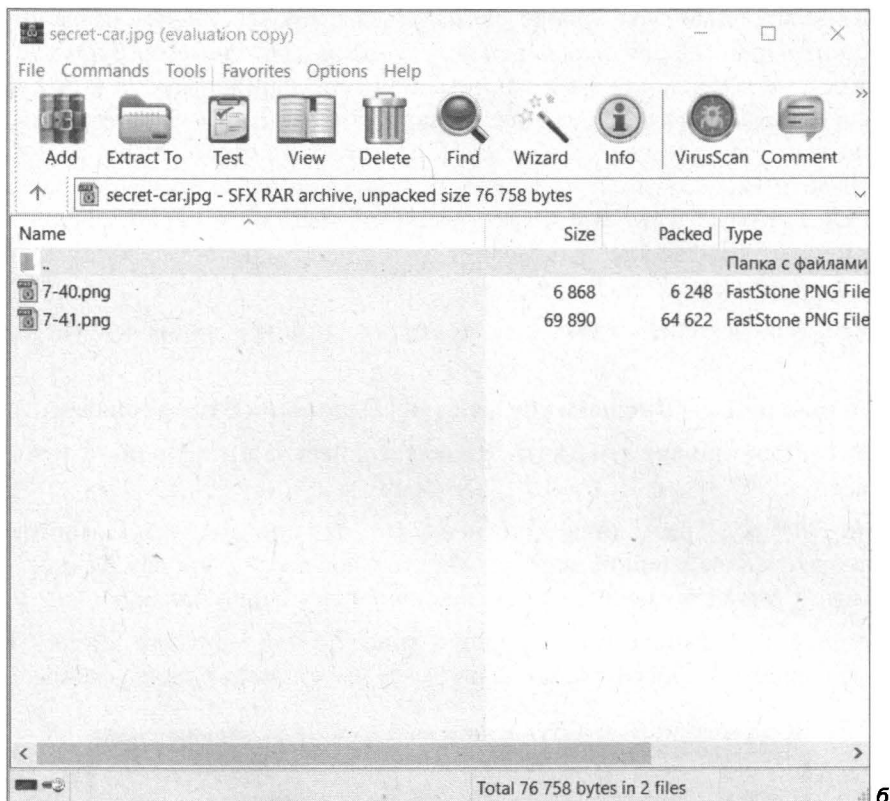


Рис. 7.41. (Часть 2 из 2) Прячем файл: б — содержимое скрытого архивного файла в окне архиватора

## 7.5. Шифрование данных на предприятиях

Домашние пользователи могут выбирать любые программы для защиты собственных данных. Выбор программы зависит от предпочтений пользователя и от наличия в программе необходимых ему функций. На предприятиях все немного сложнее, поскольку ФЗ-152 требует, чтобы для защиты персональных данных использовались только сертифицированные средства защиты. Реестр сертифицированных программных продуктов можно получить на сайте ФСТЭК<sup>1</sup>.

Выбирая программу шифрования, обратите внимание не только на наличие сертификата, но и на срок его действия. Если срок скоро закончится, а программа в целом устраивает, обратитесь к ее разработчикам — планируют ли они продлевать сертификацию. Процесс сертификации достаточно затратный, поэтому, если спрос на программу низкий, разработчики могут отказаться от ее сертификации.

<sup>1</sup> См. <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00>.

По своему опыту знаю, что лучше связываться с проверенными разработчиками вроде «КриптоПро» (не считите за рекламу) — они давно на рынке и, судя по всему, уходить с него не собираются. Их решения сертифицированы и поддерживают ГОСТовские алгоритмы шифрования. В паре с продуктами «КриптоПро» можно использовать ту же программу CyberSafe Top Secret, о которой мы говорили в *главе 6*, — тогда у вас появится возможность прозрачного шифрования папки алгоритмом ГОСТ. Кроме того, при использовании CyberSafe и «КриптоПро» вы сможете применять USB-токены, что избавит вас от необходимости ввода паролей при доступе к зашифрованной информации.

Рассмотрим, как добавить папку для прозрачного шифрования в CyberSafe Top Secret:

1. Перейдите в раздел **Шифрование файлов | Прозрачное шифрование**.
2. Нажмите кнопку **Добавить папку** и выберите папку, которую вы хотите зашифровать.
3. Нажмите кнопку **Применить** в нижней части окна программы. Появится запрос об установке ключа администратора. Обязательно нажмите кнопку **Да** (рис. 7.42) — иначе вы не сможете вносить изменения в конфигурацию папки.
4. Выберите ключ администратора папки (рис. 7.43) и нажмите кнопку **Применить**. После этого программа зашифрует все имеющиеся в папке файлы.

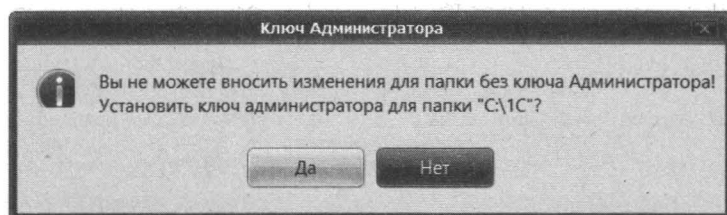


Рис. 7.42. Нажмите кнопку **Да**

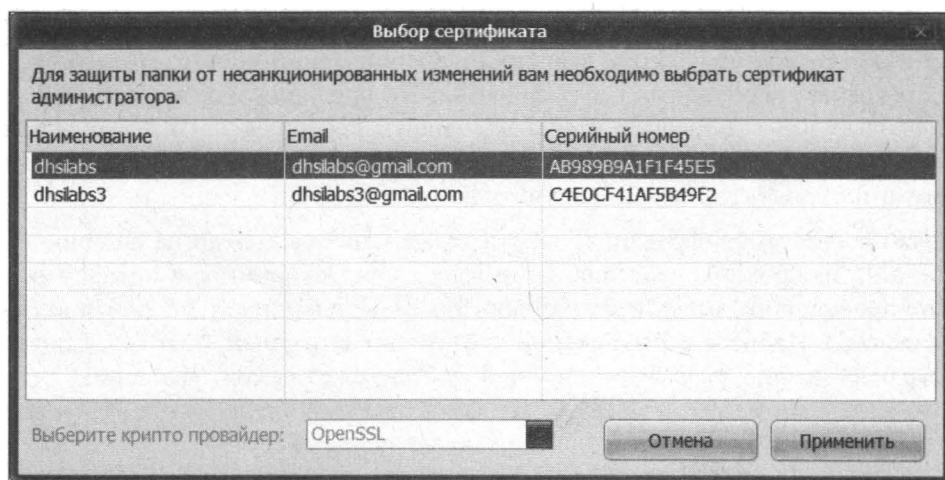


Рис. 7.43. Выберите ключ администратора

**СОВЕТ**

Если вы хотите ускорить процесс создания зашифрованной папки, шифруйте пустую папку, а уже затем добавляйте в нее файлы.

5. Зашифровав все имеющиеся в папке файлы, программа добавит папку в список, но по умолчанию она будет выключена. Нажмите кнопку **Включить** (рис. 7.44) и введите пароль сертификата — папка будет включена.

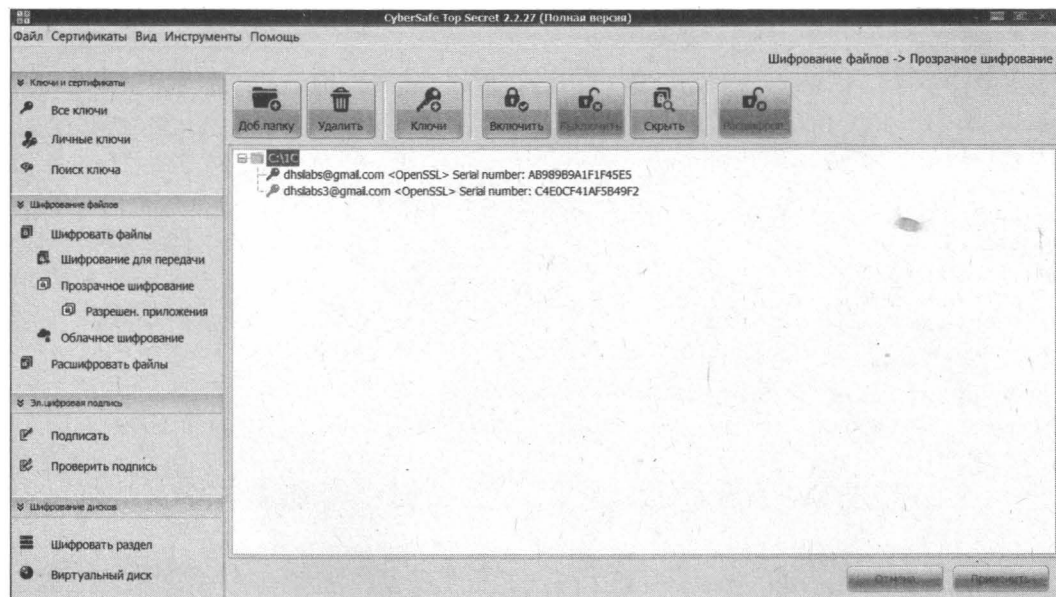


Рис. 7.44. Осталось включить папку...

Включив папку (рис. 7.45), вы можете использовать следующие кнопки:

- ☐ **Выключить** — выключает папку, после этого вы не сможете ее использовать;
- ☐ **Расшифровать** — выполняет дешифровку всех данных в папке, возвращая ее к первоначальному виду;
- ☐ **Скрыть** — скрывает папку, после этого она станет не видна в окне Проводника;
- ☐ **Ключи** — позволяет редактировать список пользователей, чьими ключами можно расшифровать папку. Редактировать список может только администратор. Так что программу можно использовать не только для шифрования папки, но и для ограничения доступа к информации.

При копировании файла во включенную зашифрованную папку он будет автоматически зашифрован. Если папка выключена, доступа к файлам не будет вообще — вы не сможете ни скопировать в нее файлы, ни просмотреть список уже имеющихся.

Программу можно использовать и для прозрачного шифрования сетевых папок. Однако у нее есть одна странная особенность: на сервере, т. е. компьютере, где находится расшаренная папка, не должна быть установлена программа Cybersafe Top

**Secret**, иначе шифрование будет работать некорректно. Разработчики сообщают, что такова особенность используемого программой драйвера прозрачного шифрования.

Подробнее об использовании программы можно прочитать в руководстве, доступном на ее сайте.

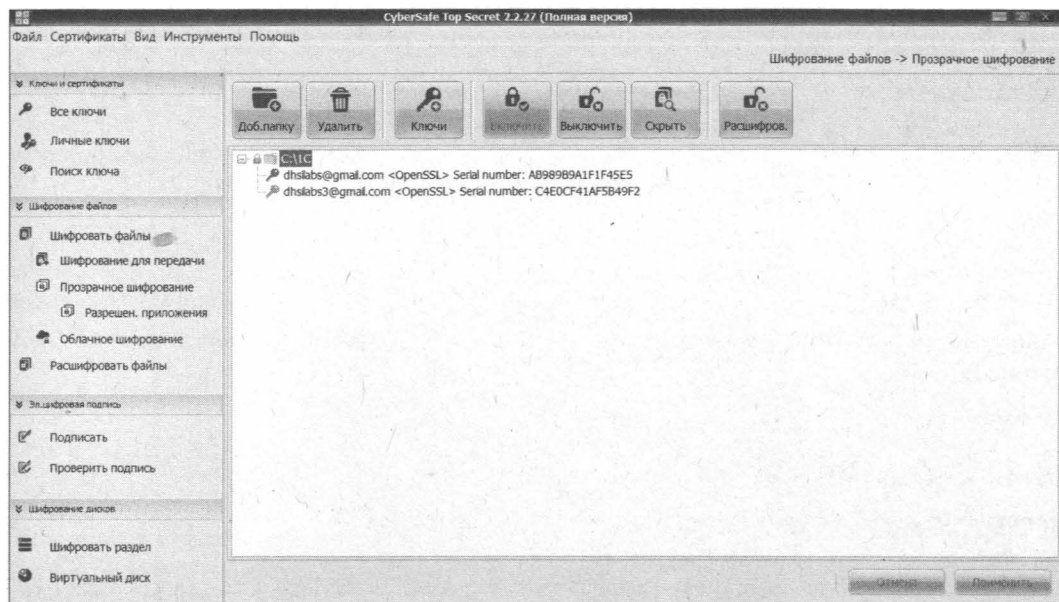


Рис. 7.45. Папка включена



## ГЛАВА 8



# Безопасность устройств на ОС Android

Всевозможные Android-устройства весьма популярны у пользователей, поэтому мы не можем обойти стороной обеспечение безопасности таких устройств. И в этой главе мы рассмотрим рекомендации, позволяющие сделать ваше устройство безопаснее.

## 8.1. Включение кода разблокировки устройства

Любая защита Android-устройства не имеет смысла, если вы не настроили код разблокировки устройства, и устройство разблокируется свайпом в сторону. Двухфакторная аутентификация и настройка разблокировки подробно рассматриваются в следующей главе, рассказывающей о защите устройств от утечки данных. Но я вам рекомендую настроить разблокировку своего устройства прямо сейчас, руководствуясь инструкциями из *главы 9*.

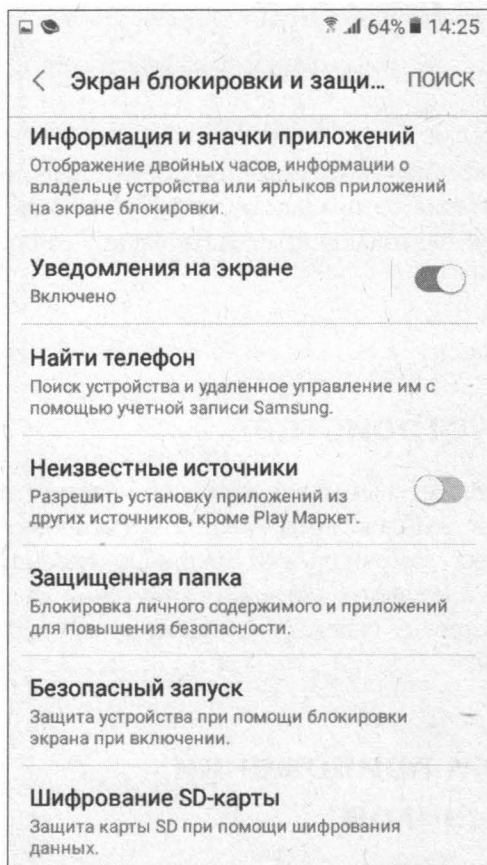
## 8.2. Отказ от установки приложений из неизвестных источников

Очень часто причиной всех несчастий у владельцев Android-устройств является установка вредоносной программы. Чтобы исключить хотя бы неявную или случайную установку такой программы, рекомендуется запретить установку программ из неизвестных источников.

Безопасным источником считается только Google Play Маркет — по сути, так оно и есть. В этом смысле, например, ваша SD-карта — тоже неизвестный источник, поэтому — если установка программ из неизвестных источников запрещена — просто так установить с нее APK-файл, присланный приятелем, уже не получится. Зато вы предотвратите потенциальную угрозу.

Для отключения установки из неизвестных источников перейдите в меню **Настройки | Экран блокировки и защита** и *выключите* (переведите в неактивное состояние) параметр **Неизвестные источники** (рис. 8.1).

Чтобы вновь получить возможность устанавливать APK-файлы, полученные извне, включите этот параметр для конкретной установки. По крайней мере, вы установите эти APK-файлы осознанно. Думаю, не стоит говорить, что для большей безопасности после установки действительно требуемых APK-файлов параметр **Неизвестные источники** следует выключить снова.



**Рис. 8.1.** Отключение установки из неизвестных источников

## 8.3. Осторожно: неизвестные сети Wi-Fi!

### Шифруем передаваемые данные

Не подключайтесь к неизвестным сетям Wi-Fi, особенно к публичным, происхождение которых вам неизвестно. Может быть, кто-то просто не смог правильно настроить маршрутизатор Wi-Fi, не установил на нем соответствующий пароль, и теперь к его сети может получить доступ любой желающий, и вы в том числе.

А может, такая сеть развернута злоумышленниками преднамеренно, чтобы перехватывать все передающиеся по ней данные, в том числе и конфиденциальные, — такие как пароли и номера банковских карт и сопутствующая им финансовая информация.

Вообще, с осторожностью относитесь к публичным сетям (аэропорта, ресторана, отеля и т. п.). Никогда нельзя знать, как они настроены. Если приходится передавать данные по таким сетям, шифруйте передаваемые данные.

В главе 3 мы говорили о выборе VPN-сервиса для вашего компьютера. Наверняка вы уже выбрали какой-либо VPN-сервис, исходя из поставленных задач. Причем практически каждый VPN-сервис предоставляет своим пользователям Android-клиент.

Если VPN нужен вам редко — например, при подключении к тем же неизвестным сетям в путешествии, вам вполне хватит бесплатного тарифного плана GREEN от SecurityKISS — 300 Мбайт трафика в сутки (см. разд. 3.2.7). Для более серьезной работы этого, конечно, мало, но, находясь в дороге, вы сможете прочитать почту, зайти на какой-нибудь сайт, воспользоваться банковским приложением — и все это безопасно, поскольку весь ваш трафик будет зашифрован.

Установите это приложение на свой смартфон или планшет, введите данные аккаунта (имя пользователя и пароль), выберите сервер (если нужно) и нажмите кнопку **Connect** (рис. 8.2).

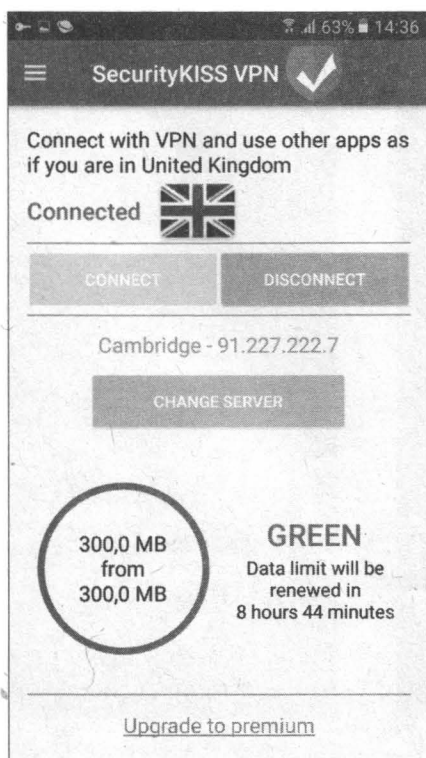


Рис. 8.2. VPN-клиент SecurityKISS для Android

## 8.4. Анонимность в Android: установите Tor

Android-устройства, мягко говоря, не анонимны. Если даже вы используете VPN-сервис, то все равно все действия выполняете под своим аккаунтом. Конечно, аккаунт можно создать непосредственно для конкретного устройства и не использовать его в реальной жизни — тогда интересующимся еще предстоит потрудиться, выясняя, кто вы. Но если аккаунт используется повседневно, например для чтения почты, покупок и т. п., то ни о какой анонимности не может быть и речи.

О том, что такое Tor, было рассказано в *главе 2*. Сейчас же мы разберемся, как использовать его в Android.

Tor-клиент для Android называется Orbot и загрузить его можно по ссылке: <https://play.google.com/store/apps/details?id=org.torproject.android>.

Установив Orbot, запустите его. Пролистайте информационные страницы и нажмите кнопку **Готово** (рис. 8.3).

Далее вы увидите экран приложения (рис. 8.4). Центральная кнопка **Запустить** служит для запуска прокси. Список **Мир (авто)** позволяет выбрать выходной



Рис. 8.3. Первый запуск Orbot

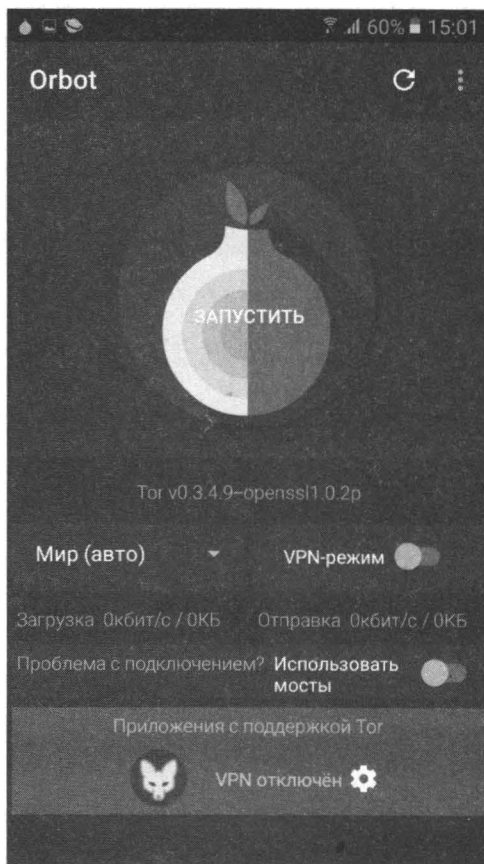


Рис. 8.4. Экран приложения Orbot

узел — здесь можете выбрать, IP-адрес какой страны мира вы хотите получить. Переключатель **VPN-режим** активирует VPN-режим.

Теперь разберемся, как всем этим пользоваться. Для запуска прокси Тог нажмите кнопку **Запустить** и дождитесь, когда прокси будет запущен (рис. 8.5).

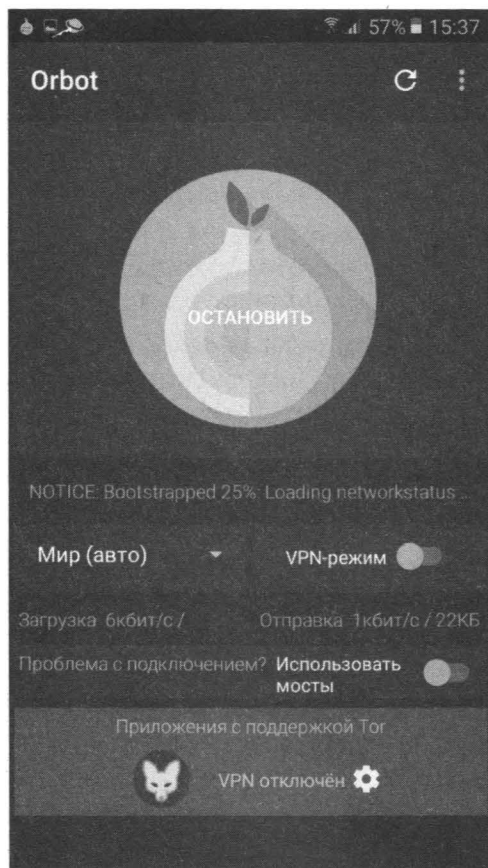


Рис. 8.5. Прокси запущен

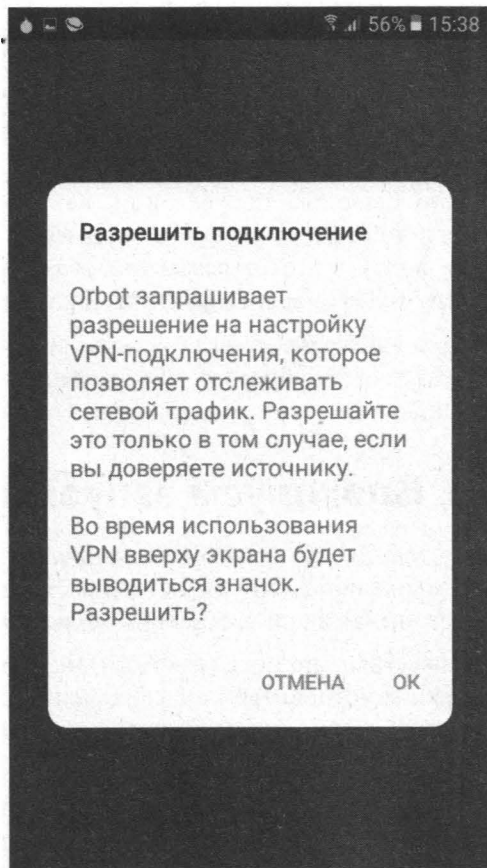


Рис. 8.6. Включение VPN

После этого (до включения VPN-режима) работать через Тог смогут лишь приложения, настроенные на прокси. Напомню, что раньше нужно было настраивать на прокси приложения самостоятельно, и не всегда это получалось. Теперь же у нас есть VPN-режим (рис. 8.6), включив который, вы можете перенаправить через Тог трафик всех ваших приложений: Skype, Viber, браузеров и т. п. По сути, вы получаете бесплатный VPN, пусть и скорость его не очень высока.

Проведите небольшой эксперимент:

1. Включите прокси — нажмите кнопку **Запустить**.
2. Используя любой браузер, например Google Chrome или стандартное приложение Браузер от Android, определите свой IP-адрес (можно для этого использо-

вать сайт [www.geoiptool.com](http://www.geoiptool.com) или любой другой). Вы увидите свой IP-адрес, предоставленный вам провайдером (при работе через Wi-Fi) или оператором сотовой связи.

3. Включите VPN-режим.
4. Обновите страничку с IP-адресом. Вы увидите уже другой IP-адрес — произвольный IP-адрес сети Tor.

VPN — это, конечно, хорошо, но вас все равно могут деанонимизировать. Ведь вы работаете с использованием привычных аккаунтов (Skype, Viber, Google), которые наверняка регистрировали не через Tor. И это понятно — вы не установите Orbot, пока не создадите Google-аккаунт.

Можно было бы посоветовать вам создавать анонимные аккаунты, не сообщая ничего личного о себе, — например, с помощью публичных сетей аэропорта или кафе, но путь этот отрезан требованием авторизации в таких публичных сетях по номеру телефона, т. е., фактически, по паспорту.

Однако вы все же можете использовать для анонимного посещения Сети приложение Orfox — это браузер, который при серфинге не использует ваш Google-аккаунт. Он уже настроен на прокси, и для его работы не нужно даже включать VPN-режим.

## 8.5. Блокируем запуск приложений

Представьте, что кто-то подсмотрел ваш PIN-код разблокировки смартфона, а затем, дождавшись, что вы оставите смартфон на столе, разблокировал его. Теперь он может читать ваши сообщения во всех мессенджерах, ваши SMS, вашу почту...


Приложение App Lock (разработчик SPSoft) — это защитник ваших личных данных на любом устройстве под управлением ОС Android. С его помощью можно защитить все: SMS, электронную почту, фотографии, контакты, а также запретить запуск отдельных приложений.


Использовать приложение предельно просто — нужно задать графический ключ, указать, что нужно защищать, и перевести приложение в режим защиты. После этого никто к вашим личным данным доступа не получит. А в платной версии программы предусмотрена возможность организовать фото- и видеосъемку нарушителя, что как раз и поможет обнаружить недобросовестного человека, который попросил ваш смартфон якобы позвонить, а сам попытался залезть в хранящиеся на нем личные данные.

Обойти защиту приложения невозможно, если, конечно, быстренько не получить на чужом смартфоне права root. А поскольку это дело не пяти минут, вы можете быть уверены, что никто, взявши ваш смартфон с просьбой позвонить, или когда вы оставите его на столе, отойдя от него ненадолго, не сможет добраться до ваших личных данных.

Приложение App Lock имеет одну важную особенность. Если его удалить какими-либо специальными утилитами, то оно унесет вместе с собой все, что защищало. То есть, если некто попытается удалить с вашего телефона это приложение, чтобы получить доступ к защищаемым им данным, то эти данные тоже будут удалены. Во

всяком случае это лучше, чем если бы они попали в руки «захватчика». А вы ни в коем случае не должны забыть открывающий приложение графический ключ! Иначе придется очень постараться, чтобы избавиться от приложения без потери данных. И еще — полагаю, не стоит говорить, что для разблокировки экрана и приложения App Lock следует использовать разные графические ключи.

При первом запуске App Lock попросит вас установить PIN-код для его разблокировки, после чего вы увидите основной экран. На вкладку **Приложения** (рис. 8.7) с помощью кнопки  добавьте приложения, запуск которых вы хотите запретить посторонним (рис. 8.8).

App Lock почти готов к использованию. Но прежде я хочу обратить ваше внимание на еще одну интересную его особенность. Перейдите к списку защищаемых приложений (см. рис. 8.8). Напротив каждого приложения вы увидите кнопку . Если режим FAKE активен, то при запуске приложения вместо приглашения ввести пароль будет отображено окно, имитирующее ошибку запуска приложения. Приложение не запустится, а злоумышленник решит, что просто произошел сбой. Чтобы запустить приложение, защищенное режимом FAKE, следует запустить App Lock и выключить режим FAKE, а уже затем запускать приложение. Ну а при запуске приложения с выключенным режимом FAKE будет запрошен пароль.

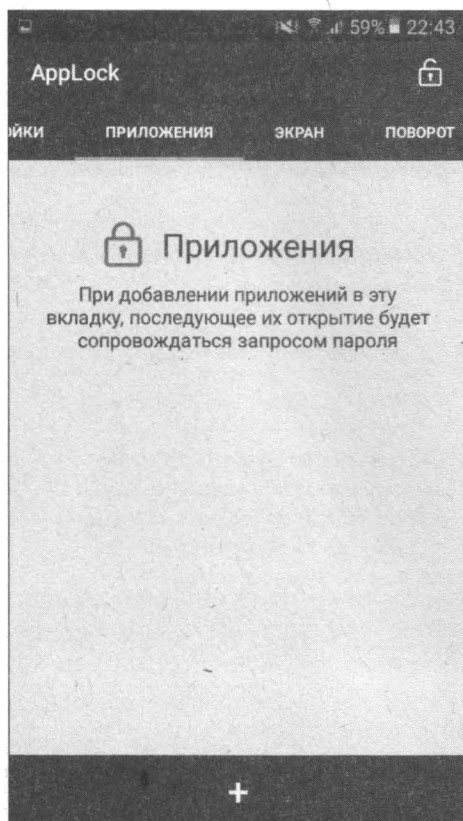


Рис. 8.7. Основной экран App Lock

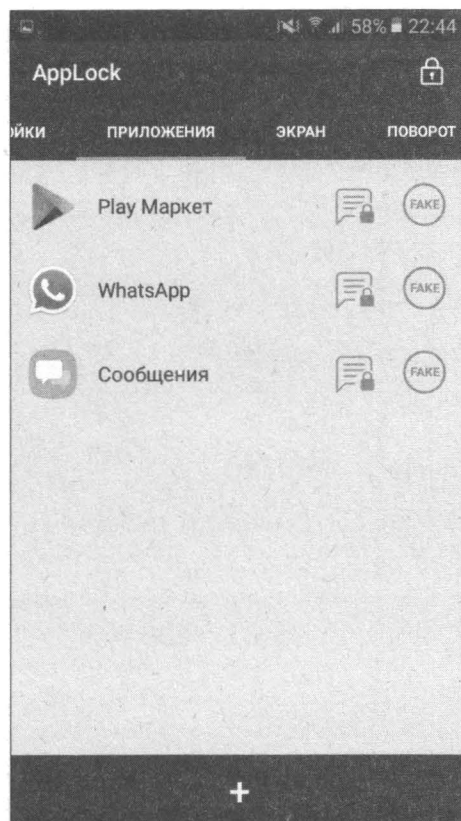


Рис. 8.8. Ряд защищаемых приложений добавлен в список вкладки Приложения



## 8.6. Шифрование данных в Android

### 8.6.1. Шифрование стандартными средствами

Операционная система Android поддерживает шифрование данных. Однако в отличие, например, от iOS, Android автоматически не шифрует данные, находящиеся на устройствах. Тем не менее шифрование можно легко включить, а как именно, мы сейчас и узнаем.

Шифрование устройства означает, что если смартфон заблокирован, файлы на нем зашифрованы. При этом любые файлы, передаваемые с вашего смартфона, например, на компьютер или другой смартфон, зашифрованы не будут. Сам процесс обмена данными (по Bluetooth, Wi-Fi и т. п.) тоже не зашифрован — для этого следует использовать методы, рассмотренные в *главе 6*. Но если вы скопируете файл с компьютера или с другого смартфона на свой смартфон, то он автоматически станет зашифрованным.

Для расшифровки файлов используется пароль, который вы вводите для разблокировки смартфона. Если шифрование выключено, то этот пароль просто ограничивает доступ к экрану вашего смартфона и ничего более полезного не делает. А вот

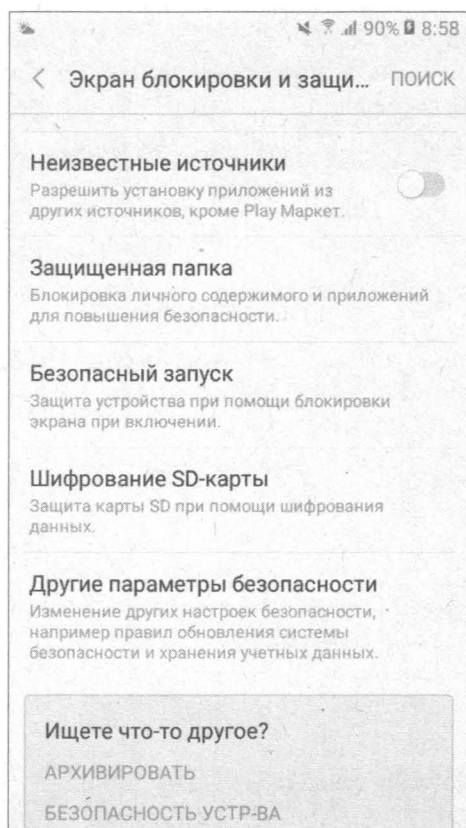


Рис. 8.9. Выберите команду Шифрование SD-карты

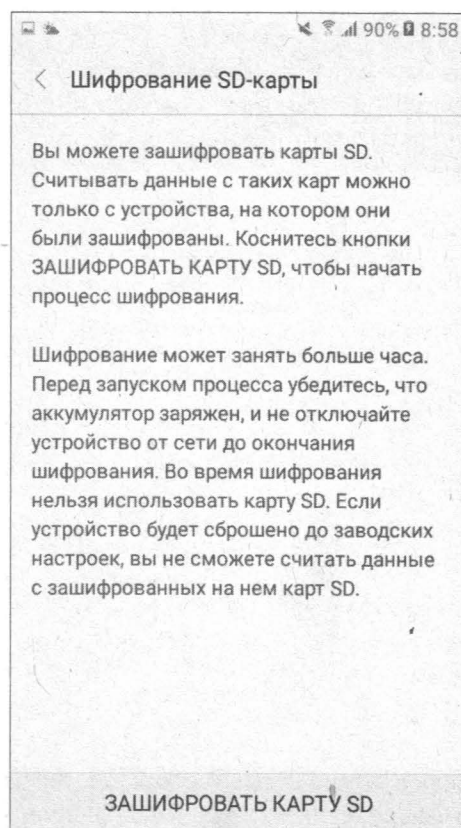


Рис. 8.10. Включение шифрования

если шифрование включено, то пароль — это ключ, служащий для дешифрования данных. И даже если злоумышленник найдет способ обхода экрана блокировки, ваши файлы все равно останутся зашифрованными.

Включить шифрование на Android-устройстве довольно-таки несложно: перейдите в **Настройки**, затем в раздел **Экран блокировки и защита** (в некоторых версиях Android этот раздел называется **Безопасность**) и выберите команду **Шифрование SD-карты** (рис. 8.9).

Появится экран, на котором нужно нажать кнопку **Зашифровать SD-карту** и подождать (рис. 8.10).

## 8.6.2. Сторонние программы шифрования

Могу порекомендовать две программы шифрования данных (все они доступны на Play Маркет):

- ☐ LUKS Manager;
- ☐ EDS Lite.

### Программа LUKS Manager

Программа LUKS Manager — старейшая программа шифрования файлов в Android. Она 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 смартфона).

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

Есть у программы и недостатки. В частности, она требует для своей работы прав root. Не поддерживает LUKS Manager и контейнеры TrueCrypt, которые стали сейчас де-факто практически стандартом. А жаль — очень удобно было бы создать на компьютере зашифрованный контейнер TrueCrypt, поместить его на флешку, а затем — при необходимости — на смартфон, где можно было бы работать с ним как с обычной папкой.

### Программа EDS Lite

Программа EDS Lite — хоть и молодая, но весьма 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 и эта программа не идеальна. Шифрование осуществляется не «на лету», и с зашифрованным контейнером нельзя работать как с обычной папкой. Однако программа содержит 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 EDS

Lite и скопировать в него все файлы, которые нужно зашифровать. Не очень, конечно, это удобно (нельзя использовать сторонние файловые менеджеры типа ES Проводник), но работать можно.

Плохо здесь то, что остальные программы не поддерживают контейнеры EDS Lite. То есть, чтобы зашифровать документ, созданный в текстовом редакторе, вам придется явно поместить его в контейнер.

А хорошо, что после помещения файлов в контейнер с ними можно работать без копирования на карту памяти. Например, если вы поместили в контейнер музыку, то ее можно будет воспроизвести из контейнера, но только потреково, — т. к. стандартное приложение для воспроизведения не увидит содержимое контейнера.

Да, есть определенные неудобства. Зато программа поддерживает два алгоритма шифрования: AES-256 и SHA-512.

Давайте рассмотрим программу EDS Lite подробнее.

Установите и запустите программу. В боковом меню (рис. 8.11) найдите команду **Управление контейнерами** и нажмите кнопку **+** для создания нового контейнера. Программа попросит выбрать (рис. 8.12), что вы хотите сделать: создать новый

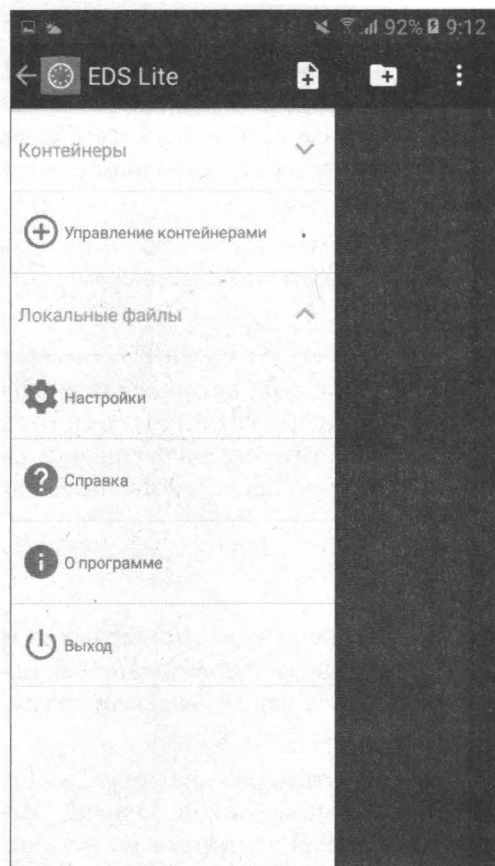


Рис. 8.11. Боковое меню программы EDS Lite

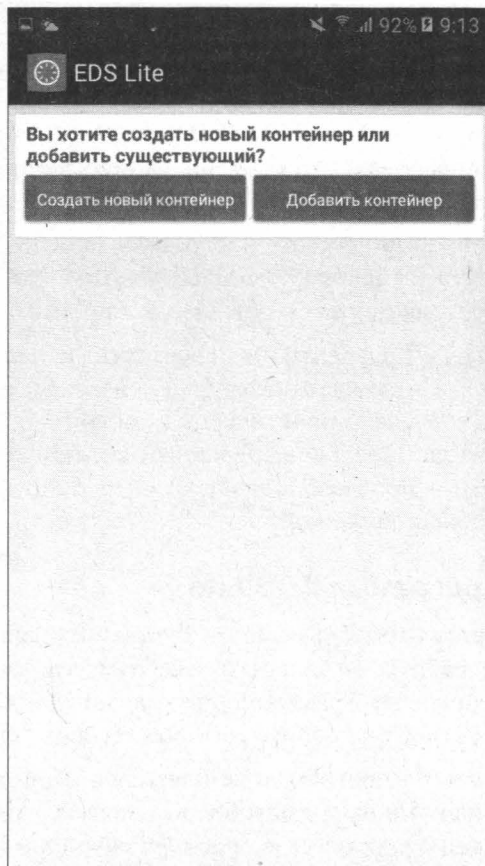


Рис. 8.12. Программа EDS Lite: создать новый контейнер или добавить существующий?

контейнер или добавить уже существующий. Выберите создание нового контейнера.

Экран создания контейнера показан на рис. 8.13. Основные параметры здесь:

- ❑ **Формат контейнера** — по умолчанию используется формат TrueCrypt, но вы можете выбрать любой другой (рис. 8.14).

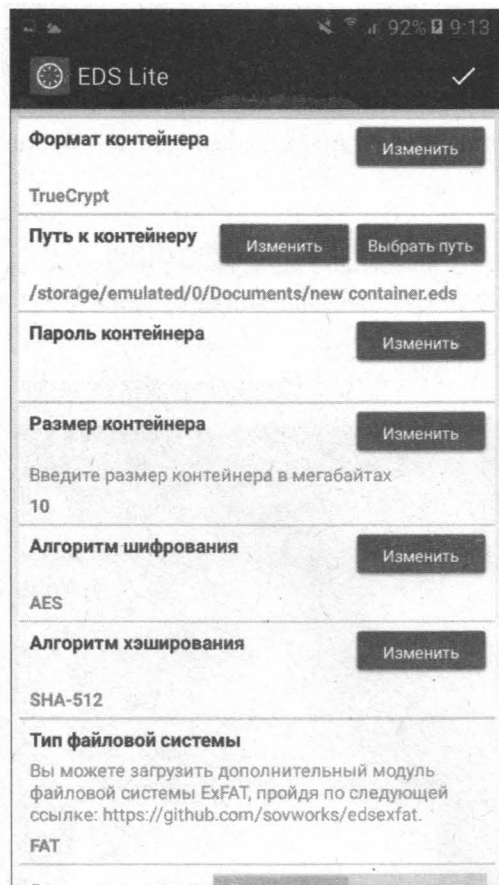


Рис. 8.13. Программа EDS Lite: создание нового контейнера

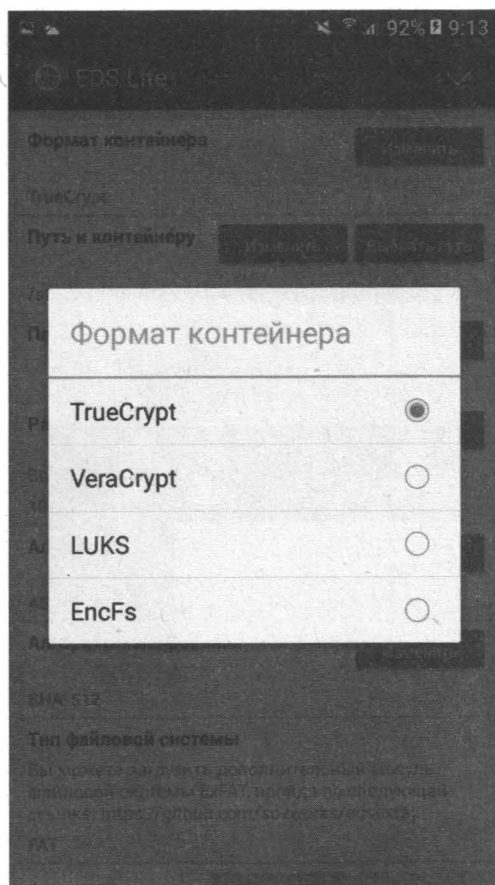


Рис. 8.14. Программа EDS Lite: выбор формата контейнера

- ❑ **Путь к контейнеру** — лучше создавать контейнеры на внешней SD-карте. Даже в случае выхода устройства из строя, внешнюю SD-карту можно будет извлечь и прочитать данные. Да и места на внешней карте, как правило, больше;
- ❑ **Пароль контейнера** — программа, к сожалению, допускает использование простых паролей. Ради интереса я ввел пароль `qwerty`, и программа его «проглотила». Не предусмотрено и поле 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. 8.13 показано, что созда-

ется контейнер размером 10 Мбайт. Это значение по умолчанию, и оно очень мало. Столь маленький контейнер можно создать или чтобы научиться работать с программой, или если вам нужно хранить в контейнере только лишь текстовые документы, которые не занимают много места. Определите размер контейнера, исходя из своих потребностей. Кому-то и 20 Мбайт будет достаточно, а кому-то и 2 Гбайт мало.

Остальные параметры можно оставить без изменения. Нажмите кнопку с галкой в верхнем правом углу окна программы (см. рис. 8.13) и подождите, пока контейнер не будет создан. Все созданные контейнеры появятся в боковом меню (рис. 8.15).

Давайте теперь разберемся, как поместить файл в контейнер. Первым делом нужно открыть контейнер.

### ПРИМЕЧАНИЕ

Не пытайтесь открыть контейнер из списка контейнеров — у вас ничего не получится. Это, очевидно, просчет разработчиков программы с точки зрения эргономики. Открыть контейнер можно только через боковое меню.

Выберите контейнер в боковом меню программы и введите его пароль (рис. 8.16).

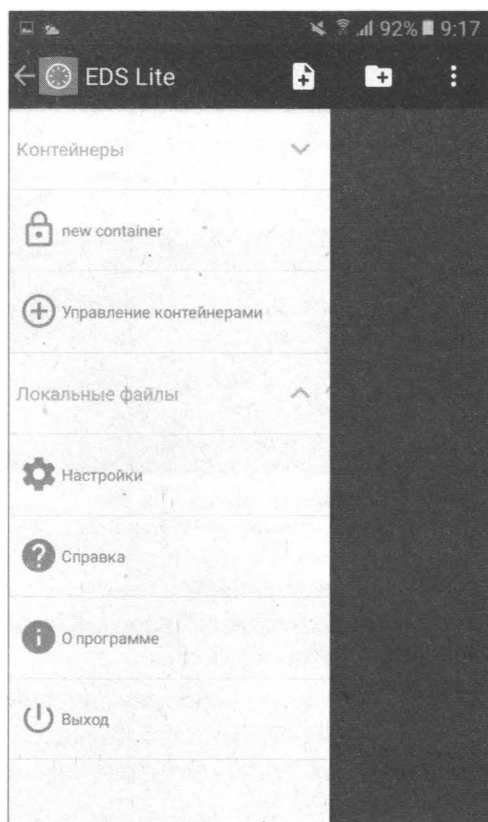


Рис. 8.15. Программа EDS Lite: список контейнеров

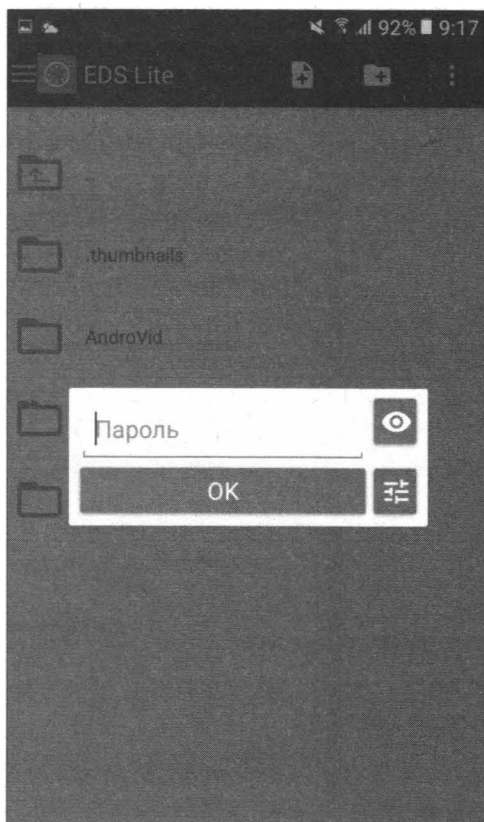




Рис. 8.16. Программа EDS Lite: ввод пароля

Используя боковое меню, перейдите к месту файловой системы, где находится секретный файл. Выберите файл или файлы (рис. 8.17), нажмите кнопку копирования , перейдите к контейнеру (тоже через боковое меню) и нажмите кнопку вставки . Дождитесь, пока файлы будут помещены в контейнер (рис. 8.18).

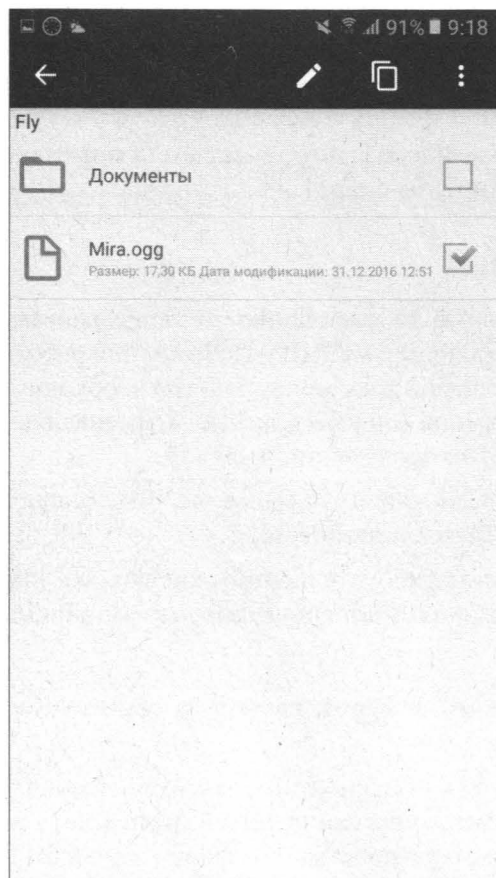


Рис. 8.17. Программа EDS Lite:  
выбор файлов для помещения в контейнер

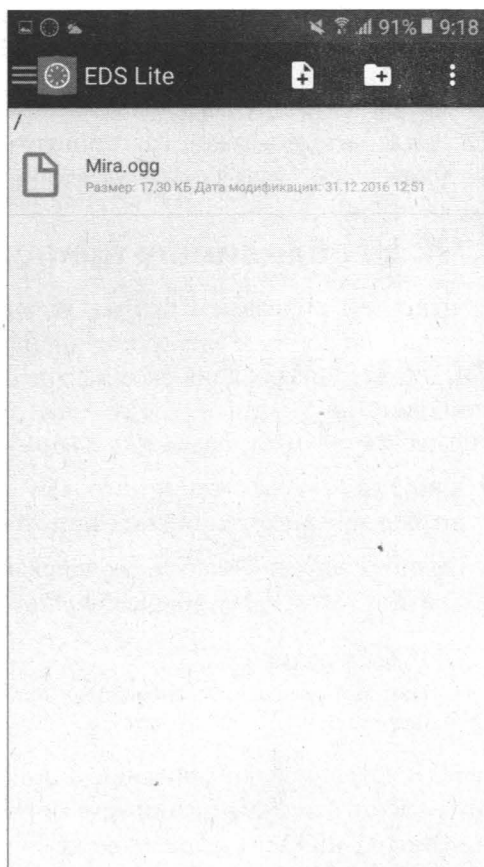


Рис. 8.18. Программа EDS Lite:  
файлы вставлены в контейнер

Теперь не забудьте удалить исходный файл, чтобы его копия не осталась на файловой системе устройства.

Подведем итог по части преимуществ программы EDS Lite:

- ☐ не требует прав root;
- ☐ позволяет зашифровать только те файлы, которые нужно, а не всю карту или все устройство.

Недостаток только один — несколько неудобная работа с файлами. Использовать программу или нет — решать только вам. Существует полная версия этой программы: EDS. Она призвана исправить недостатки бесплатной — в ней вы можете подмонтировать контейнер к каталогу файловой системы и работать как с обычной



папкой. Перспектива заманчива, однако для монтирования нужны права root, а не каждый пользователь захочет «ломать» свое устройство, особенно если оно на гарантии, — ведь неродная прошивка означает автоматический отказ от гарантии. Впрочем, стоит полная версия недорого, и если ваше устройство уже «рутировано», попробовать однозначно стоит.

## 8.7. Шифруем почту

В *главе 6* было показано, как защитить электронную почту на вашем компьютере. Здесь мы рассмотрим защиту электронной почты на смартфоне.

### 8.7.1. Необходимые приложения

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

- ❑ MailDroid — собственно, это сам почтовый клиент. Ссылка на Play Маркет: <https://play.google.com/store/apps/details?id=com.maildroid>;
- ❑ Crypto Plugin — плагин, поддерживающий работу с сертификатами. на Play Маркет: <https://play.google.com/store/apps/details?id=com.flipdog.crypto.plugin>.

#### ПРИМЕЧАНИЕ

Нам не нужны Pro-версии этих 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 их на SD-карту или во внутреннюю память вашего устройства (создание ключей было рассмотрено в *главе 6*).

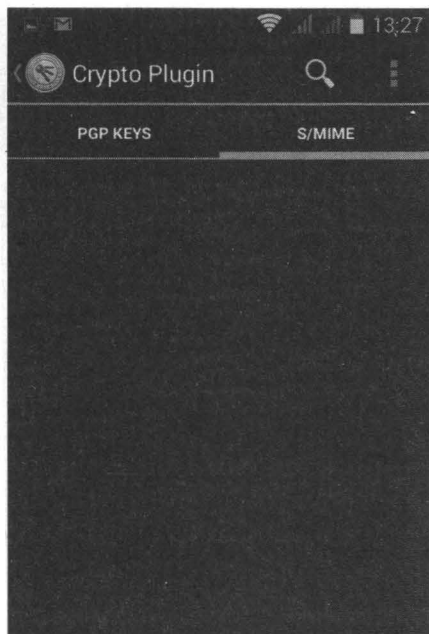
### 8.7.2. Настройка Crypto Plugin

Первым делом надо настроить плагин Crypto Plugin. Перейдите на вкладку S/MIME (рис. 8.19) и выберите команду **Import Certificate** (рис. 8.20).

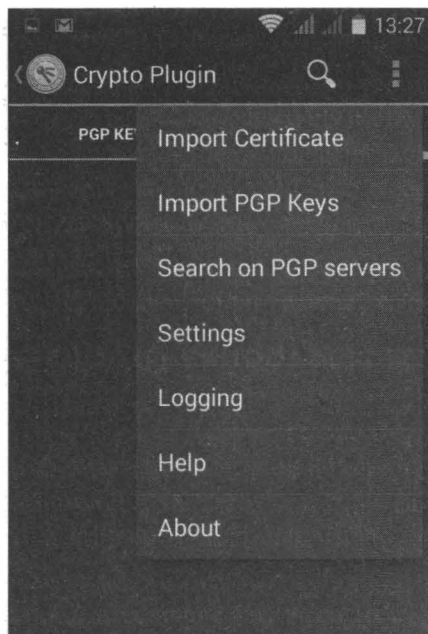
Сначала следует импортировать корневой сертификат. Его файл называется Root Certificate (см. рис. 6.10, б). Перейдите к каталогу своего устройства, в который вы поместили файл Root Certificate.cer, и выберите его (рис. 8.21). Программа спросит вас, как открыть файл, — выберите вариант **Standard**. Импортированный сертификат появится в списке сертификатов (рис. 8.22).

Затем операцию импорта нужно повторить для вашего личного сертификата (файл с расширением **pkx**) и сертификатов всех, с кем вы планируете обмениваться зашифрованными сообщениями и ЭЦП (рис. 8.24). При импорте личного сертифи-





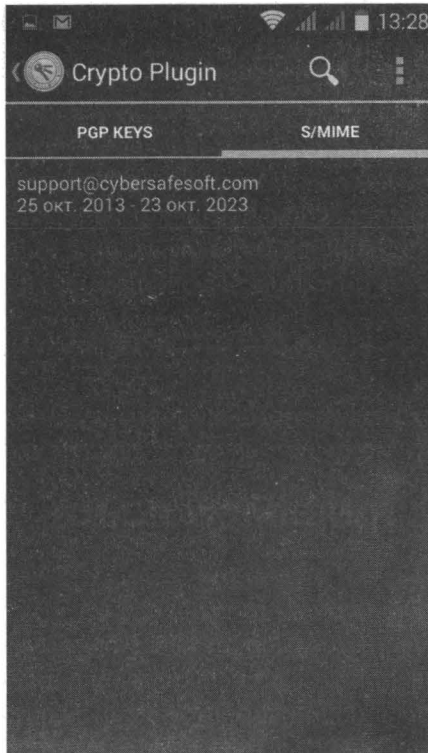
**Рис. 8.19. Плагин Crypto Plugin:**  
вкладка S/MIME



**Рис. 8.20. Плагин Crypto Plugin:**  
выберите команду Import Certificate



**Рис. 8.21. Плагин Crypto Plugin:**  
открытие сертификата



**Рис. 8.22. Плагин Crypto Plugin:**  
корневой сертификат импортирован



Рис. 8.23. Плагин Crypto Plugin: импортированы все сертификаты

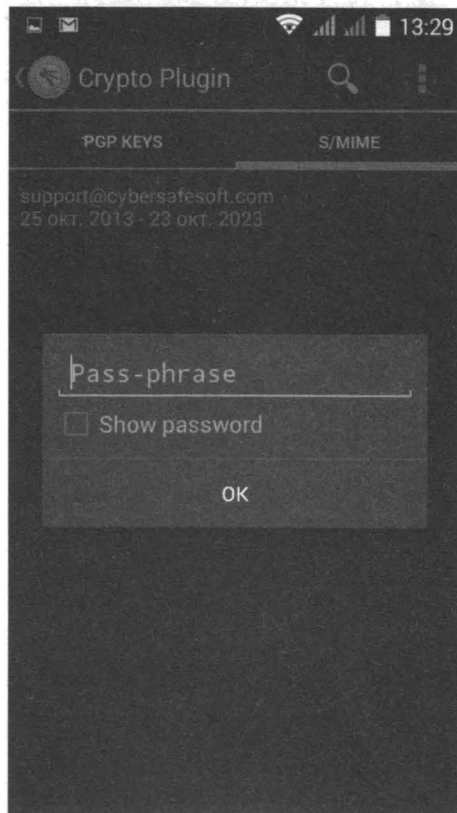


Рис. 8.24. Плагин Crypto Plugin: запрос пароля при импорте личного (приватного) сертификата

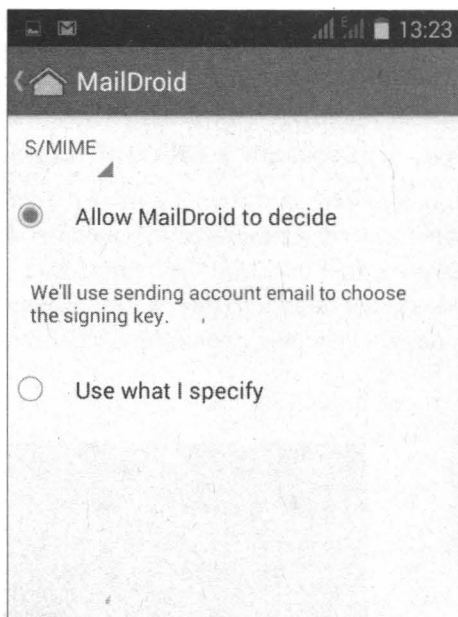
ката будет запрошен пароль (рис. 8.25). Обратите внимание: ваш личный сертификат помечен в списке как **PRIVATE**.

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

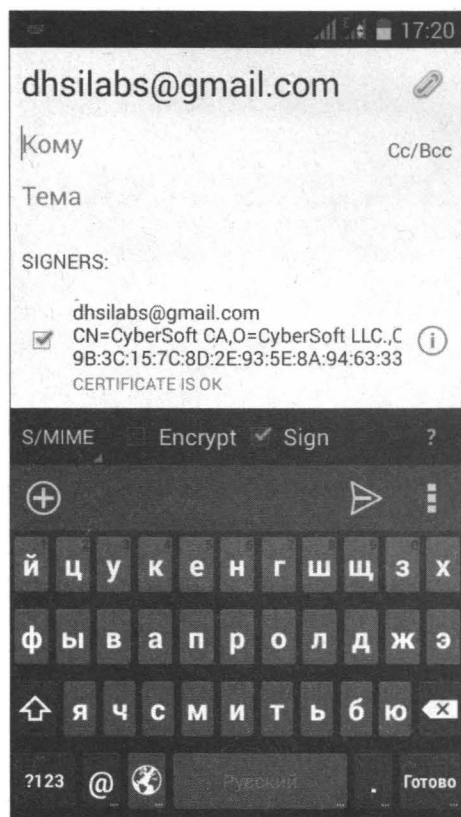
### 8.7.3. Настройка MailDroid

Перед началом обмена зашифрованными сообщениями необходимо проверить некоторые настройки программы. Откройте экран настроек MailDroid. Перейдите в раздел **Encryption Plugin**. Убедитесь, что выбран режим шифрования **S/MIME** и включен переключатель **Allow MailDroid to decide** (рис. 8.25).

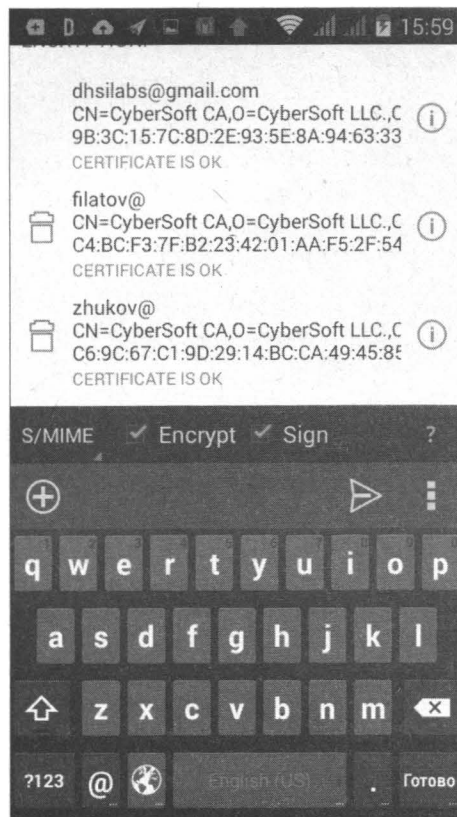
При создании нового сообщения в MailDroid вы можете подписать и зашифровать его. Если нужно только подписать сообщение — включите переключатель **Sign** (рис. 8.26). Если нужно не только подписать, но и зашифровать сообщение, включите еще и переключатель **Encrypt**. При подписании сообщения надо выбрать, какой сертификат будет использоваться. Выбор сертификата происходит в области **SIGNERS**. Скорее всего, у вас будет всего один сертификат.



**Рис. 8.25.** Программа MailDroid: включение режима шифрования



**Рис. 8.26.** Программа MailDroid: электронная подпись письма и выбор сертификата



**Рис. 8.27.** Программа MailDroid: сертификаты получателей

При шифровании письма сертификаты всех его 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. 8.27). Она также выполнила проверку сертификатов получателей — обратите внимание на результат проверки сертификата: **CERTIFICATE IS OK**.

Теперь рассмотрим работу с зашифрованными и подписанными сообщениями. Пришедшее вам зашифрованное сообщение будет отмечено значком замка. Откройте это сообщение. Программа сообщит, что оно зашифровано: **Encrypted**. Нажмите на ссылку **Click** для расшифровки сообщения (рис. 8.28). Введите пароль вашего сертификата (рис. 8.29). Если пароль введен правильно, сообщение будет расшифровано.

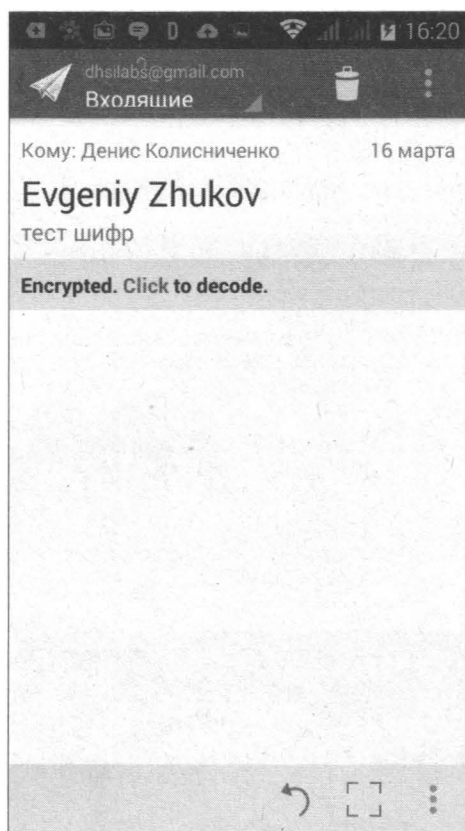


Рис. 8.28. Программа MailDroid: нажмите **Click** для расшифровки

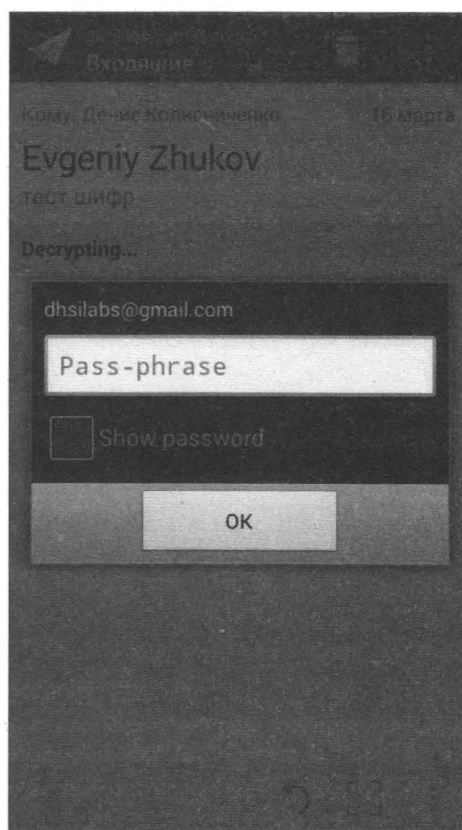


Рис. 8.29. Программа MailDroid: введите пароль сертификата

### 8.7.4. Последний шаг

После установки и настройки MailDroid следует отключить стандартный почтовый клиент Gmail, чтобы не получать уведомления о новой почте из двух программ.

Для этого выполните следующие действия:

- ☐ откройте окно настроек Android, выбрав меню **Настройки**;
- ☐ выберите **Приложения**;
- ☐ перейдите на вкладку **Все**;
- ☐ выберите **Gmail**;
- ☐ нажмите кнопку **Остановить**;
- ☐ нажмите кнопку **Отключить**.

## 8.8. Отключение GPS-модуля

Во избежание отслеживания вашего передвижения (некоторые вредоносные программы могут передавать ваши GPS-координаты третьей стороне) отключите GPS-модуль, когда вы им не пользуетесь. Конечно, есть моменты, когда GPS необходим. В этом случае придется определить, какая программа (кроме программы навигации) обращается к демону `gpsd`.

Отключение GPS-модуля также поможет сэкономить заряд аккумулятора. Именно поэтому я рекомендую всегда отключать GPS, когда он вам не нужен. Лично мой планшет с включенным GPS-модулем значительно быстрее разряжается (а при запущенной программе навигации его вообще хватает на 3 часа).

Итак, перейдите в меню **Настройки** | **Подключения** и снимите флажок с параметра **Геоданные**. Помните, что отключение этих параметров всего лишь не позволит программам получать доступ к данным о вашем местоположении.

Если же вы не хотите, чтобы оператор сети знал<sup>1</sup>, где вы находитесь, выключите устройство и извлеките из него аккумулятор. Кнопка выключения — это не аппаратное выключение, когда физически размыкаются контакты, а всего лишь так называемый *soft-off* — т. е. теоретически устройство все еще может принимать и передавать данные. Гарантировать, что произошло полное отключение устройства может лишь извлечение аккумулятора. Вот только многие современные смартфоны не позволяют извлекать аккумулятор, и в этом случае избавиться от слежки (если она есть) вряд ли выйдет. Поэтому, если вдруг возникла такая реальная необходимость, самый лучший способ оторваться от нее — «забыть» смартфон в общественном транспорте ☺.

---

<sup>1</sup> Может ли оператор установить местоположение выключенного телефона? Ответ на этот вопрос читайте по адресу: <http://habrahabr.ru/post/112449/>.



## ГЛАВА 9



# Устраняем утечки информации

## 9.1. Чем грозит утечка персональных данных?

Для начала нужно определиться, что есть *персональные данные*. «Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)». Это определение из того самого ФЗ-152<sup>1</sup>, в котором сказано, что такое персональные данные и как их следует защищать.

Другими словами, персональные данные — это любая информация о вас, которая может использоваться не всегда с благими намерениями. Поэтому персональные данные нужно защищать. ФЗ-152 описывает, как следует защищать персональные данные, хранимые и обрабатываемые операторами персональных данных, — любыми компаниями, которым вы эти данные предоставляете. Естественно, вы не знаете, как тщательно тот или иной оператор хранит ваши персональные данные, поэтому здесь правило одно: чем меньше информации о себе вы предоставляете, тем лучше.

А вот ваш компьютер, ваш облачный диск, ваша страница в социальной сети — это просто кладезь персональных знаний о вас. Так что в этой главе мы попытаемся помочь вам устранить утечки этой информации — чтобы ваши персональные данные не попали в чужие руки.

Утечка персональных данных помогает выследить человека, спланировать преступление против него или же выдать постороннего человека за субъекта персональных данных. Это опасно как с моральной, так и с материальной стороны, поскольку чревато как потерей денег, так и нервов и времени, что порой гораздо дороже материальной составляющей.

Примеры последствий утечки персональных данных в крупных масштабах легко найти в Интернете. Мы же рассмотрим в качестве примера историю гражданина N. Итак, гражданин N владеет почтовым ящиком `n@example.com`, а также счетом

---

<sup>1</sup> Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных».



в банке «Б» с онлайн-доступом. В качестве логина для доступа в банк он использует адрес своей электронной почты `p@example.com`. Гражданин N — далеко не самый глупый гражданин, и он установил для электронной почты и для личного кабинета онлайн-банкинга разные пароли.

Как-то раз гражданин N зарегистрировался в одном из интернет-магазинов с использованием электронной почты `p@example.com` и произвел оплату товара платежной картой банка «Б». Нет, его не обманули — товар был доставлен вовремя, а со счета была списана оговоренная ранее сумма. Все честно.

Но оказалось, что в этом интернет-магазине работал нечестный сотрудник А, который захотел воспользоваться служебным положением и завладеть средствами гражданина N.

По номеру платежной карточки сотрудник А легко вычислил банк гражданина N. Адрес онлайн-банкинга — это всем известная информация. Сначала А попытался ввести пароль, указанный гражданином N при регистрации в магазине. Как же так? Пароли ведь хранятся зашифрованными! А вы уверены в том, что так устроен любой интернет-магазин? Вполне вероятно, что именно этот магазин хранит пароли пользователей в открытом виде. Бывает и так, причем очень часто, что нередко в качестве платформы интернет-магазина используется популярная система Magento, которая как раз и хранит пароли пользователей в зашифрованном виде. Но в конфигурационном файле Magento находится ключ, которым шифруются пароли и другая информация. Это надо для перехода (если нужно) на другую платформу. Если сотрудник А — не рядовой менеджер, а администратор магазина, то у него есть доступ к ключам, и расшифровать ему ваш пароль — дело техники.

Пароль, понятное дело, не подошел, поскольку гражданин N не поленился и для регистрации в магазине придумал третий пароль. Теперь у него есть три пароля: от электронки, от магазина и от банкинга. Понятно, если бы он указал один пароль во всех трех случаях, это бы существенно упростило задачу не очень честному сотруднику А.

Однако при регистрации N указал персональные данные о себе — кличку любимого домашнего питомца. Эти данные обычно используются для восстановления пароля на случай, если пользователь его забудет. Увы, но N указал одни и те же персональные данные во всех трех случаях. Так что сначала сотрудник А получил доступ к его электронной почте — ведь данные для восстановления пароля у него уже были, а затем и к банкингу — путем сброса пароля доступа в онлайн-банк. На e-mail, которым уже овладел А, пришла ссылка сброса пароля, пароль был успешно сброшен, и А попал в онлайн-банкинг гражданина N. После чего он перевел все его средства на несколько виртуальных платежных карт, выпущенных зарубежными банками. Собственно, на этом все — гражданин N остался без денег. Конечно, потом будет заявление в полицию, злоумышленника будут искать, и т. п. Однако, если А не был столь глуп, чтобы засветить свой IP-адрес, найти его будет не так уж и просто. Да и какая разница — все это будет потом. А пока у гражданина N случился нервный срыв, и он оказался на больничной койке. Такая вот нередкая история...

Разберем ошибки гражданина N:

- ❑ первая типичная ошибка — использование одного и того же e-mail для личной и публичной переписки. Всегда надо иметь как минимум два разных почтовых ящика: один e-mail использовать для регистрации во всевозможных форумах, магазинах и прочих публичных местах, а другой — для личной переписки и, в том числе, для входа в онлайн-банкинг;
- ❑ вторая типичная ошибка — гражданин N не настроил двухфакторную аутентификацию в онлайн-банкинге, поэтому его деньги списались со счета без какого бы то ни было подтверждения. При двухфакторной аутентификации он должен был бы получить SMS с кодом, подтверждающим перевод денег. Однако и в этом случае A мог бы обмануть N.

Рассмотрим такую ситуацию. A инициирует перевод денег со счета N на свой. Гражданин N получает от банка SMS о том, что с его счета будет списана такая-то сумма, и в этом SMS содержится код подтверждения операции. С момента инициации перевода до момента получения им SMS проходит несколько секунд. Практически моментально гражданину N звонит «сотрудник банка» (как вы догадались, это наш A) и сообщает, что с его счета злоумышленниками была списана крупная сумма денег, и просит назвать код из SMS для отмены операции. Если гражданин N не сориентировался и не понял, что к чему, он сообщает код. В результате деньги уходят. Вы можете возразить: ведь A «засветит» свой номер. Может, засветит, а может и нет. Он может арендовать зарубежный номер и позвонить с него — так будет даже солиднее. Пока правоохранительные органы будут разбираться, кто этот номер арендовал (и не факт, что это получится), деньги уже будут два раза как потрачены;

- ❑ и чтобы не совершить третью типичную ошибку: никому (даже сотруднику банка) нельзя сообщать коды подтверждения операций, которые приходят от онлайн-банкинга. Если вам позвонили с таким вопросом, нужно прервать разговор со злоумышленником и позвонить по номеру, указанному на обороте карты — так вы точно дозвонитесь в банк. Затем надо заблокировать карту и заказать в банке новую. Так вы сохраните свои деньги.

Как видите, гражданина N не спасло даже использование трех разных паролей (причем не важно, насколько сложны они были). Его сгубило небрежное отношение к своим персональным данным и отсутствие двухфакторной аутентификации.

Тем не менее, сложность пароля никто не отменял. И если бы для доступа к почтовому ящику `n@exmaple.com` использовался пароль типа 123456, результат был бы аналогичным. Поэтому в следующем разделе мы поговорим о создании надежного пароля.

## 9.2. Как придумать надежный пароль?

### Критерии надежности. Генераторы паролей

#### 9.2.1. Выбор хорошего пароля

Многие пользователи используют пароли вроде 1, 1234, qwerty, а потом удивляются, почему их почтовый ящик или страница в социальной сети взломаны. Ответ прост — к ним подобрали пароль. Причем злоумышленнику это сделать было очень просто (точнее программе, которую запустил хакер, не пришлось долго работать) — такие пароли подбираются весьма быстро.

Некоторые сервисы не позволяют вводить слишком простые пароли — например, ограничивают их по минимальной длине и требуют наличия в пароле как букв, так и цифр. Но пользователи и тут выкрутились. Например, если требуется длина 8 символов, то вводят пароль 12345678, а если требуется наличие как букв, так и цифр, — qwerty11. Но все это неправильные пароли.

Существуют два основных способа подбора паролей: по словарю и методом грубой силы (от англ. brute force). Первый способ заключается в использовании словаря наиболее популярных слов — программа последовательно перебирает весь свой словарь. Если пароля нет в словаре, то и его подбор невозможен. Второй способ заключается в подборе перестановок букв в слове. Эффективность этого метода зависит от длины пароля — чем меньше длина, тем выше эффективность. Теоретически методом грубой силы можно подобрать любой пароль. Но если пароль длинный (как минимум — 8 символов), на его подбор будет потрачено очень много времени. А за это время может произойти что угодно: или администратор сервера определит, что идет атака brute force, или вы поменяете пароль (и сделаете его еще сильнее), или информация потеряет актуальность... Мы разберемся, как создать хороший пароль, устойчивый к обоим видам атак.

Вот несколько советов, которые помогут вам создать хороший пароль.

- Минимальная длина пароля — 8 символов. Чем больше — тем лучше. От количества символов (длины пароля) зависит количество перестановок букв в слове. Чем больше перестановок, тем сложнее программе подобрать пароль. Наверняка такой подбор будет замечен сервером, и попытка взлома вашего почтового ящика окажется неудачной. Если длина пароля 8 символов, а сам пароль состоит, например, из цифр 0–9, латинских букв нижнего регистра a–z и латинских букв верхнего регистра A–Z, то перестановок может быть  $(10+26+26)^8$ . То есть программе нужно будет сделать 218340105584896 попыток, чтобы подобрать пароль. Но попыток будет еще больше, поскольку программа заведомо не знает, сколько символов в пароле. Следовательно, ей придется проделать гораздо больше попыток, чем  $(10+26+26)^8$ , — хотя и первая может быть удачной, поскольку все зависит от сложности пароля. Многие серверы блокируют на несколько часов доступ к аккаунту после 3–5 неудачных попыток ввода пароля. Следовательно, программе нужно будет трудиться очень долго. Если вы можете запомнить пароль из 10 символов, это еще лучше. Если же с памятью совсем плохо, то далее будут рассмотрены программы для автоматического ввода паро-

лей. Также существенно усложняет брутфорс наличие в пароле символов, отличных от алфавитно-цифровых, — например, символов пунктуации.

- ❑ В пароле должны присутствовать как буквы, так и цифры, причем регистр букв должен меняться. Желательно, чтобы цифры не повторялись. Вот пример пароля с изменяющимся регистром символов и цифрами: B<sup>r</sup>oaD178.
- ❑ Используйте не только алфавитно-цифровые символы. Самый обычный знак подчеркивания существенно усложняет пароль и увеличивает количество перестановок. Вот пример усложненного пароля: B\_<sup>r</sup>oaD178.
- ❑ С одной стороны, хорошо, когда пароль легко запомнить. Так меньше вероятность, что вы его забудете. С другой стороны, старайтесь, чтобы последовательность символов в пароле не являлась значащим словом — такие пароли быстро подбираются с помощью словаря. Наши пароли B<sup>r</sup>oaD178 и B\_<sup>r</sup>oaD178 не идеальны с точки зрения словарной атаки. Ведь оба пароля содержат значащие (словарные) слова: *broad* и *road*. Идеальная защита от словарной атаки — пароль, сгенерированный из случайных символов, например: sRkTnbs19g.

Однако такой пароль ничего не означает и не вызывает у человека никаких ассоциаций, поэтому сложен для запоминания. Чтобы защитить пароль и от словарной атаки, и от brute force, комбинируйте в пароле как словарные слова, так и случайные символы. Например: *road\_sjt\_91*. Такой пароль сложен для обоих способов подбора. Для brute force он достаточно длинный (11 символов) и к тому же содержит знак подчеркивания. И словарной атаке он тоже не по зубам — в словаре наверняка найдется слово *road*, но в нем вряд ли будет последовательность *sjt*.

- ❑ Некоторые пользователи вводят русские слова при включенной английской раскладке. Например, последовательность символов *ljhjuf* означает всего лишь слово «дорога». Но такие «перевернутые» словари уже давно есть у хакеров, так что этот метод уже не действует, и хотя сам пароль выглядит грозно, однако толку от него — 0.
- ❑ Не используйте в пароле ваши личные данные (номер паспорта, номер телефона, дату рождения), имена близких и родственников, домашних питомцев и т. п. Все это общедоступная информация, и если злоумышленник — кто-то из близкого вам окружения — он сможет подобрать пароль.
- ❑ Некоторые сервисы, например Mail.Ru, для восстановления пароля требуют ввести ответ на контрольный вопрос. Контрольные вопросы очень просты: номер паспорта, имя любимого питомца и т. п. Этим могут воспользоваться злоумышленники — ведь узнать номер вашего паспорта или имя питомца, думаю, можно, особенно если пароль пытаются подобрать люди, с которыми вы знакомы. Поэтому выберите любой контрольный вопрос, но в качестве ответа введите заранее подготовленный второй пароль.
- ❑ Опять-таки, для восстановления пароля может быть использован второй ваш e-mail. Но если к нему получит доступ злоумышленник (по причине простого пароля), он сможет легко взломать ваш основной почтовый ящик — почтовый сервер сам отправит новый пароль по указанному в настройках адресу...

Используйте эти рекомендации для создания сложного пароля. А если нужен действительно серьезный пароль, то лучше всего использовать генератор паролей, который будет рассмотрен далее.

Помните, что пароль следует периодически заменять. Конечно, каждый день его менять не стоит, иначе сами запутаетесь. Меняйте пароль, например, раз в три месяца. Но смените пароль сразу же, если была замечена попытка входа с другого IP-адреса. Некоторые сервисы, например тот же Mail.Ru, сообщают, с какого адреса был выполнен последний заход и когда именно. Если вы видите, что IP-адрес этого захода не ваш, значит, ваш почтовый ящик уже кто-то взломал. А то, что вы еще можете войти в него под своим паролем, означает, что злоумышленник не хочет, чтобы вы знали о том, что ящик взломан, — он просто хочет читать вашу почту и надеется, что вы не заметите попытки взлома. Сложнее, если вы и злоумышленник находитесь в сети одного провайдера, — тогда адреса, скорее всего, будут одинаковыми, — вы решите, что в прошлый раз вам просто был назначен другой адрес... Вот для этого и нужно периодически менять пароли — даже если вы не заметите, что ящик кто-то взломал, вы рано или поздно все равно поменяете пароль, и злоумышленнику придется начать его подбор сначала.

## 9.2.2. Генераторы паролей

Генераторы паролей используются для создания особо сложных и длинных паролей. Генераторов паролей — несчетное множество. Каждый школьник, обладая начальными навыками программирования, может создать программу, генерирующую случайную последовательность символов.

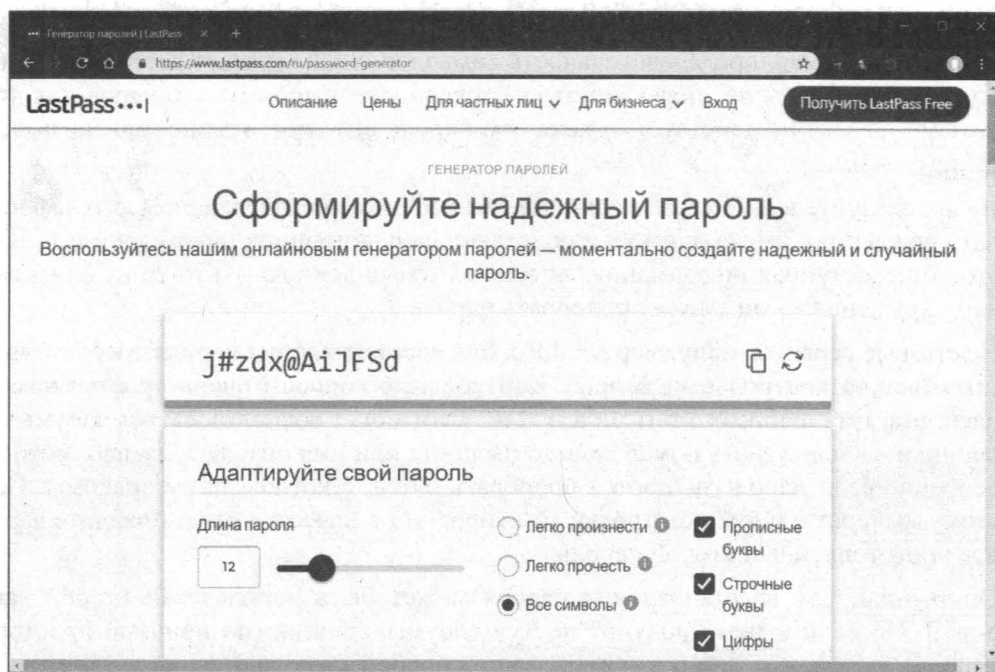




Рис. 9.1. Онлайн-генератор паролей LastPass

Все генераторы паролей работают одинаково. Вы устанавливаете параметры пароля (длину, тип используемых символов и т. п.) — и получаете один или несколько сгенерированных паролей.

Типичный пример онлайн-генератора паролей находится по адресу: <https://www.lastpass.com/ru/password-generator> (рис. 9.1). Вы задаете здесь параметры пароля: его длину, наличие прописных, строчных букв и цифр — и получаете готовый пароль. Рядом с паролем расположены две кнопки: первая  — копирует пароль в буфер обмена, а вторая  — генерирует следующий случайный пароль с такими же параметрами.

Вы можете использовать любой другой генератор, который легко найти в Интернете по запросу `password generator`, если предложенный генератор вам не понравился.

## 9.3. Как сохранить пароль?

### Менеджеры паролей

Сгенерировать сложный пароль, как было только что показано, очень просто. Со всем иным делом — его запомнить, что практически невозможно, если, конечно, у вас не феноменальная память на разную абракадабру.

Где же хранить пароль (точнее, пароли — ведь их у вас будет много)? Предлагаю несколько вариантов:

- ☐ на желтой липкой бумажке, приклеенной к монитору, — самое глупое решение (надеюсь, все понимают почему);
- ☐ в обычном текстовом файле — достаточно удобно, поскольку все пароли сразу под рукой. Но у этого способа один недостаток — файл виден невооруженным взглядом. Его может прочитать любой желающий — шпионская программа (если каким-то образом узнает, что у вас там пароли), ваши знакомые, коллеги и т. д.;
- ☐ в обычном текстовом файле, размещенном на зашифрованном носителе, — вот это самый практичный способ. Можно также зашифровать отдельный файл, а не весь носитель, если у вас кроме файла с паролями больше нет конфиденциальной информации. Правда, и у этого способа есть свой недостаток — если ключи доступа к носителю потеряются, вы навсегда потеряете свои пароли. Поэтому имеет смысл сделать копию файла паролей (например, на флешку) или распечатать его на бумаге и хранить в надежном месте (например, в сейфе);
- ☐ использование средств браузера — с одной стороны, весьма удобный способ. Но шпионские программы уже давно научились воровать сохраненные в браузере пароли<sup>1</sup>, да и в случае вынужденного сброса браузера вы их тоже потеряете. Поэтому я бы не рекомендовал прибегать к этому способу. Все-таки вероятность

---

<sup>1</sup> Вот примеры таких программ: `WebBrowserPassView` (вы без проблем найдете ее в Интернете) или `PasswordFox`, используемая для восстановления паролей, сохраненных в последних версиях браузера `Firefox`.

вынужденного сброса браузера выше, чем вероятность выхода из строя зашифрованного носителя;

- использование специальных программ. Существуют программы, предназначенные для хранения и автоматического ввода сложных паролей — менеджеры паролей. Этот способ хорош тем, что обеспечивает не только надежное хранение паролей, но и их автоматический ввод. Вам уже не придется вручную выделять строку символов (а ведь легко при этом не захватить один из символов, и пароль окажется неверным).

Так что давайте сейчас рассмотрим последний указанный способ хранения и ввода паролей подробнее. Надеюсь, что с желтыми бумажками, текстовым файлом и браузером вы сможете разобраться самостоятельно.

Существует много программ для хранения и автоматического ввода паролей. Одна из таких программ — KeePass Password Safe<sup>1</sup>, бесплатная утилита, имеющая к тому же portable-версию, что позволяет запускать ее с флешки. Обратите на это внимание — не устанавливать программу, а использовать ее portable-версию для хранения паролей на флешке гораздо рациональнее. Это исключит потерю паролей при переустановке системы, да и программа не будет привлекать лишнее внимание, если кто-то окажется за вашим компьютером.

Если вам не нравится это приложение, вы можете выбрать любое другое, благо в Интернете можно без проблем найти сравнение менеджеров паролей: как платных, так и бесплатных. Обзор некоторых других программ можно прочитать по адресу: <https://habr.com/ru/post/357192/>.

Все менеджеры паролей работают по одному принципу. Для доступа к базе паролей программы нужно изначально создать и ввести один мастер-пароль — постарайтесь, чтобы он был сложным. Попад в базу паролей, вы можете скопировать нужный пароль в буфер обмена и вставить его поле ввода пароля. Не забывайте только делать резервную копию базы данных с паролями (папки с portable-версией программы). Если флешка или другой накопитель выйдет со строя, вы потеряете все пароли.

На практике менеджеры паролей очень облегчают жизнь, особенно если у вас отдельный пароль к каждому ресурсу. Помнить 20–30 разных и сложных паролей просто невозможно.

Кроме программы KeePass, могу также порекомендовать программу Secure Data Manager<sup>2</sup>. Вот только для работы этой программы нужна виртуальная машина Java (JRE). Программа Secure Data Manager сама по себе весьма удобная, архив с ней занимает всего 2 Мбайт, а вот JRE... Нет смысла устанавливать JRE в свою систему, особенно если для других целей она вам не нужна, да и устанавливать JRE ради программы в 2 Мбайт — это как из пушки по воробьям...

---

<sup>1</sup> См. <https://keepass.info/download.html>.

<sup>2</sup> См. <http://sdm.sourceforge.net/>.



Но как бы там ни было, обе программы: и KeePass, и Secure Data Manager — являются программами с открытым кодом и распространяются по лицензии GPL, а это автоматически означает отсутствие «черных ходов», — вы можете быть уверены, что они не «сливают» на сторону ваши пароли. Исходный код этих программ доступен любому желающему, поэтому, если бы программы передавали пароли третьим лицам, это стало бы сразу ясно.

Однако помните, что раз исходный код программ доступен каждому желающему, скачивать программы можно только с их официальных сайтов, а не с разных «файлопомоек», где злоумышленники могут изменить код программы, откомпилировать ее и выложить в общий доступ. Если вы скачаете такую «модифицированную» программу, есть вероятность, что ваши пароли будут кому-то переданы, а этого не хотелось бы...

## 9.4. Секретные вопросы

Секретные вопросы помогают восстановить пароль в случае, если вы его забыли. В то же время они помогают злоумышленникам взломать ваш аккаунт. В начале этой главы уже был приведен пример неправильного применения секретного вопроса.

Относительно секретных вопросов есть несколько рекомендаций:

- ☐ если есть возможность отказаться от ввода секретного вопроса, откажитесь. Ведь вы используете менеджер паролей, и пароль вы не забудете. Поэтому и необходимости в секретном вопросе нет;
- ☐ если нельзя отказаться, тогда для разных сервисов используйте разные секретные вопросы;
- ☐ чтобы запомнить, где и какой секретный вопрос/ответ вы указывали, можно использовать те же менеджеры паролей. В описании пароля пишите Секретный ответ для <название сервиса>, в качестве самого пароля — ответ на секретный вопрос.

## 9.5. Двухфакторная аутентификация

Двухфакторная аутентификация подразумевает дополнительную проверку пользователя — действительно ли он тот, за кого себя выдает. Она позволяет сервисам убедиться, что вы — это вы, а вам — не потерять доступ к сервису.

В большинстве случаев работает двухфакторная аутентификация так: вы вводите логин и пароль к сервису. Если они правильные, то на ваш номер телефона поступает или голосовой звонок с инструкциями, или приходит код в SMS, который нужно ввести для подтверждения доступа к сервису или выполняемой операции.

В книге невозможно описать, как настроить двухфакторную аутентификацию ко всем в мире сервисам. Можно лишь напомнить это сделать. Прямо сейчас (если вы этого еще не сделали) позвоните в call-центр вашего банка и узнайте, как включить

двухфакторную аутентификацию для доступа к своему онлайн-банкингу. Также рекомендую понизить максимальную сумму онлайн-платежа. Да, это немного неудобно — для увеличения суммы (если нужно будет произвести оплату онлайн на большую сумму) придется увеличивать лимит, но так вы не потеряете все свои деньги, если кто-то узнает данные вашей карты (CCV/CVV-код, дату окончания, номер) и попытается произвести оплату онлайн.

Также настроить двухфакторную аутентификацию нужно для всех почтовых ящиков. Если у вас есть несколько телефонных номеров, используйте разные номера для каждого из ящиков. При использовании Gmail перейдите по ссылке: <https://myaccount.google.com/security-checkup>. Это средство проверки безопасности аккаунта, которое сообщит о возможных проблемах с аккаунтом и позволит настроить двухфакторную аутентификацию (рис. 9.2).

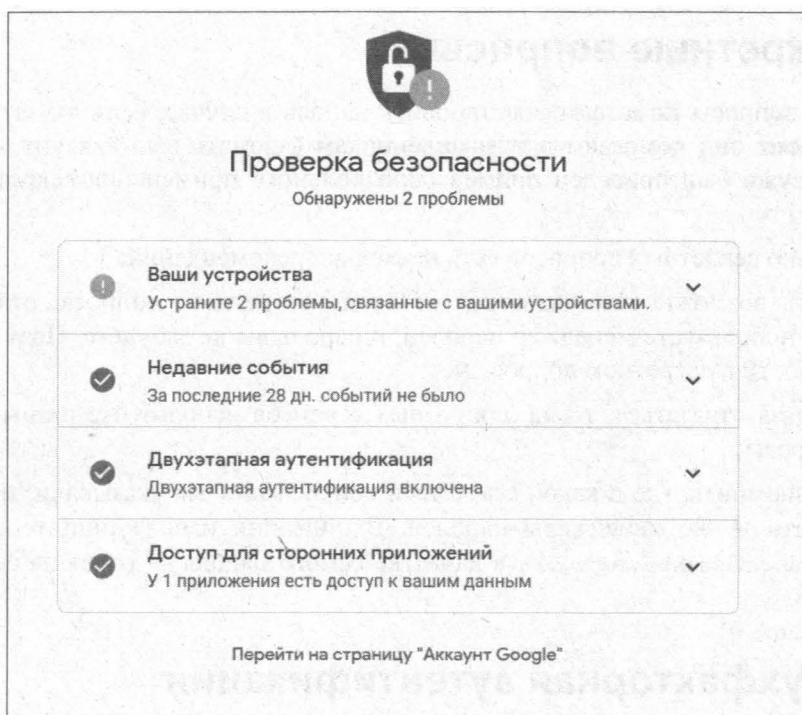


Рис. 9.2. Проверка безопасности Google-аккаунта

## 9.6. Авторизация с помощью биометрических данных

Бывают случаи, когда все идет насмарку, даже если вы настроили двухфакторную аутентификацию. Рассмотрим некую, впрочем, надуманную ситуацию. Представьте, что для Android-смартфона не настроен код разблокировки, а сама разблокировка устройства осуществляется свайпом в сторону. Тогда прочитав код от того же

банкинга сможет кто угодно, если в его руках окажется ваш смартфон. А такое вполне может произойти: забыли его в магазине, на столе на работе, в такси и т. п. Даже если вы и не лишитесь материальных ценностей, все равно кто угодно может просмотреть фотографии, прочитать переписку и пр. В общем, приятного мало.

Поэтому обязательно настраиваем код разблокировки устройства. Спешу вас, правда, огорчить. Такой код достаточно легко подобрать — как цифровой пароль, так и графический. Камера наблюдения, которых сейчас наставлено очень много, может запечатлеть момент, когда вы разблокируете свое устройство. Код также можно попытаться «прочитать» по отпечаткам пальцев, оставленных на экране смартфона.

Именно поэтому рекомендуется для разблокировки использовать биометрические данные. Самый простой пример таких данных — отпечаток пальца. Сканером отпечатка пальца оснащены сейчас даже недорогие устройства. Кроме отпечатков пальцев, на более «серьезных» смартфонах часто используются средства визуального распознавания пользователя — вроде FaceID на iPhone. К сожалению, на недорогих Android-устройствах такие средства все еще не очень хорошо работают, и распознавание может состояться даже по фотографии пользователя, поэтому предпочтительнее все-таки использовать именно отпечатки пальцев. На iPhone X/XR/XS сканер отпечатков пальца не предусмотрен, а разблокировка устройства осуществляется или по мастер-коду, или по FaceID. Благо FaceID работает корректно на этих устройствах.

Для установки кода разблокировки на Android-устройстве перейдите в **Настройки**, затем в **Экран блокировки и защита** и выберите **Тип блокировки**. На появившемся экране выберите способ разблокировки: рисунок, PIN-код или пароль. Самая высокая безопасность у пароля, но вводить пароль для разблокировки устройства — неудобно, и эта затея быстро вам надоест. Графический пароль (рисунок) и PIN-код обеспечивают примерно одинаковую безопасность, поэтому выбирайте тот, который удобнее вам (рис. 9.3).

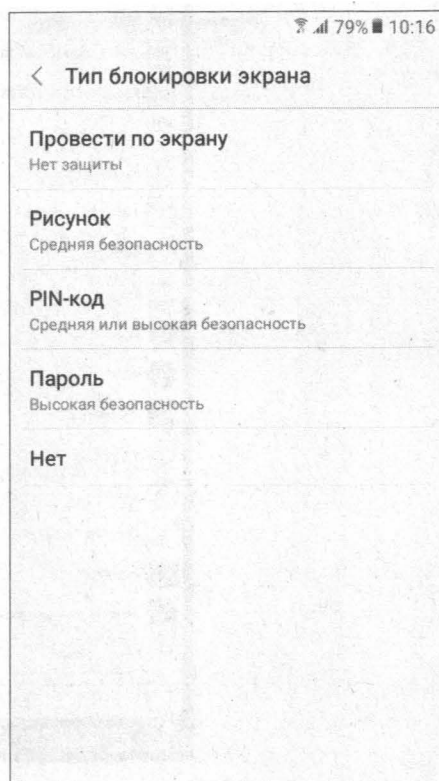


Рис. 9.3. Выбор типа разблокировки экрана на Android-устройстве

## 9.7. Заметаем следы правильно

Иногда приходится работать не за своим компьютером, а, например, за компьютером родственника или каждый день — за рабочим (офисным) компьютером. Далеко не всегда нужно, чтобы кто-то (у кого тоже есть доступ к этому компьютеру) видел какие сайты вы посещали, с какими документами работали и т. п. И в этом разделе мы рассмотрим, как «замести следы» — скрыть результаты своей деятельности за компьютером. Этот материал будет также полезен, если вы хотите подарить свой компьютер друзьям или родственникам. Конечно, в идеале надо бы переустановить систему, но если не хочется тратить на это время, то сойдет и такая чистка.

### 9.7.1. Очистка списков недавних мест и программ

Обе операционки: и «семерка», и «десятка» — предательски следят за вами и готовы по первому требованию предоставить на сторону всю необходимую информацию. Мы же сейчас разберемся, как эту информацию вычистить. И начнем со списков недавних мест и программ. Список недавних (в «десятке» — часто используемых) программ хранится в главном меню (рис. 9.4), а список недавних мест — в Проводнике (рис. 9.5).



Рис. 9.4. (Часть 1 из 2) Список часто используемых программ в Windows 7 (а)



6

Рис. 9.4. (Часть 2 из 2) Список часто используемых программ в Windows 10 (б)

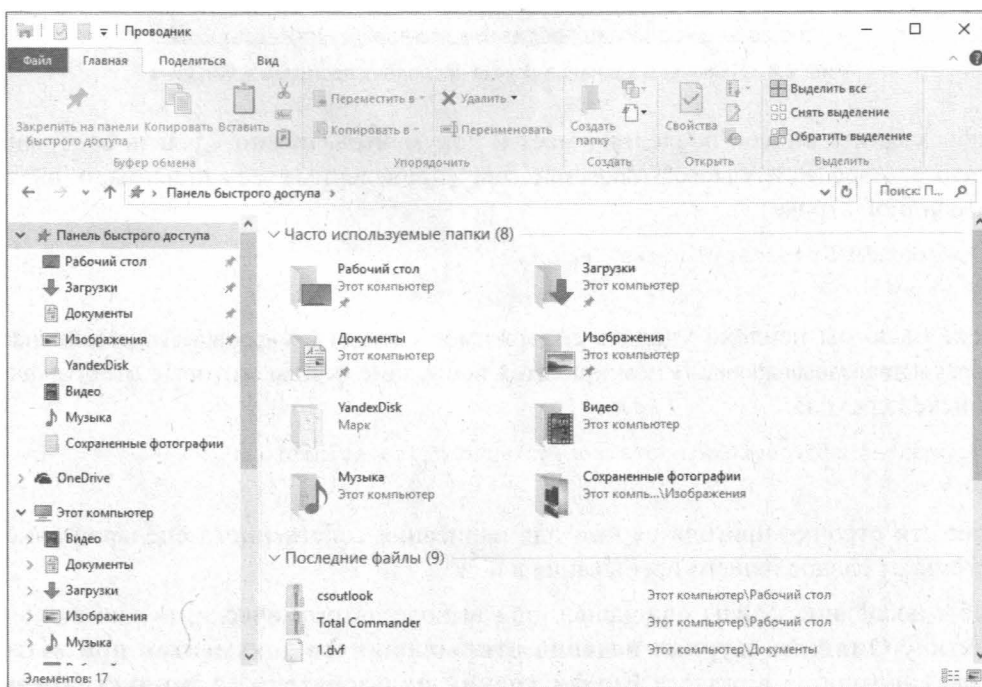


Рис. 9.5. Список часто используемых папок и последних файлов



Теперь переходим к «десятке». Отключить список недавно добавленных и часто используемых приложений можно через окно **Параметры**. Откройте его и перейдите в раздел **Персонализация** | **Пуск**. Отключите все, что там есть (рис. 9.7).

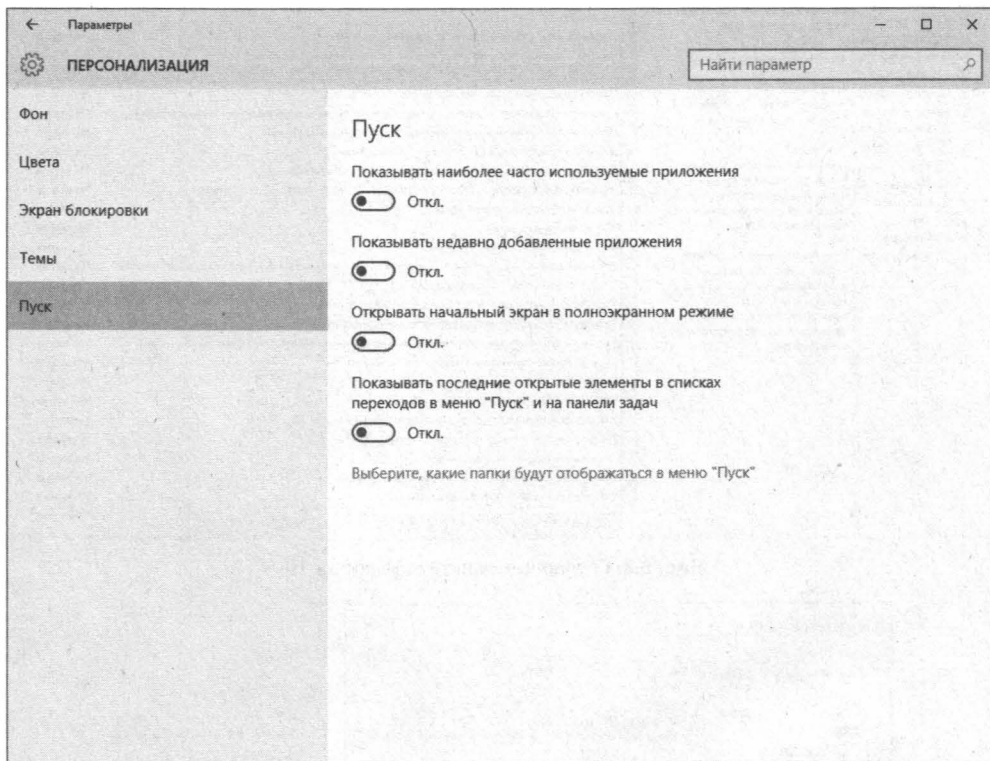


Рис. 9.7. Отключение хранения списка программ в Windows 10

Однако кардинально это проблему не решит, поскольку, если включить эти параметры снова, наши списки в таком же составе вновь появятся. Поэтому придется отключать эту «фишку» через групповые политики (рис. 9.8). Откройте файл `gpedit.msc` и перейдите в раздел **Конфигурация пользователя** | **Административные шаблоны** | **Меню «Пуск»** и панель задач. Включите политики:

- ☐ Очистка списка недавно использовавшихся программ для новых пользователей;
- ☐ Очистить журнал недавно открывавшихся документов при выходе;
- ☐ Очистить журнал уведомлений на плитке при выходе;
- ☐ Удалить список программ, закрепленных в меню «Пуск».

Очистить недавние места в «десятке» проще. Откройте Проводник, перейдите на вкладку **Вид**, нажмите кнопку **Параметры**. В открывшемся окне отключите параметры **Показывать недавно использовавшиеся файлы на панели быстрого доступа** и **Показывать часто используемые папки на панели быстрого доступа**. Нажмите также кнопку **Очистить** и кнопку **ОК** (рис. 9.9).



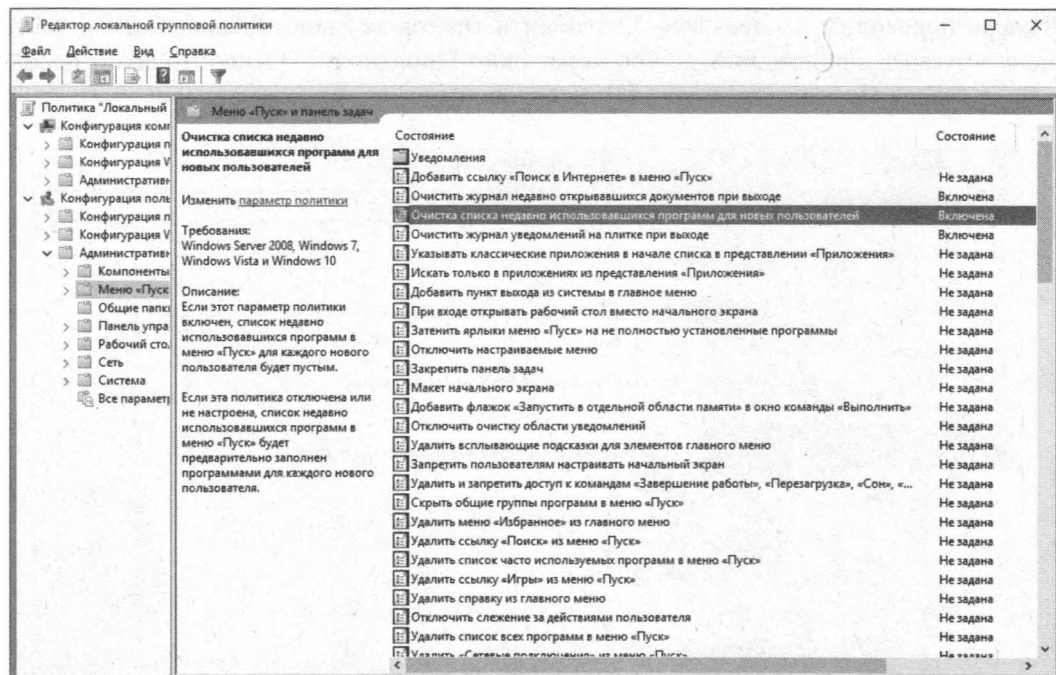


Рис. 9.8. Групповые политики Windows 10

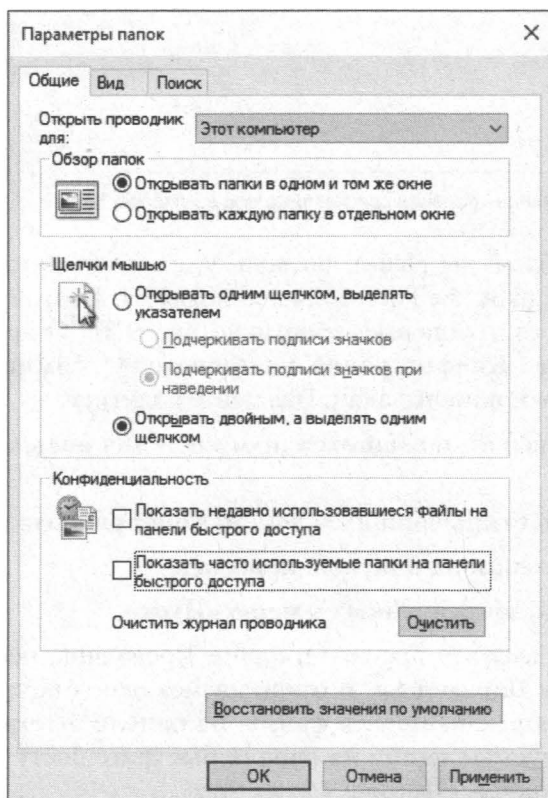


Рис. 9.9. Параметры папок Windows 10

Как видите, даже у такой простой задачи, как очистка последних объектов, весьма непростое решение — ведь приходится применять редактирование групповых политик.

### 9.7.2. Очистка списка USB-накопителей

На некоторых режимных объектах к компьютеру разрешено подключать только накопители (флешки), зарегистрированные в журнале. Причем, как водится, журнал самый что ни на есть обычный — бумажный. При этом сам компьютер никак не ограничивает подключение незарегистрированных накопителей. Не ограничивает, зато протоколирует. Если при проверке обнаружат, что пользователь подключал незарегистрированные накопители, у него будут проблемы. Разберемся, как помочь пользователю.

Загляните в разделы реестра:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\  
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\
```

Вот они — все накопители, которые вы подключали к своему компьютеру (рис. 9.10).

Казалось бы, нужно просто все здесь вычистить. Но не так все просто. Во-первых, разрешения на эти ветки реестра установлены таким образом, что вы ничего не удалите даже в Windows 7 (рис. 9.11), не говоря уже о «десятке».

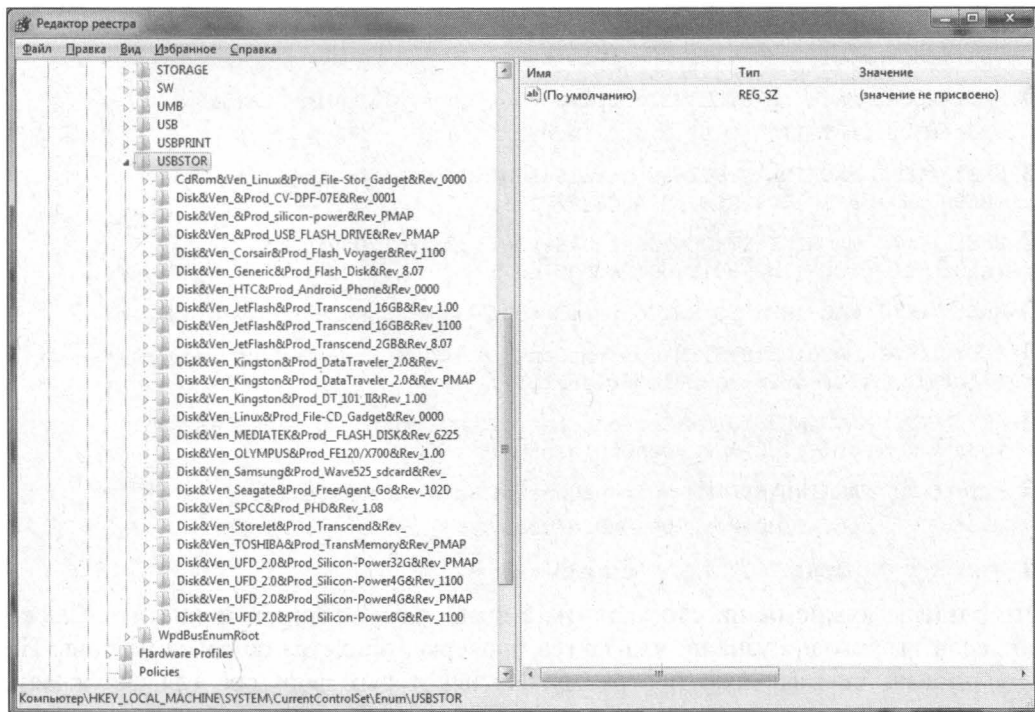


Рис. 9.10. Раздел реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR`

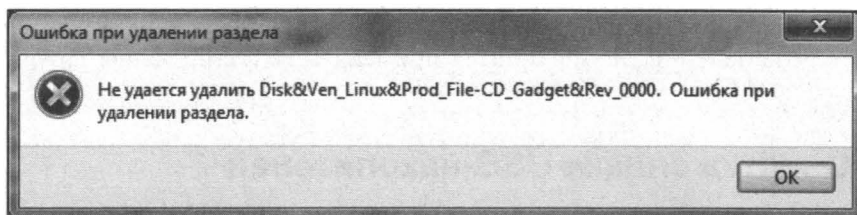


Рис. 9.11. Упс...

Во-вторых, назначать права и разрешения вручную достаточно долго, особенно если накопителей много. В-третьих, права админа не помогут (рис. 9.11 был создан, когда я выполнял операцию удаления как раз с правами админа). В-четвертых, кроме этих двух разделов нужно почистить еще и следующие:

- ☐ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume;
- ☐ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Class\{36FC9E60-C465-11CF-8056-444553540000};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{53f5630d-b6bf-11d0-94f2-00a0c91efb8b};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{56907941-3AFE-11D4-AE2C-00A0CC242D2C};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\STORAGE\RemovableMedia;
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{3abf6f2d-71c4-462a-8a92-1e6861e6af27};
- ☐ KEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b};
- ☐ KEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{53f5630a-b6bf-11d0-94f2-00a0c91efb8b};
- ☐ HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices.

Эти разделы нужно не просто удалить, а правильным образом почистить. Скажем так, если вы сегодня узнали, что завтра проверка, придется остаться на ночь. Или использовать специальную программу. На некоторых форумах, где обсуждается этот вопрос, рекомендуют программу USBDeview. Однако я ее протестировал и заявляю, что она вычищает информацию далеко не из всех разделов, — после ее

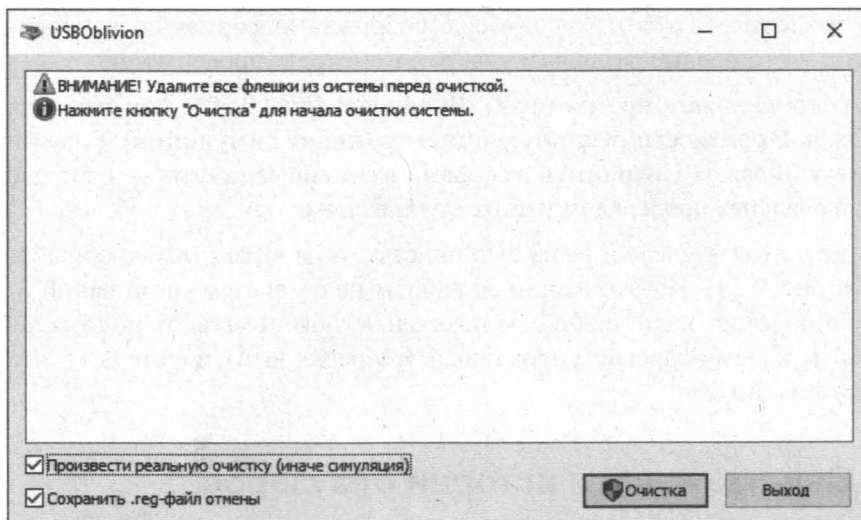


Рис. 9.12. Программа USBObivion

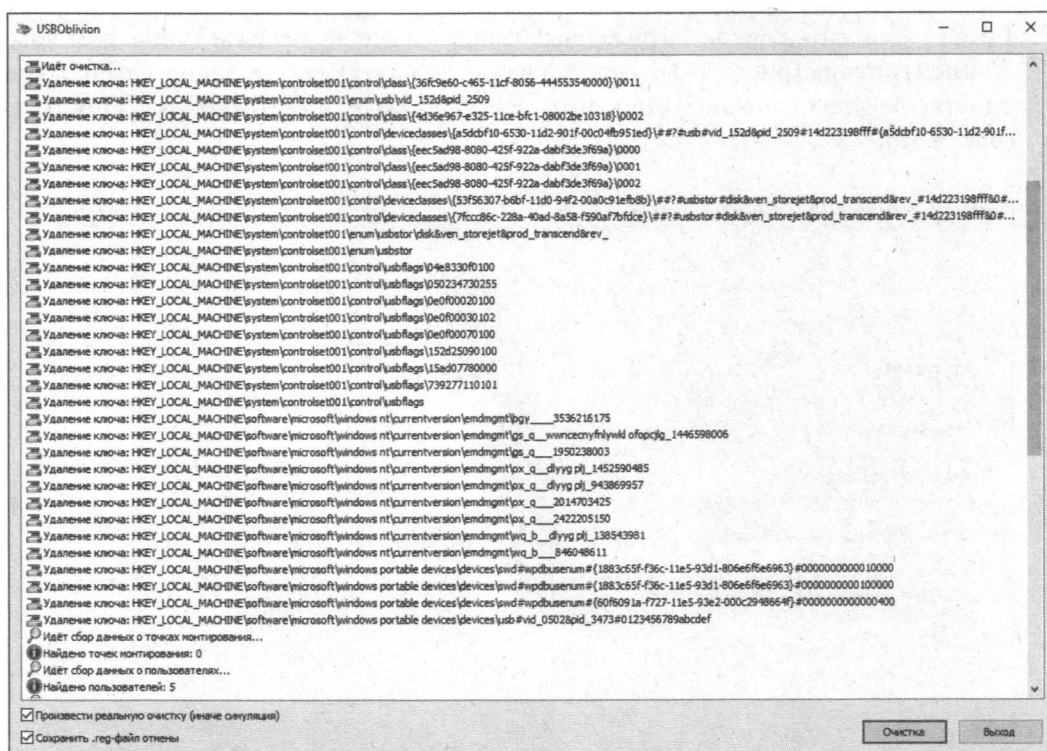


Рис. 9.13. Программа USBObivion в действии

прогона разделы USBSTOR и USB все еще содержат информацию о подключаемых носителях. А это первые разделы, куда будут смотреть проверяющие.

Могу порекомендовать программу USBObivion<sup>1</sup> (рис. 9.12). Запустите ее, установите флажок **Произвести реальную очистку (иначе симуляция)** и нажмите кнопку **Очистка**. Флажок **Сохранить .reg-файл отмены**, если цель — не проверка программы, а реальная проверка на работе, лучше снять.

Программа не только делает реальную очистку, но и выводит подробный лог своих действий (рис. 9.13). По окончании ее работы не останется упоминаний о подключении к компьютеру каких-либо накопителей. Чтобы не вызвать подозрений, лучше подключить к нему зарегистрированный (разрешенный) носитель — чтобы хоть один носитель, но был.

### 9.7.3. Очистка кэша и истории браузеров

Третий пункт в нашем наборе рекомендаций по заметанию следов — очистка кэша и журнала браузеров. Хорошо, если вы используете один браузер, если же нет, то придется чистить все:

- ❑ Edge — очистить список загруженных файлов и все журналы можно с помощью **Концентратора** (рис. 9.14) — просто нажмите на соответствующие ссылки. При очистке журнала нужно установить все флажки и нажать кнопку **Очистить** (рис. 9.15);

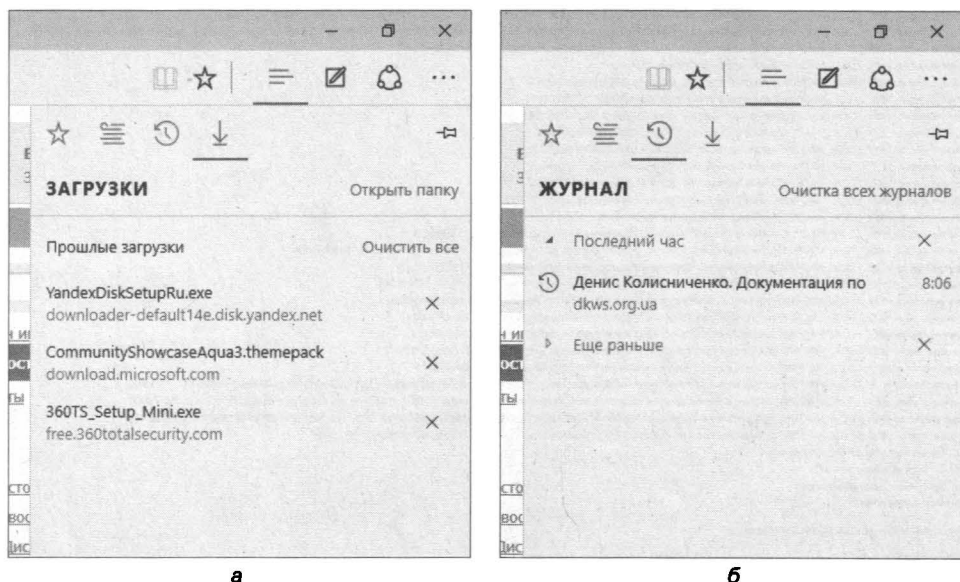


Рис. 9.14. Концентратор браузера Edge: а — раздел Загрузки; б — раздел Журнал

<sup>1</sup> См. <http://www.cherubicsoft.com/en/projects/usboblivion>.

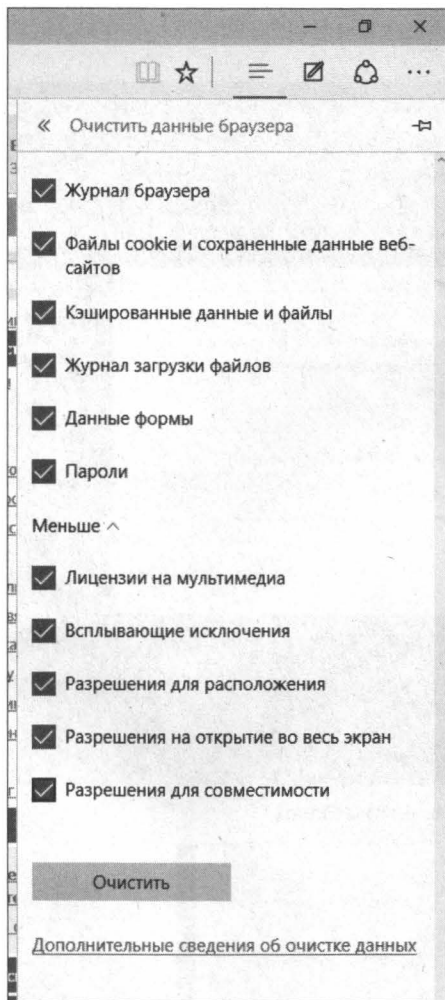


Рис. 9.15. Генеральная уборка в Edge

- ❑ Firefox — откройте настройки, перейдите в раздел **Приватность и защита** (рис. 9.16), нажмите кнопку **Удалить данные**, отметьте все и нажмите кнопку **Удалить**;
- ❑ Chrome, Opera — нажмите комбинацию клавиш <Ctrl>+<Shift>+<Del>, на появившейся странице выберите очистку за все время, установите все флажки и нажмите кнопку **Удалить данные** (рис. 9.17);
- ❑ IE — его еще кто-то использует? Рекомендации можно найти на сайте Microsoft.

В результате вы не только сотрете следы, но и сэкономите место на диске. А чтобы на рабочем компьютере не приходилось чистить журналы браузера, все личные сайты нужно посещать в режиме инкогнито. Конечно, администратор при желании увидит журнал на шлюзе, но на вашем компьютере все будет чисто. Оптимальное решение — использовать Тог. В этом случае даже администратор не увидит, какие сайты вы посещаете (при условии, что за вашей спиной нет камеры наблюдения).

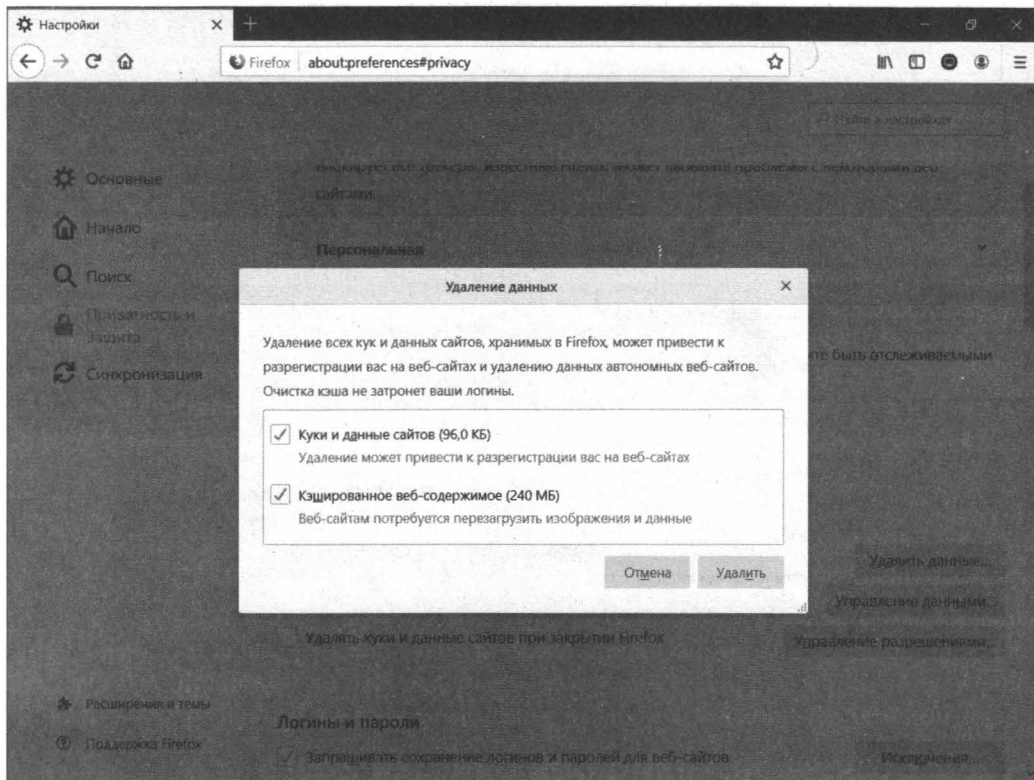


Рис. 9.16. Чистим Firefox

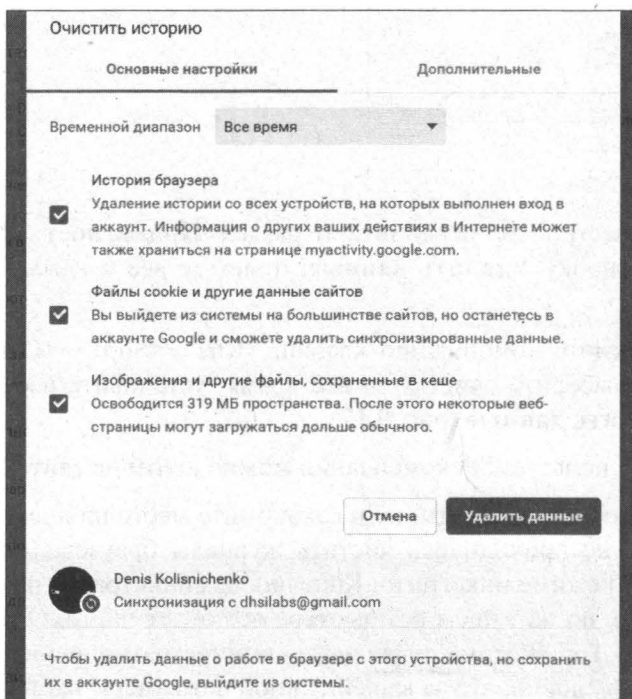


Рис. 9.17. Очистка Chrome



### 9.7.4. Удаляем записи DNS

Узнать, какие сайты вы посещали, можно не только из журнала браузера, но еще и из кэша DNS<sup>1</sup>. Когда вы вводите адрес сайта в браузере, то ваш компьютер обращается к DNS, чтобы разрешить (перевести) имя сайта в IP-адрес. Кэш разрешенных ранее имен хранится на вашем компьютере. Просмотреть его можно командой:

```
ipconfig /displaydns
```

Вывод этой команды я приводить здесь не буду — он слишком длинный. Вам только надо знать, что для очистки этого кэша используется другая команда:

```
ipconfig /flushdns
```

### 9.7.5. Очистка Flash Cookies

За вами следят все, кому не лень. Даже flash-плеер и тот отслеживает ваши посещения. Flash Cookies собираются в каталоге %appdata%\Macromedia\Flash Player\#SharedObjects. Что с ним сделать, думаю, понятно:

```
cd %appdata%\Macromedia\Flash Player\#SharedObjects  
echo y | del *.*
```

Вообще команду del можно вводить и с одной звездочкой (del \*), но с двумя (del \*.\* ) мне как-то больше нравится.

### 9.7.6. Удаление списка последних документов MS Office

Для удобства пользователей список последних документов хранят все программы офисного пакета. Чтобы избавиться от этой помощи, в новых версиях Office перейдите в параметрах в раздел Дополнительно (рис. 9.18) и в полях Число документов в списке последних файлов и Число последних документов для быстрого доступа установите 1. Значение 0 программа установить не позволяет, поэтому устанавливаем 1, а затем открываем какой-то безобидный файл.

В старых версиях Office на вкладке Общие окна параметров можно или также установить значение 1, или вообще снять флажок помнить список из ... файлов (рис. 9.19).

---

<sup>1</sup> DNS (англ. Domain Name System, система доменных имен) — компьютерная распределенная система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства).

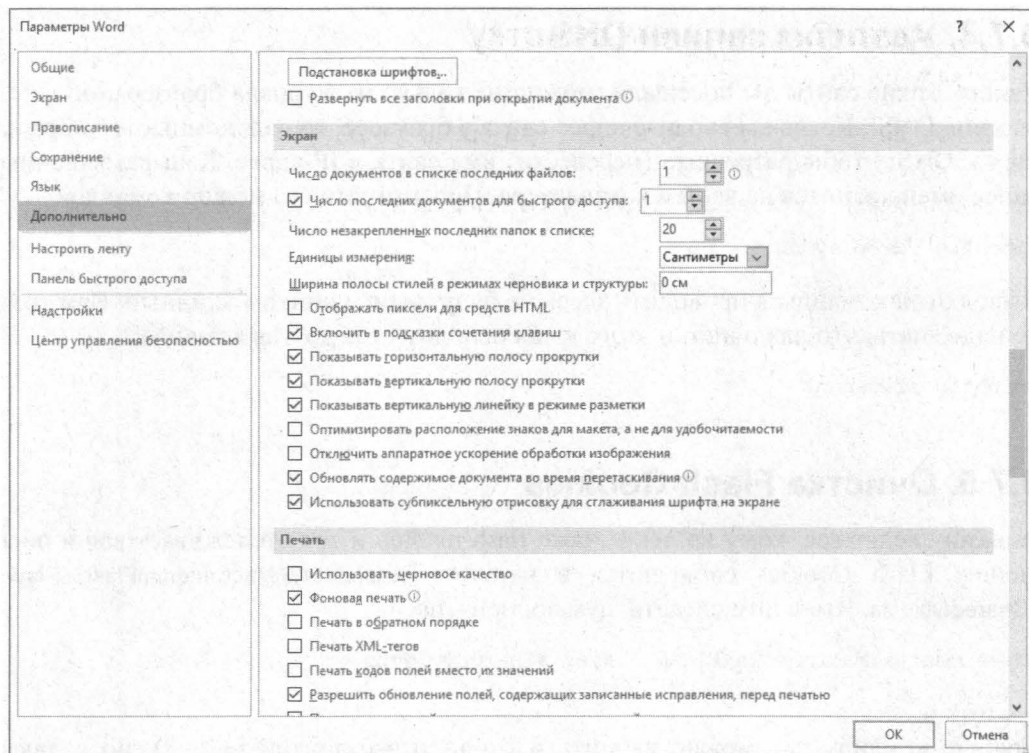


Рис. 9.18. Параметры MS Word 2016: раздел Дополнительно

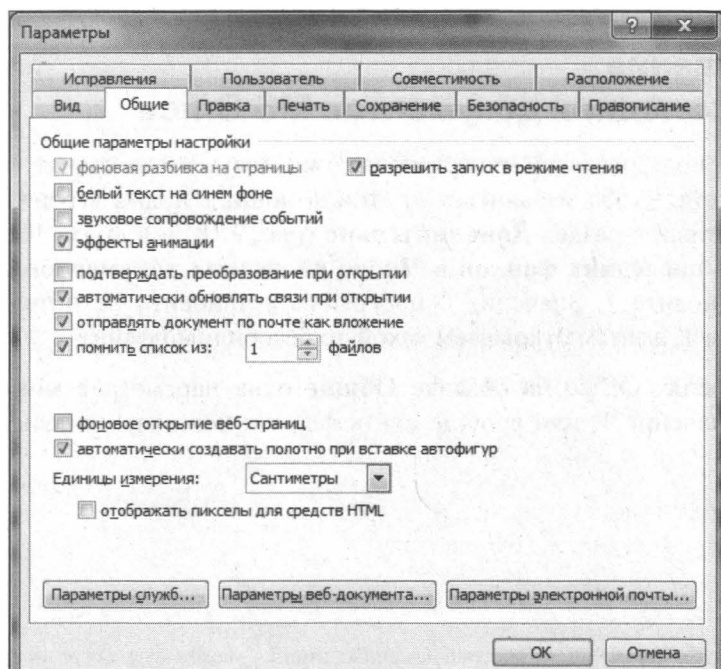


Рис. 9.19. Параметры MS Word 2003: вкладка Общие

## 9.7.7. Автоматизируем очистку с помощью CCleaner

Обратите внимание, что нам нужна программа CCleaner Desktop, а не CCleaner Cloud, которая платная — ее функционал значительно шире, чем нам нужно. Так что переходим по адресу: <https://www.ccleaner.com/ru-ru/ccleaner> и выбираем бесплатную версию.

Чем мне нравится CCleaner, так это тем, что она:

- ❑ поддерживает последние версии Windows и последние версии браузеров, в том числе Edge (рис. 9.20), — в отличие от почти аналогичной Free History Eraser;

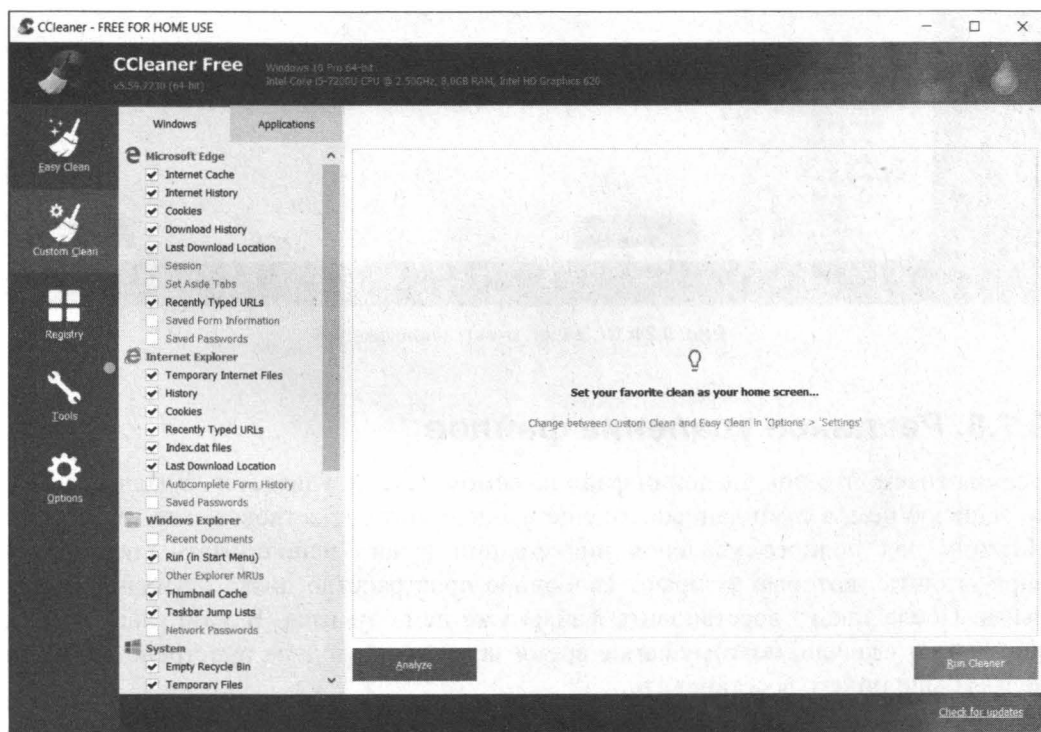


Рис. 9.20. CCleaner: очистка системы

- ❑ может очистить не только систему, но и приложения (рис. 9.21);
- ❑ может работать в bat-режиме, и дальше будет показано, как вызывать процесс «уборки» из командного файла.

Использовать ее просто — выберите те элементы, которые нужно очистить, и нажмите кнопку **Run Cleaner**.

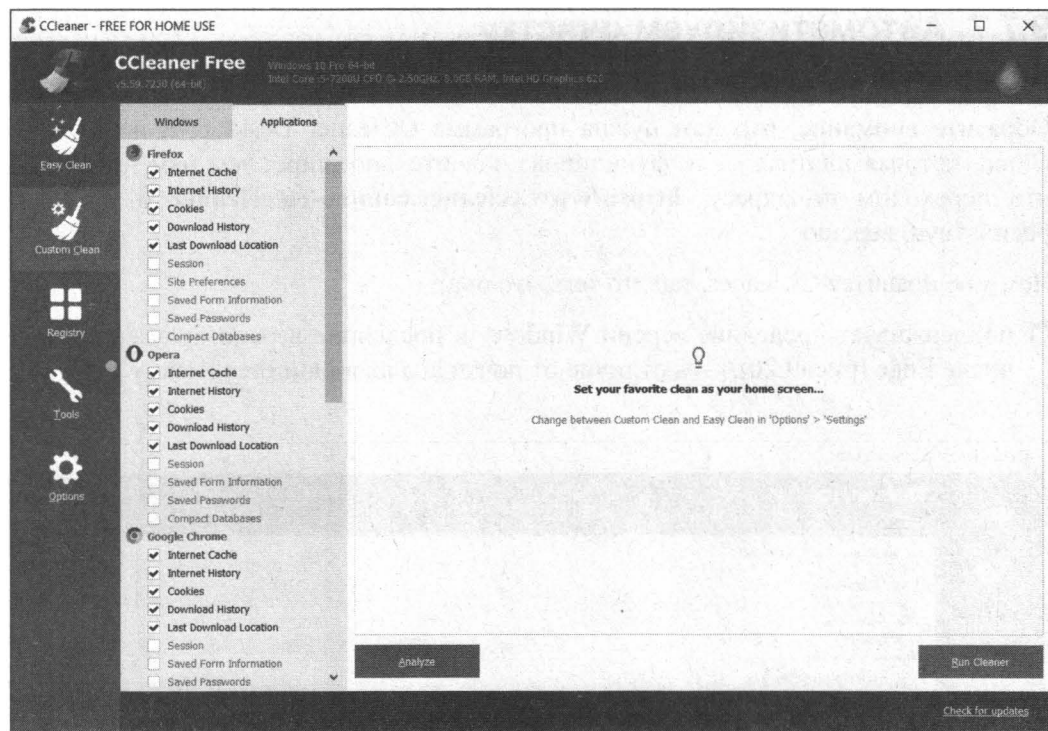


Рис. 9.21. CCleaner: очистка приложений

### 9.7.8. Реальное удаление файлов

Все мы знаем, что при удалении файл на самом деле не удаляется. Удаляется только запись о нем, а сами данные все еще продолжают существовать где-то на диске. Поэтому для полного удаления информации нужно использовать специальные *wipe*-утилиты, которые затирают свободное пространство диска случайными данными. После такого восстановить файлы уже не получится. В этой главе мы уже много чего удаляли, поэтому самое время затереть свободное пространство, чтобы нельзя было ничего восстановить.

Существует много утилит для затирания информации. Но мы воспользуемся той, что уже у нас есть, а именно программой CCleaner. Зайдите в меню **Tools | Drive Wiper**, выберите диск, который хотите стереть, укажите, что стирать: **Free Space Only** (Только свободное место) и способ стирания (рис. 9.21). Приложение поддерживает несколько стандартов стирания: от самого простого, подразумевающего одну перезапись, до метода Гутманна (35 проходов).

CCleaner — далеко не единственная программа такого рода. Есть много подобных программ. Например, BCWipe, с функциями которой можно ознакомиться по адресу <http://www.jetico.com/wiping/61-accordion-ru-2/558-acc-ru-2-2>. Она способна не только стирать свободное пространство, но и выполнять в том числе стирание файла подкачки, который также может содержать конфиденциальную информацию. Ее

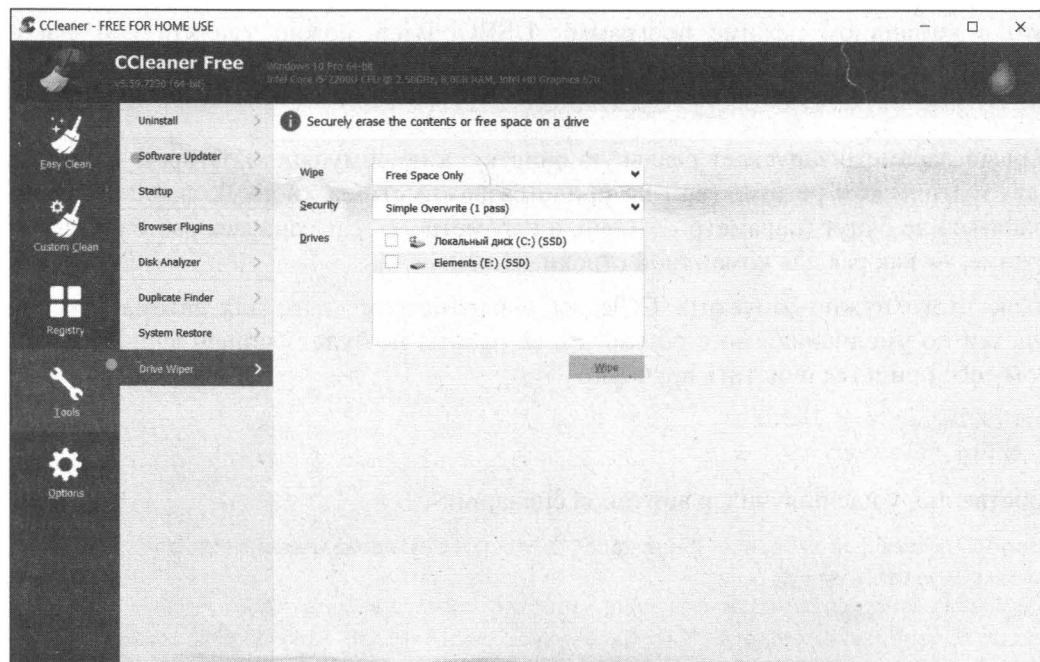


Рис. 9.22. Стирание свободного места

недостаток в том, что она платная, но для одноразового стирания (например, перед проверкой) подойдет и бесплатная trial-версия.

Подробнее об удалении данных на разных носителях мы поговорим в *главе 11*.

### 9.7.9. Создаем bat-файл для очистки всего

Теперь попытаемся автоматизировать некоторые рассмотренные ранее операции. Начнем с удаления файлов из каталога Recent. Удалять их командой `del`, как было показано ранее, — можно, но лучше сразу использовать CCleaner для безопасного удаления:

```
\путь\CCleaner.exe /delete "%appdata%\Microsoft\Windows\Recent\*" 1
\путь\CCleaner.exe /delete
"%appdata%\microsoft\windows\recent\automaticdestinations\*" 1
\путь\CCleaner.exe /delete "%appdata%\Macromedia\Flash Player\#SharedObjects" 1
```

К сожалению, CCleaner нельзя вызвать так, чтобы она почистила в режиме командной строки все свободное пространство, поэтому придется удалять файлы через нее, а не командой `del`, или же использовать команду `del`, а потом вручную запустить CCleaner и вызвать очистку свободного пространства. Последний параметр (1) означает удаление с тремя проходами. Это оптимальный режим, поскольку с одним проходом (0) — слишком просто, а все остальные — слишком долго<sup>1</sup>.

<sup>1</sup> С параметрами командной строки CCleaner можно ознакомиться по адресу: <http://myccleaner.net/ccleaner-ndash-parametryi-komandnoy-stroki/>.

Зато в командном режиме программы USBOblivion можно удалить USB-накопители:

```
\путь\USBOblivion.exe -enable -auto -nosave -silent
```

Первый параметр запускает реальную очистку, а не симуляцию. Второй — работу в автоматическом режиме (вам не придется нажимать на кнопку), файлы \*.reg сохраняться не будут (параметр -nosave), а параметр -silent означает работу в тихом режиме, — как раз для командной строки.

После этого нужно запустить CCleaner с параметром /AUTO для автоматической очистки по умолчанию, но в результате ее работы не будет очищен кэш DNS, поэтому его придется очистить вручную:

```
путь\CCleaner.exe /AUTO  
ipconfig /flushdns
```

Собственно, у нас получился вот такой сценарий:

```
\путь\CCleaner.exe /delete "%appdata%\Microsoft\Windows\Recent\*" 1  
\путь\CCleaner.exe /delete  
"%appdata%\microsoft\windows\recent\automaticdestinations\*" 1  
\путь\CCleaner.exe /delete "%appdata%\Macromedia\Flash Player\#SharedObjects" 1  
\путь\USBOblivion.exe -enable -auto -nosave -silent  
путь\CCleaner.exe /AUTO  
ipconfig /flushdns
```

## 9.7.10. Создаем AutoHotkey-скрипт для очистки всего

Теперь напишем немного другой сценарий. Он будет запускать браузер Chrome в режиме инкогнито, а по завершении вашей сессии в Chrome (задана функция WinWaitClose, которая ждет закрытия окна) мы запустим CCleaner для автоматической очистки браузера (удаления кэша браузера и временных файлов), а после этого очистим кэш DNS:

```
Run, C:\path\to\chrome.exe -incognito  
WinWait, - Google Chrome  
WinWaitClose  
Run, C:\путь\ccleaner.exe /AUTO  
Run, cmd /c "ipconfig /flushdns"  
MsgBox, Browsing Session is Cleaned.
```

Для запуска этого сценария вам понадобится программа AutoHotKey<sup>1</sup>, которая позволяет выполнять действия нажатием клавиши или комбинацией клавиш, а также выполнить несколько действий нажатием одной клавиши.

---

<sup>1</sup> См. <https://autohotkey.com/>.

## ГЛАВА 10



# Мой дом — моя крепость: безопасность домашних устройств

## 10.1. Стоит ли защищать домашнюю сеть?

В последнее время весьма популярными стали беспроводные домашние сети на основе Wi-Fi. Такие сети создаются, даже если дома всего один компьютер. Ведь стоит беспроводной маршрутизатор недорого, а комфорта — масса. Имея ноутбук, вы можете, оставаясь в сети, свободно перемещаться по всей квартире. А если у вас только стационарный компьютер, наличие беспроводного маршрутизатора позволяет не тянуть через всю квартиру портящий интерьер Ethernet-кабель. Достаточно на входе в квартиру установить беспроводной маршрутизатор — кабеля минимум, порчи интерьеру — тоже. Это уже не говоря о простоте подключения к Интернету и вообще к домашней сети различных современных устройств: коммуникаторов, планшетов, мобильных телефонов (поддержка Wi-Fi есть даже в относительно недорогих моделях), игровых приставок, сетевых хранилищ данных и пр.

Современные беспроводные маршрутизаторы практически не требуют настройки — программа первоначальной настройки просит разве что выбрать способ подключения к Интернету и указать имя пользователя и пароль (и то не всегда — все зависит от способа подключения ко Всемирной сети). Да и пароль на вход в панель управления самого маршрутизатора по умолчанию не сложнее пароля новых SIM-карт. Так, на моем маршрутизаторе по умолчанию был установлен «ультрасложный» пароль 1234.

Все это сделано для облегчения настройки устройства — чтобы пользователь, обладающий начальными знаниями, мог настроить маршрутизатор без привлечения посторонних специалистов. Как обычно и бывает — комфорт в ущерб безопасности. Ведь некоторые настройки могут блокировать доступ, а этого нельзя сделать — нужно «чтоб сразу работало».

Вот и получается, что ваша домашняя сеть, настроенная утилитой быстрой настройки, доступна не только вам, но и всем желающим в радиусе действия сети, который составляет в наших условиях (бетонные стены, разные электронные устройства: радиотелефоны, микроволновки и т. п.) от 30 до 50 метров. Вы только представьте — 30 метров вокруг маршрутизатора! Сюда войдут ближайшие квар-



тиры по лестничной клетке, не нужно также забывать про квартиры этажом ниже и выше. При желании все ваши соседи смогут пользоваться Интернетом за ваш счет.

У многих сейчас так называемые *безлимитные пакеты* — трафик, как и время работы, не учитывается, а раз в месяц за доступ к Интернету взимается фиксированная сумма. Так стоит ли защищать свою домашнюю сеть, учитывая, что никаких финансовых потерь вы не понесете? — все равно, сколько трафика будет передано, абонентская плата от него не зависит. Не спешите отвечать сразу. Ответ должен быть взвешенный. Отбросьте в сторону амбиции — они ни при чем в этом случае.

Давайте прежде подумаем — что будет, если кто-то проникнет в вашу сеть? В самом безобидном случае он просто станет пользоваться Интернетом и общими ресурсами сети — например, общими дисками с фильмами, которые вы коллекционируете. В домашних (и не только) сетях часто такое практикуется — все фильмы помещаются на один компьютер с самым большим жестким диском, а на остальные компьютеры они копируются по мере необходимости. Также частенько используют NAS<sup>1</sup> или просто подключают внешний жесткий диск к маршрутизатору, если он такое поддерживает.

Даже если незваный гость не окажется вандалом, а попросту будет «на шару» использовать ваше интернет-соединение — приятного мало. Ведь в вашей сети появится еще один клиент, что снизит общую скорость доступа к Интернету — придется делить канал с еще одним пользователем. А если «гостю» будет мало ваших фильмов и он начнет качать свои (на вкус и цвет... — сами понимаете), то снижение производительности всей сети и снижение скорости доступа к Интернету вам гарантировано.

Но снижение скорости — еще полбеды. Если этот «гость» окажется хакером и взломает из вашей сети чей-то компьютер (например, банковский) или еще как-то напакостит, то придут к вам — ведь засветится именно ваш IP-адрес. А беспроводные маршрутизаторы, как правило, не ведут журналов доступа, поэтому доказать вы ничего не сможете. И даже если доступ к чужим кредиткам «гость» получать не будет, а просто, скажем, станет рассылать спам, то в черный список опять-таки попадет ваш IP-адрес. В конечном итоге вы не сможете отправлять письма... Попробуйте потом доказать, что ничего такого не рассылали.

Есть и еще один нюанс проникновения в вашу сеть: перехват личных данных, вандализм и кража конфиденциальной информации. Например, технически подготовленному «соседу» ничего не стоит заполучить ваш пароль к странице в социальной сети, к почтовому ящику. Он также сможет просмотреть фотографии и другие документы, доступные компьютерам вашей сети (поскольку является полноценным клиентом). А некоторая категория «доброжелателей» специально проникает в чужие сети с одной целью — что-нибудь уничтожить или инфицировать компьютеры сети вирусом. Вандалы! Видимо, этим они пытаются прикрыть комплекс неполноценности. Но не будем углубляться в психологию, пусть это делают специалисты, а наша задача несколько иная.

---

<sup>1</sup> NAS (англ. Network Attached Storage) — сервер для хранения данных на файловом уровне.

Мы получили ответ на поставленный вопрос — однозначно, нужно защищать свою домашнюю сеть. А защитить ее можно только путем соответствующей настройки вашего маршрутизатора.

#### **ПРИМЕЧАНИЕ**

Далее будут приведены общие советы по такой настройке, а конкретно настройку мы рассмотрим на примере моего домашнего маршрутизатора TP-Link TL-WR820N (N300) — неплохой вариант для построения домашней сети для нетребовательных пользователей. Однако, изучив руководство по эксплуатации своего маршрутизатора, вы без проблем найдете аналогичные параметры в его панели управления.

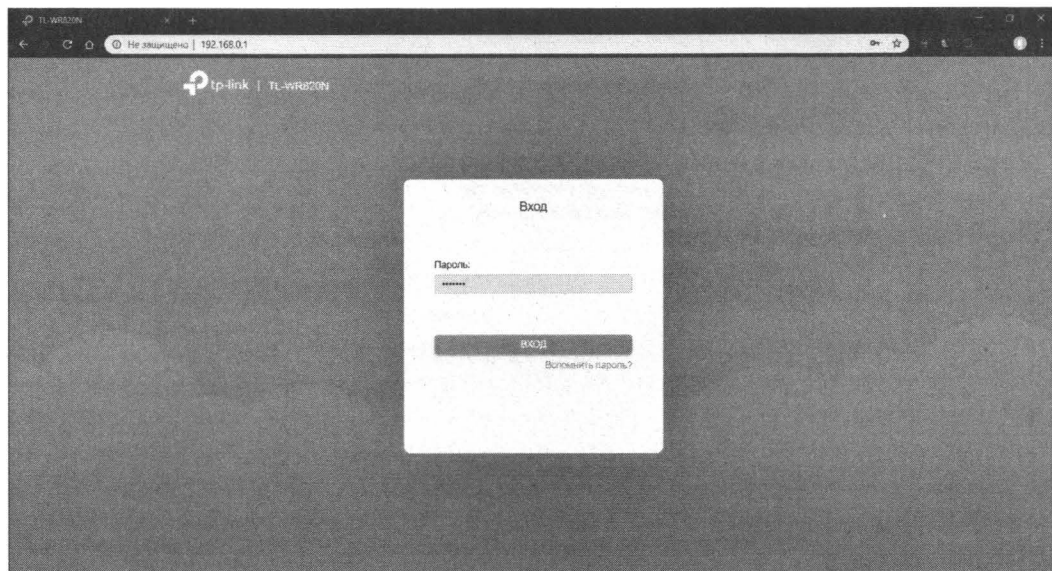
## **10.2. Защита маршрутизатора**

### **10.2.1. Изменение пароля доступа к маршрутизатору**

Итак, вы установили беспроводной маршрутизатор, он подключился к Интернету, а беспроводные адаптеры ваших домашних компьютеров подключились к созданной маршрутизатором беспроводной сети. Все работает, все компьютеры имеют доступ к Интернету.

Сейчас мы изменим пароль доступа к маршрутизатору. Обратите внимание — это не пароль доступа к беспроводной (Wi-Fi) сети. Это доступ к панели управления маршрутизатором, чтобы никто, кроме вас, не смог изменить его параметры.

Ранее, как правило, доступ к панели управления маршрутизатором (рис. 10.1) был возможен только с компьютера, подключенного к Ethernet-порту маршрутизатора, — для этого в комплекте с маршрутизатором поставляется короткий Ethernet-кабель. Однако современные модели разрешают и доступ по беспроводной сети.



**Рис. 10.1.** Вход в панель управления маршрутизатора TP-Link N300

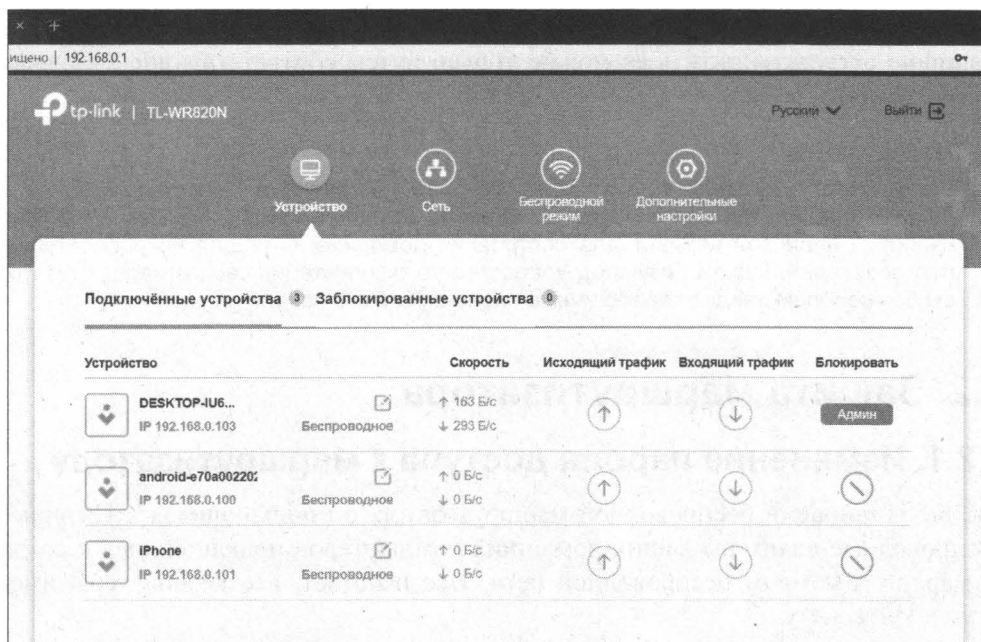


Рис. 10.2. Главная страница панели управления маршрутизатора TP-Link N300

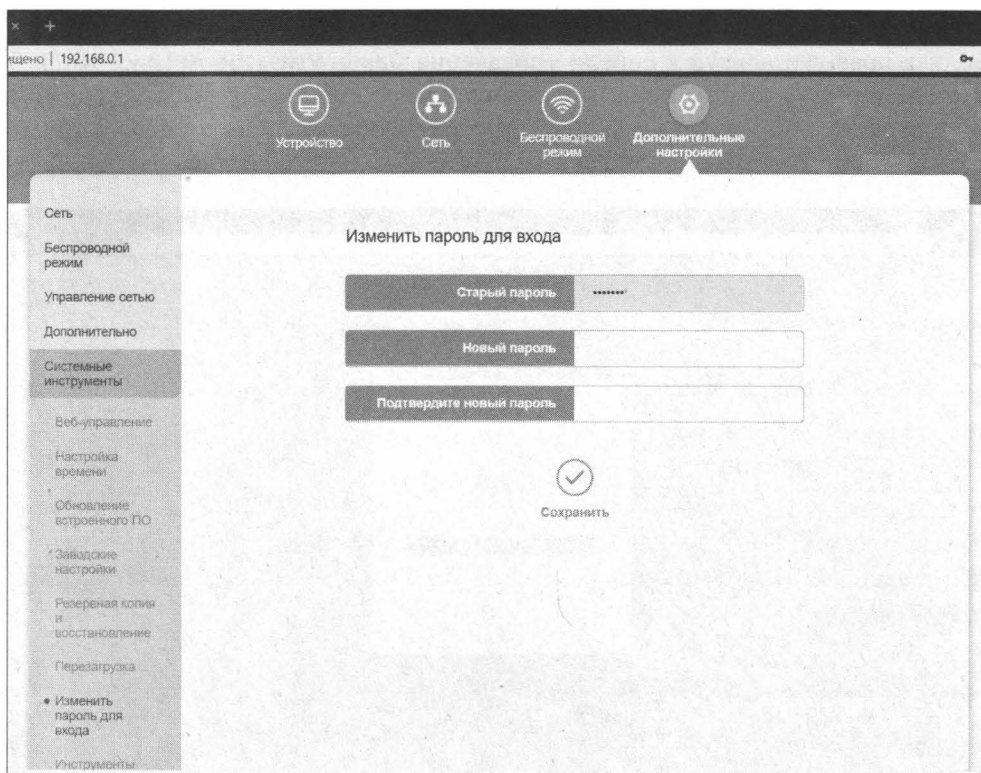


Рис. 10.3. Смена пароля для входа в панель управления маршрутизатора TP-Link N300

Другими словами, в панель управления маршрутизатором через вашу беспроводную сеть может зайти кто угодно. Именно поэтому важно установить надежный пароль на эту панель управления.

Сразу после входа будет отображена главная страница панели управления (рис. 10.3). Ее содержимое зависит от модели маршрутизатора и от установленной прошивки. В моем случае выводится список подключенных устройств.

Для смены пароля перейдите в раздел **Дополнительные настройки | Системные инструменты | Изменить пароль для входа** (рис. 10.3). Здесь нужно ввести старый пароль, новый и его подтверждение.

### 10.2.2. Изменение имени сети (SSID). Скрытие SSID

SSID (Service Set Identifie) — это имя сети. По умолчанию значение SSID одинаково для всех беспроводных маршрутизаторов одного производителя. Представьте только, что вы примерно в одно и то же время со своим соседом обзавелись одинаковыми (или почти) маршрутизаторами. Имена ваших сетей окажутся одинаковыми, что не есть хорошо.

При изменении SSID помните, что новый SSID не должен содержать: адрес, вашу фамилию, номер телефона, номер квартиры и прочую общедоступную информацию. Лучше всего использовать никому не понятную последовательность символов — тогда сам злоумышленник побоится подключаться к такой сети, решит, что она специально создана для перехвата паролей и другой передаваемой через нее информации.

А еще лучше, когда все будет настроено, вообще скрыть широковещание SSID — тогда в округе вообще никто не будет знать, что у вас есть беспроводная сеть. Конечно, опытного злоумышленника этим не остановишь, но все же это лучше, чем ничего.

Для изменения SSID в панели управления Tp-Link перейдите в раздел **Дополнительные настройки | Беспроводной режим | Основная сеть** (рис. 10.4). Здесь можно изменить имя беспроводной сети (это и есть SSID), пароль для доступа к Wi-Fi, а также включить/выключить широковещание сети.

В этом разделе также можно изменить тип защиты — о том, что это такое, вы узнаете далее в этой главе.

Учтите, что если широковещание сети выключено, то при попытке подключения к ней имя сети (SSID) на всех подключаемых клиентах: других компьютерах, смартфонах, планшетах — придется вводить вручную. Поэтому выключение широковещания может создать определенные неудобства.

### 10.2.3. Отключения гостевой сети

Некоторые маршрутизаторы поддерживают так называемый *гостевой доступ*. В этом случае не разрешается доступ к локальной сети, но разрешается доступ к Интернету, при этом можно ограничить скорость и время доступа (рис. 10.5).

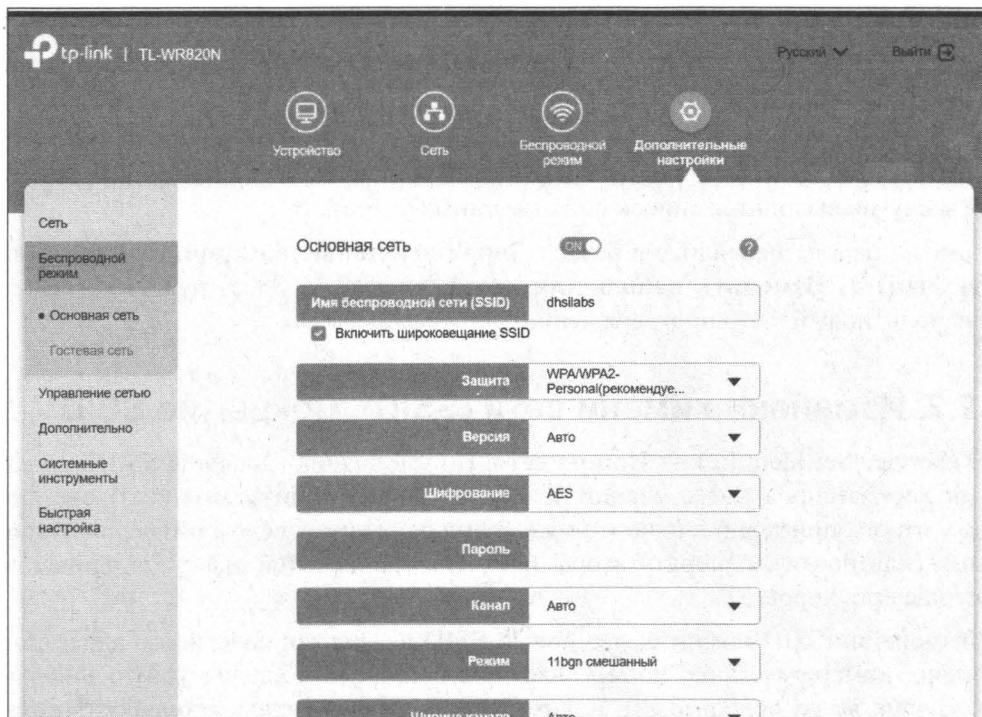


Рис. 10.4. Изменение параметров беспроводного режима основной сети

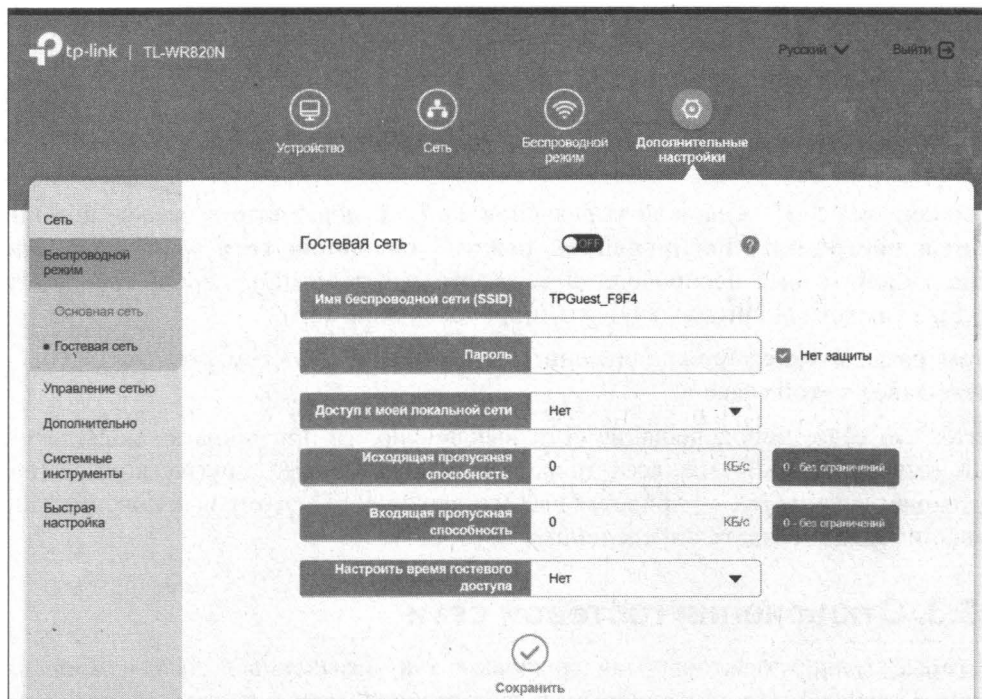


Рис. 10.5. Выключаем гостевую сеть

Если вам не нужна гостевая сеть (в большинстве случаев это так), ее лучше выключить.

## 10.2.4. Изменение IP-адреса маршрутизатора

IP-адрес маршрутизатора по умолчанию тоже легко вычислить, зная, хотя бы, производителя устройства. Поэтому не помешает изменить и IP-адрес маршрутизатора. Это можно сделать в разделе **Дополнительные параметры | Сеть | Настройка локальной сети** (рис. 10.6).

### **ВНИМАНИЕ!**

При назначении маршрутизатору нового IP-адреса будьте осторожны. Параметры **Начальный IP-адрес** и **Конечный IP-адрес** в разделе **DHCP-сервер** задают диапазон арендуемых IP-адресов: из этого диапазона IP-адреса будут назначаться клиентам маршрутизатора. Так вот, IP-адрес, заданный параметром **IP-адрес**, не должен принадлежать к этому диапазону.

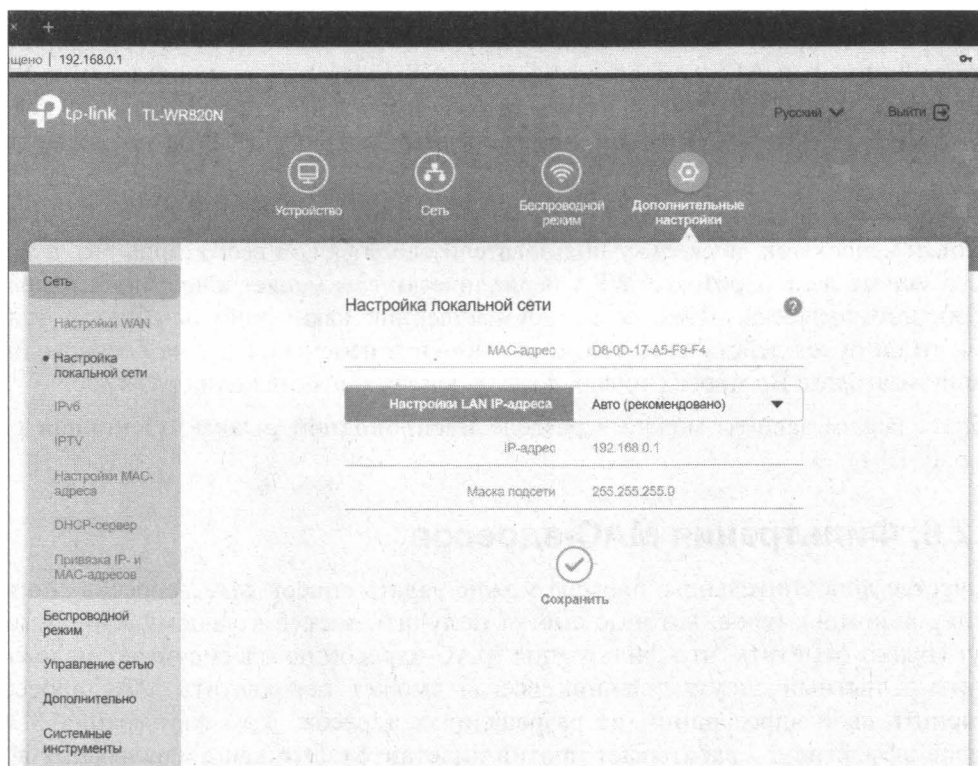


Рис. 10.6. Установка IP-адреса маршрутизатора

## 10.2.5. Используйте WPA или WPA2

Протоколы WPA (Wi-Fi Protected Access), WPA2 и WEP (Wired Equivalent Privacy) обеспечивают защиту и шифрование данных, передаваемых беспроводным маршрутизатором и беспроводным клиентом. Предпочтительнее использовать WPA2,



но если этот протокол устройством не поддерживается, следует использовать WPA. Шифрование WEP заметно хуже, чем WPA, но это лучше, чем вообще ничего. Хотя взломать защиту WEP можно с помощью ряда стандартных инструментов, что означает, что взлом WEP — весьма обычная процедура.

#### **ПРИМЕЧАНИЕ**

Сейчас можно взломать даже WPA2. Интересующимся рекомендую прочитать следующую статью: <http://fsearch.kiev.ua/ru/searchpracticaru/-internetscurity-ru/1749-how-to-crack-wi-fi-evil-wpa2-psk-passwords-using-dictionary-attacks-via>. Но в любом случае, лучше защиты, чем WPA2, пока не придумали.

При шифровании данных, которые передаются между маршрутизатором и беспроводным клиентом, протоколы WPA и WEP используют специальный ключ (пароль). Завладев ключом, злоумышленник сможет не только установить соединение с беспроводной точкой доступа, но и расшифровать данные, передающиеся между клиентами беспроводной сети.

На смену WEP в свое время пришел протокол WPA. Для управления ключом шифрования в WPA применяются несколько алгоритмов, в их числе TKIP (Temporal Key Integrity Protocol) и AES (Advanced Encryption Standard). Для использования WPA необходимо, чтобы все клиенты были совместимы с этим протоколом (не говоря уже о маршрутизаторе). Впрочем, все современные точки доступа поддерживают WPA.

Если используется протокол WEP, то ключ приходится вводить вручную. Это существенный недостаток, поскольку пользователи вводят ключ всего лишь раз, а затем им его менять лень. Протокол WPA периодически сам меняет ключ, причем делает он это автоматически. Даже если злоумышленник каким-нибудь образом узнает ключ, то он будет действовать только до момента изменения ключа беспроводным маршрутизатором. Во многих точках доступа ключи меняются один раз в час.

Выбрать режим защиты можно в разделе **Беспроводной режим | Основная сеть** (см. рис. 10.4).

### **10.2.6. Фильтрация MAC-адресов**

В качестве дополнительного барьера можно задать список MAC-адресов сетевых адаптеров компьютеров, которые смогут получить доступ к вашему маршрутизатору. Нужно отметить, что фильтрация MAC-адресов не обеспечивает надежной защиты. Опытный злоумышленник всегда сможет перехватить MAC-адреса и подменить свой адрес одним из разрешенных адресов. Зато фильтрация MAC-адресов эффективно срабатывает против дилетантов. Это как сигнализация в автомобиле — какая бы она ни была хорошая, опытный злоумышленник обойдет ее, а вот дилетанты и близко к машине не подойдут.

Не все маршрутизаторы имеют функцию блокирования доступа по MAC-адресу. В некоторых моделях есть ограничения по количеству записей в списке фильтра. Использовать ее или нет — решать вам. На рассматриваемом маршрутизаторе белый/черный список устройств находится в разделе **Управление сетью | Контроль доступа** (рис. 10.7). Работает он так. Если вы включите белый список, то



подключиться к сети смогут лишь устройства, которые есть в этом списке. Если включить черный, то устройства из списка не смогут подключиться к сети.

### ПРИМЕЧАНИЕ

Вы немного удивлены, что MAC-адрес можно перехватить и изменить? Перехват MAC-адресов сетевых адаптеров, работающих в беспроводной сети, возможен, если злоумышленник находится в радиусе действия сети. Поскольку пакеты передаются «по воздуху», и перехватить их с помощью специальной программы (например, NetStumbler) — вообще не проблема. Что же касается изменения MAC-адреса, то это — довольно-таки тривиальная задача для квалифицированного пользователя, причем в любой операционной системе. Как изменять MAC-адрес, показывать я не буду, — книга посвящена защите, а не взлому беспроводной сети.

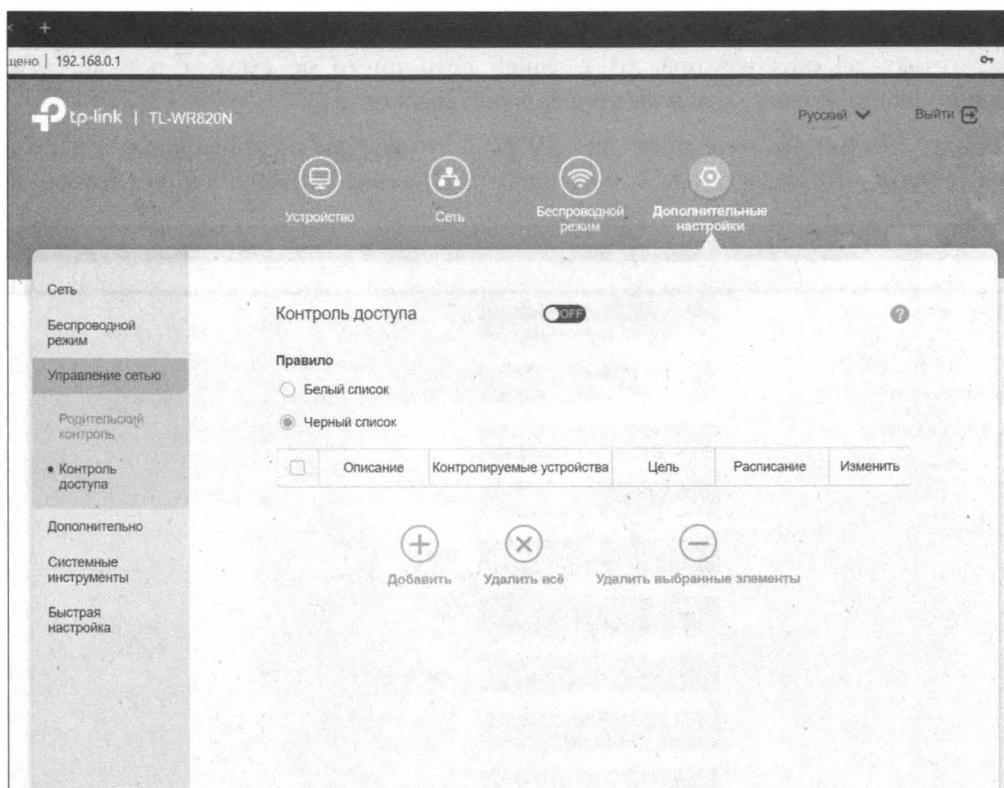


Рис. 10.7. Фильтрация по MAC-адресам

## 10.2.7. Понижение мощности передачи

Некоторые маршрутизаторы дают возможность понизить мощность передачи, что позволяет снизить число как преднамеренных, так и случайных несанкционированных подключений к сети. Понизив мощность передачи, можно добиться того, что точка доступа будет доступна только в пределах вашей квартиры. Вообще-то, использование мощной направленной антенны, позволяющей обнаружить даже самый слабый сигнал, сведет на нет все ваши старания, но, во всяком случае, от случайных подключений к своей сети вы себя оградите.

После понижения мощности передачи запустите на компьютере программу мониторинга уровня сигнала (вполне подойдет NetStumbler<sup>1</sup>) и исследуйте этот уровень в различных зонах вашего помещения. Если у граничных стен сигнал слабый, можно его еще понизить так, чтобы у границ вашей территории сигнала вообще не было. Однако после этого следует произвести повторное исследование уровня сигнала, чтобы убедиться, что беспроводная сеть есть там, где она должна быть.

Если у вас частный дом или отдельно стоящее офисное здание, выйдите из него и обойдите с ноутбуком здание вокруг — сигнала за его пределами быть не должно. Только так вы можете быть уверены, что никто случайно не подключится к вашей сети. Намеренное подключение с использованием направленных антенн, сигнал которых может проникать даже через стены вашего здания, исключать все же не стоит. Поэтому не нужно думать, что если вы понизили до минимума мощность передатчика маршрутизатора, то к вашей сети никто не сможет подключиться, и можно игнорировать остальные правила безопасности!

Параметр **Мощность передачи** (рис. 10.8) — это как раз и есть мощность передатчика. Уменьшите ее, а затем с помощью программы NetStumbler убедитесь, что

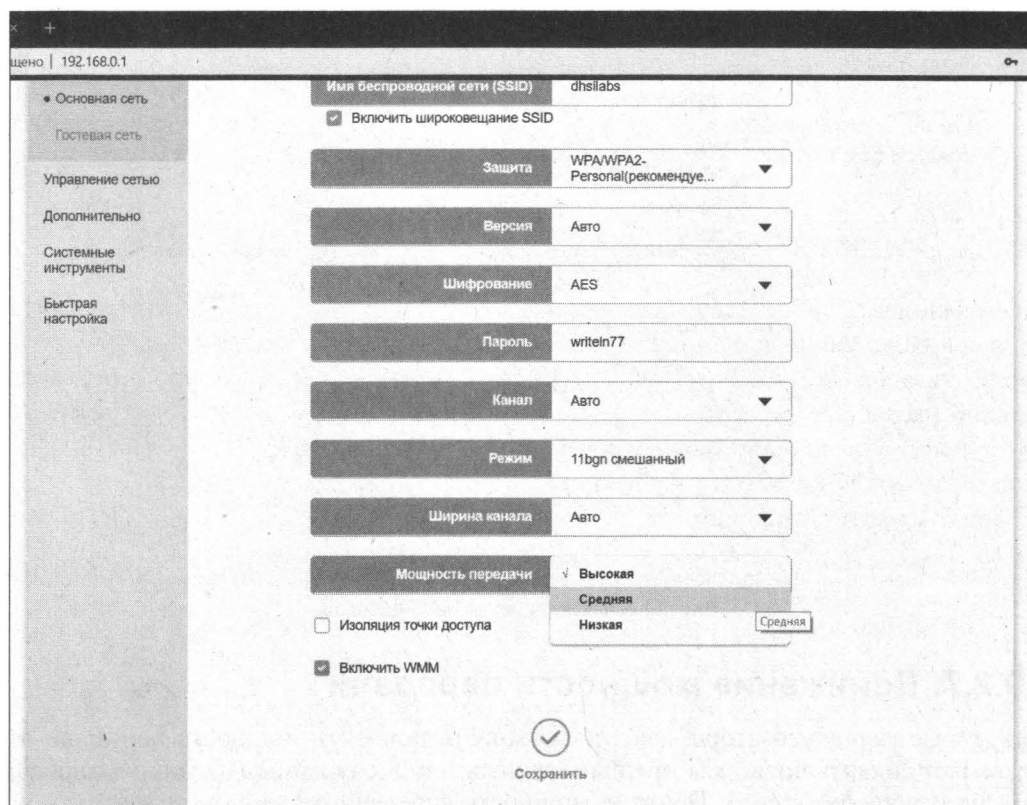


Рис. 10.8. Понижение мощности передачи

<sup>1</sup> См. <http://www.netstumbler.com/>.

беспроводная сеть есть в вашем помещении — во всех необходимых местах (проверьте силу и качество сигнала по всему помещению). В идеале за пределами вашего помещения сила сигнала должна быть минимальной, но добиться этого получается далеко не всегда.

\* \* \*

Мы рассмотрели основные параметры панели управления маршрутизатора TP-Link TL-WR820N. Нужно отметить, что эта панель управления весьма «урезанная», и я не нашел многих привычных по другим маршрутизаторам возможностей вроде блокировки URL, проброса портов и т. д. Впрочем, для нетребовательных пользователей модель неплохая и бюджетная. Она была куплена вместо сгоревшего WR-740N, но по своим возможностям не оправдала лично моих ожиданий, хотя это и серия 8XX.

#### **ПРИМЕЧАНИЕ**

Вы отключаете маршрутизатор на ночь? Нет? А зря. Дело даже не в «хакерах», а банально — в возможных перепадах напряжения и грозе, которая выводит маршрутизаторы из строя чрезвычайно часто. Также не забывайте извлекать из порта WAN-кабель (кабель провайдера). Совсем недавно во время грозы вышел из строя мой маршрутизатор — питание я выключил, а кабель извлечь забыл. Как потом оказалось, такая проблема возникла не только у меня. Конечно, гроза может быть и днем, но вдвойне обидно, когда маршрутизатором не пользовался, а он все равно вышел из строя. Днем можно хотя бы или успеть выключить его, или принять решение о работе «любой ценой», ночью же такого выбора нет.

## **10.3. Защита веб-камеры и микрофона**

Зачем защищать веб-камеру и микрофон, думаю, понятно — чтоб не подсматривали и не подслушивали. Стоит отметить, что при использовании беспроводного маршрутизатора, который рубит на корню все входящие соединения (без предварительной настройки, да и, как показывает практика, не все маршрутизаторы позволяют делать такую настройку), угрозы могут исходить только изнутри. Другими словами — от программ, установленных на компьютере и передающих видео/аудиоданные третьим лицам.

Операционная система Windows 10 позволяет через окно **Параметры** отключать веб-камеру и микрофон, а также предоставлять доступ к ним только определенным программам. Зайдите в раздел **Конфиденциальность**, а затем в разделы **Камера** (рис. 10.9) и **Микрофон** и ограничьте использование этих устройств.

В Windows 7 такой роскоши нет, поэтому придется отключать устройства через Диспетчер устройств. Щелкните на устройстве камеры и выберите команду **Отключить устройство** (рис. 10.10). Устройство микрофона, как правило, находится в разделе **Аудиовходы и аудиовыходы**.

Внешние веб-камеры отключить просто — извлеките USB-кабель камеры из разъема, и на этом все. Можно также купить камеру с возможностью физического закрытия объектива, но в ней может быть микрофон, через который все равно может

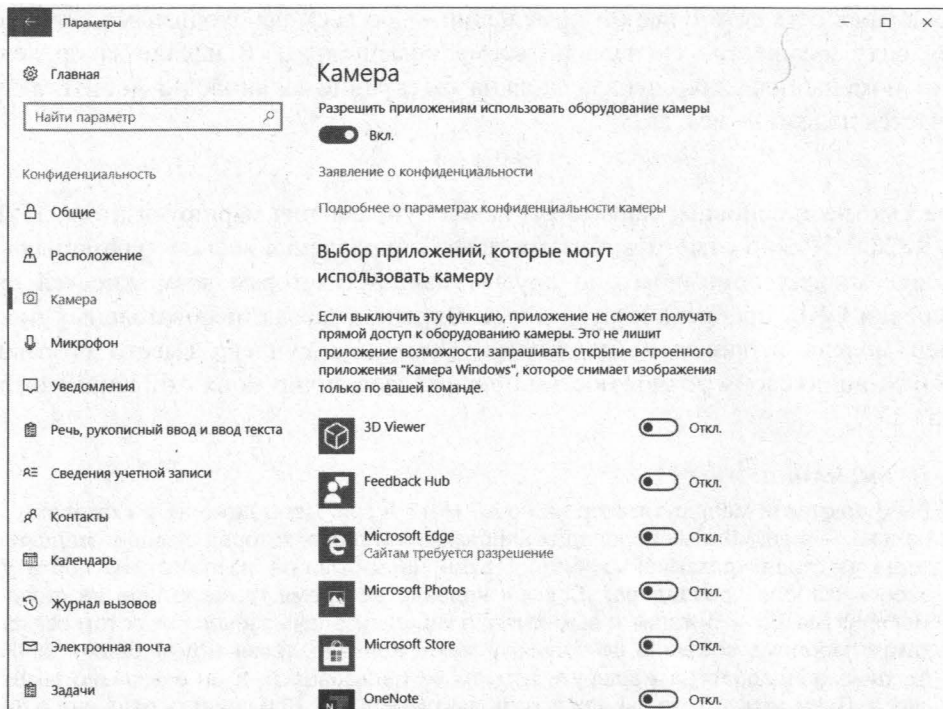


Рис. 10.9. Предоставление доступа к камере

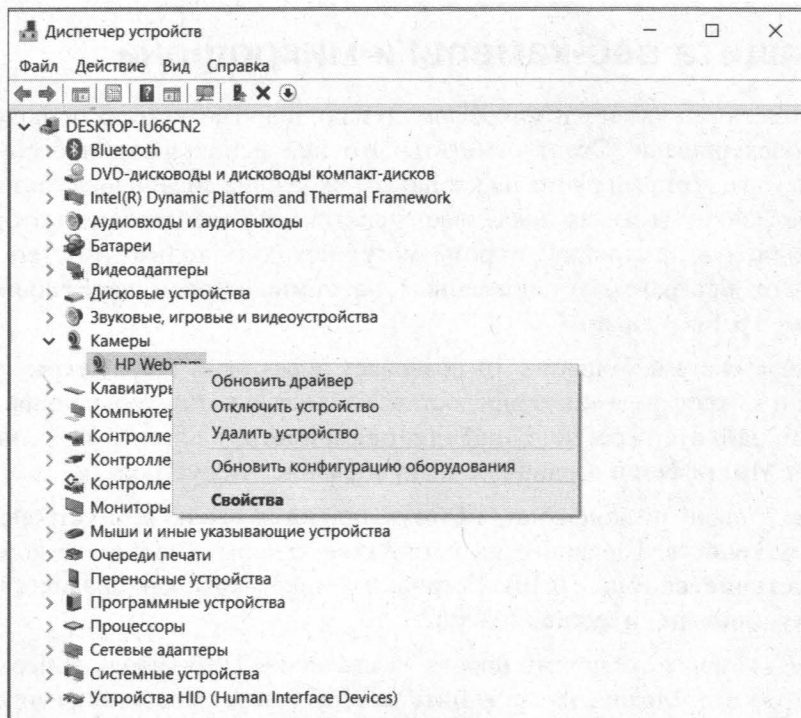


Рис. 10.10. Отключение устройства через Диспетчер устройств

осуществляться утечка данных, так что отключать устройства через Диспетчер устройств — надежнее.

Как видите, все делается программно, и наклеивать синюю изоленту на объектив камеры не пришлось.

## 10.4. Защита принтера

Все мы видели в кино, как принтеры взламывают и печатают на них всякую информацию. Как правило, это сетевые принтеры, поддерживающие печать по сети. Если ваш принтер не сетевой, то распечатать на нем документ может только локальная программа.

На мой взгляд, обычным домашним пользователям волноваться тут нечего. От подключений извне надежно защищает беспроводной маршрутизатор. А вот от несанкционированной печати с локального узла защитит либо антивирус, либо физическое отключение USB-кабеля принтера, что гораздо надежнее. И в самом деле — зачем постоянно занимать USB-порт, если принтер используется время от времени.

Что же касается защиты сетевого принтера, то пусть этим занимается сисадмин. Ему в помощь следующая статья: <http://www.spy-soft.net/hacking-printers/>. К сожалению, защита инфраструктуры предприятия выходит за рамки этой книги.



## ГЛАВА 11



# Безвозвратное удаление данных

Для начала небольшое введение на тему того, почему важно надежно удалять данные, даже если вы — не секретный агент.

Почему-то безвозвратное удаление данных часто ассоциируется с криминалом. Полагают, что если пользователю нужно безвозвратно стереть данные с жесткого диска, то он обязательно нарушил закон и не хочет, чтоб полиция узнала о его грязных делишках. Видимо, сказываются прошлые стереотипы вроде «А наши люди в булочную на такси не ездят».

Если какому-нибудь криминальному элементу понадобится удалить данные с жесткого диска, то ему это проще (а главное — быстрее) сделать способом прямого физического воздействия: сжечь, вбить гвоздь потолще или просто несколько раз ударить молотком. После такого вмешательства редкий жесткий диск или SSD выживет. Мы же рассмотрим здесь мирные варианты — когда нужно подарить или продать носитель данных (диск, флешку и т. п.). И если вы думаете, что, стерев с него данные доступными вам способами, тем самым все удалили, могу вас огорчить — часто бывает, что это не так.

Некоторое время назад группа злоумышленников скупала старые жесткие диски и восстанавливала на них информацию. Восстановленная информация использовалась с самыми разными целями. Например, если восстановилась финансовая информация (данные платежных карт, банковские пароли доступа), это приводило к финансовым потерям прошлых владельцев дисков. Личная информация, например некоторые личные фото, становилась предметом шантажа, а восстановленные пароли помогали взламывать почтовые и прочие их аккаунты, за возобновление доступа к которым тоже требовали деньги. В общем, парни крутились, как могли.

В *главе 9* мы немного затронули вопрос удаления данных, но сейчас поговорим о нем более предметно. И если описанными в ней способами мы вычистили компьютер и удалили определенные данные (в том числе историю браузера, Cookies и прочее), то здесь нам нужно убедиться, что данные действительно удалились.



## 11.1. Уничтожение информации на жестком диске

Способы уничтожения информации сильно зависят от типа устройств. И сейчас мы рассмотрим, как уничтожить данные на классическом жестком диске, не твердотельном (SSD). С твердотельными дисками мы разберемся в этой главе далее.

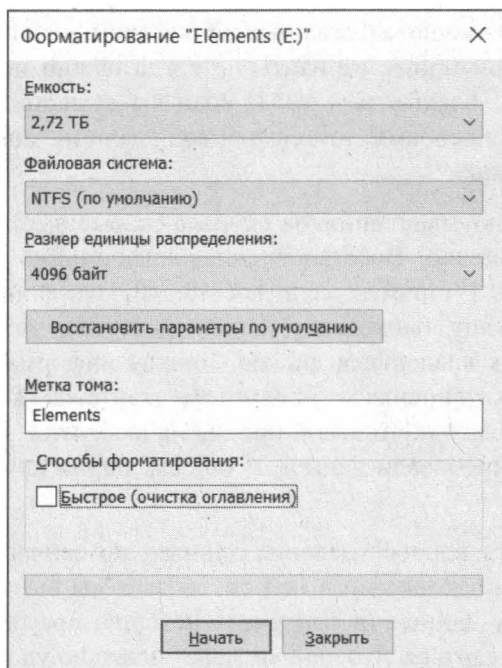
Традиционный способ уничтожения данных — форматирование. Вот только, как показывает практика, после форматирования данные относительно просто восстановить. Особенно, если использовалось быстрое форматирование. Совсем другое дело — форматирование полное.

Если на жестком диске никакой ценной информации нет, достаточно несколько раз его отформатировать, используя полное форматирование, для чего снять флажок **Быстрое** (рис. 11.1).

Но что делать, если у нас наблюдаются симптомы паранойи, или же жесткий диск действительно содержит ценную информацию, которая не должна попасть в чужие руки? В этом случае следует обратиться к алгоритмам гарантированного уничтожения информации.

В государственных учреждениях США ранее использовался стандарт DoD 5220.22-M, подразумевающий трехкратную перезапись диска. При первом проходе выполняется запись любого символа, затем — его XOR-варианта, а на третьем проходе — случайной последовательности. Получается, что за три прохода каждый байт информации на жестком диске перезаписывался так:

10101010 > 01010101 > 11011100 (последнее значение — случайное)



**Рис. 11.1.** Полное форматирование диска

Но, видимо, этот стандарт не обеспечивал должной надежности, поскольку сейчас в США носители секретной информации физически размагничивают или даже полностью уничтожают. А стандарт DoD 5220.22-М используется только для уничтожения несекретной информации.

В Канаде используется утилита DSX. Работает она так: сначала перезаписывает информацию нулями, а потом единицами, после чего записывает на диск последовательность данных, в которой закодирована информация о версии утилиты, дате и времени уничтожения информации.

В Германии для уничтожения несекретных данных используется стандарт BSI VSITR (расшифровку этой аббревиатуры вы без проблем найдете в Интернете, если она вам нужна). Стандарт подразумевает от двух до шести проходов, на каждом из которых на диск записывается псевдослучайная последовательность и ее XOR-эквивалент. Последним проходом записывается последовательность 01010101.

Какой алгоритм выбрать? Для окончательного удаления информации со всех современных жестких дисков достаточно один раз перезаписать их псевдослучайной последовательностью, все что более — делается исключительно для самоуспокоения и никак не влияет на результат.

## 11.2. Приложения для безопасного удаления данных с жестких дисков

Приложений для безопасного удаления достаточно много: Secure Erase<sup>1</sup>, DBAN<sup>2</sup> и т. д. Выбор утилиты зависит от предпочтений пользователя. Но лучше выбирать только OpenSource-утилиты, исходный код которых доступен. Важно, чтобы утилита выполняла именно удаление, а не шифрование информации.

Представим, что утилита информацию перезапишет не случайной последовательностью данных, а зашифрованной каким-то ключом версией данных пользователя, т. е. попросту зашифрует информацию. Пользователь будет считать, что информацию удалил, а кто-то сможет ее восстановить путем дешифровки.

Приложение DBAN является как раз OpenSource — его исходный код доступен всем желающим, и настоящие параноики могут даже откомпилировать его из исходников, чтобы быть уверенными в том, что утилита действительно делает то, что требуется.

Впрочем, можно обойтись и безо всяких утилит. Для этого достаточно зашифровать диск с помощью BitLocker. А после этого — отформатировать диск быстрым форматированием (для дополнительной надежности можно использовать и полное). При форматировании томов, зашифрованных BitLocker (даже при быстром), уничтожается и криптографический ключ, что делает невозможным восстановление ин-

---

<sup>1</sup> См. <https://partedmagic.com/secure-erase/>.

<sup>2</sup> См. <https://dban.org/>.

формации. Так что BitLocker можно использовать не только для шифрования данных, но и как способ быстрого и безвозвратного их удаления.

Важно только, чтобы нигде не сохранилась копия этого ключа. Убедитесь также, что ключ не загружался в облако OneDrive. При использовании учетной записи Microsoft проверить наличие дополнительных ключей можно по адресу: <https://account.microsoft.com/devices/recoverykey>.

## 11.3. Удаление информации с SSD

Безвозвратно удалить данные с твердотельного диска сложнее, чем с обычного жесткого. Чтобы удалить их действительно надежно, нужно понимать, как происходит запись/удаление информации на SSD.

Микросхемы памяти, используемые в SSD-накопителях, позволяют очень быстро считать информацию, чуть медленнее записать ее в чистый блок, и совсем медленно они записывают в блок, в котором уже есть какие-либо данные. Больше всего нас интересует как раз третий вариант — ведь нам нужно имеющуюся информацию перезаписать другой информацией.

Чтобы записать данные в ячейку, контроллер SSD должен сначала стереть данные в этой ячейке, а затем уже записать в нее новые. Поскольку сей процесс не очень быстрый, производители SSD разработали ряд оптимизационных алгоритмов, благодаря которым в распоряжении контроллера всегда есть нужное количество пустых ячеек, т. е. в большинстве случаев при записи информации на SSD она записывается вчистую, а не в уже использованную ячейку. Именно поэтому, когда твердотельный диск новый и пустой, он работает быстрее, чем когда на нем уже есть информация, и чем больше информации на SSD, тем медленнее он работает.

Что случится, если ОС захочет записать данные в ячейку с определенным адресом, но в этой ячейке уже содержатся какие-нибудь данные? Тогда контроллер SSD выполнит подмену адресов: нужный адрес будет назначен другой — пустой ячейке, а занятая ячейка или получит другой адрес, или уйдет в неадресуемый пул для последующей *фоновой* очистки.

Вот здесь и начинается безудержное веселье. Оказывается, информация просто-напросто вовсе не удалилась с SSD. Когда-то она, конечно, будет удалена, но должно пройти время. Пользователь думает, что удалил файл, но на самом деле информация на диске осталась. Пользователь думает, что перезаписал файл нулями, на самом деле он записал нулями неиспользуемые ячейки, а ячейки с данными остались в целостности и сохранности. Все это существенно усложняет нашу задачу.

Получается, что при обычном использовании на диск записывается больше данных, чем он может вместить. Пул свободных ячеек сокращается, и настает момент, когда контроллеру становится доступным лишь пул из неадресуемого пространства. Эта проблема решается с помощью механизма TRIM<sup>1</sup>, который работает совместно

---

<sup>1</sup> TRIM (от англ. to trim, подрезать) — команда интерфейса ATA, позволяющая операционной системе уведомить твердотельный накопитель о том, какие блоки данных не несут полезной нагрузки, и их можно не хранить физически.

с ОС. Если пользователь удаляет какой-то файл, форматирует диск или создает новый раздел, система передает контроллеру информацию о том, что определенные ячейки не содержат полезных данных и могут быть очищены.

Самое интересное, что в результате работы TRIM сама ОС не перезаписывает эти блоки, т. е. не стирает информацию физически. Она просто передает информацию контроллеру SSD, и с этого момента начинается (или может начаться — все решает контроллер) фоновый процесс удаления информации.

Что случится, если злоумышленник попытается считать данные из ячеек, на которые поступила команда TRIM, но которые не очищены физически. Тут все зависит от типа контроллера. Существуют три типа контроллеров, точнее, три алгоритма работы контроллеров:

- ☐ Non-deterministic trim — контроллер может вернуть фактические данные, нули или еще что-то, причем результаты попыток могут различаться от попытки к попытке. Так, при первой попытке это могут быть нули, при второй — единицы, при третьей — фактические данные;
- ☐ Deterministic trim (DRAT) — контроллер возвращает одно и то же значение (чаще всего нули) для всех ячеек, помеченных командой TRIM;
- ☐ Deterministic Read Zero after Trim (DZAT) — гарантированное возвращение нулей для всех ячеек, помеченных командой TRIM.

Узнать тип контроллера в Linux можно так:

```
$ sudo hdparm -I /dev/sda | grep -i trim
* Data Set Management TRIM supported (limit 1 block)
* Deterministic read data after TRIM
```

Контроллеры первого типа сейчас практически не встречаются. Ранее подобным поведением отличались накопители стандарта eMMC, но к настоящему моменту они практически все успешно вымерли, как мамонты. Как правило, на обычных ПК сегодня используются диски с контроллерами второго типа, а третий тип контроллеров присутствует только на дисках, предназначенных для работы в составе многодисковых массивов.

Казалось бы, все просто. Если у нас есть контроллер даже со вторым типом TRIM, то для ячейки, помеченной на удаление, мы гарантированно получим нули. Но не тут-то было.

А TRIM вообще включен и поддерживается ОС? Поддержка TRIM есть только в Windows 7 и более новых ОС. И лишь при соблюдении ряда условий. Первое условие — диск должен быть подключен напрямую по SATA/NVME, для USB-накопителей TRIM не поддерживается (бывают приятные исключения, но на то это и исключения). Второе — TRIM поддерживается только для NTFS-томов. Третье условие — TRIM должны поддерживать как драйверы диска/контроллера, так и BIOS.

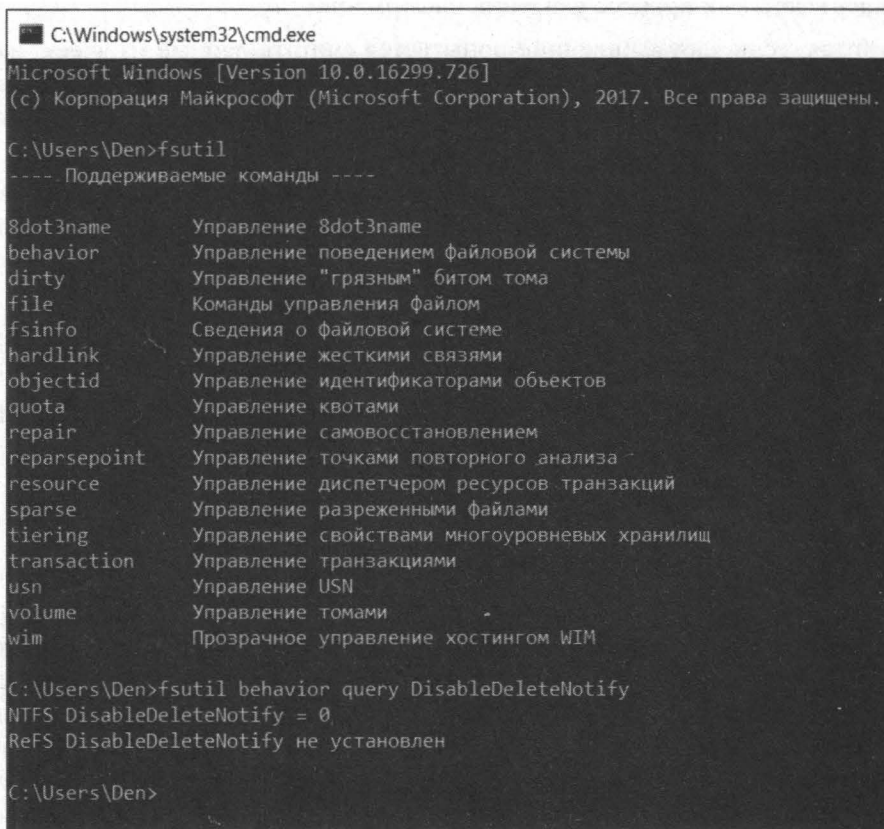
#### **ПРИМЕЧАНИЕ**

В Windows XP и Windows Vista нет встроенной поддержки TRIM, но ее можно включить с помощью Intel SSD Toolbox (старых версий, специально для указанных ОС).

Проверить работоспособность TRIM в Windows можно с помощью команды:

```
fsutil behavior query DisableDeleteNotify
```

Значение 0 (рис. 11.2) означает, что TRIM включен и работает корректно. Значение 1 — TRIM выключен. Для USB-дисков с большой вероятностью TRIM будет выключен.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.726]
(c) Корпорация Майкрософт (Microsoft Corporation), 2017. Все права защищены.

C:\Users\Den>fsutil
---- Поддерживаемые команды ----

8dot3name      Управление 8dot3name
behavior        Управление поведением файловой системы
dirty          Управление "грязным" битом тома
file           Команды управления файлом
fsinfo         Сведения о файловой системе
hardlink       Управление жесткими связями
objectid       Управление идентификаторами объектов
quota          Управление квотами
repair         Управление самовосстановлением
reparsepoint   Управление точками повторного анализа
resource       Управление диспетчером ресурсов транзакций
sparse         Управление разреженными файлами
tiering        Управление свойствами многоуровневых хранилищ
transaction    Управление транзакциями
usn            Управление USN
volume         Управление томами
wim            Прозрачное управление хостингом WIM

C:\Users\Den>fsutil behavior query DisableDeleteNotify
NTFS DisableDeleteNotify = 0
ReFS DisableDeleteNotify не установлен

C:\Users\Den>
```

Рис. 11.2. Команда fsutil

Включить TRIM можно командой:

```
fsutil behavior set disabledeletenotify NTFS 0
```

Для файловой системы ReFS команда будет другой:

```
fsutil behavior set disabledeletenotify ReFS 0
```

Для отключения TRIM команды будут такими же, только вместо 0 нужно указать 1.

#### ПРИМЕЧАНИЕ

Сейчас появились внешние твердотельные накопители, и вопрос о включении TRIM, бывает, касается и их. В большинстве случаев для внешних SSD, подключаемых по USB, включить TRIM нельзя, т. к. эта команда SATA не передается по USB (но в сети есть информация об отдельных контроллерах USB для внешних накопителей с под-

держкой TRIM). Для SSD, подключаемых по Thunderbolt, поддержка TRIM возможна (зависит от конкретного накопителя).

Остановить процесс очистки невозможно. И если на твердотельный диск подается питание, то контроллер будет продолжать уничтожать данные ячеек, помеченных TRIM. Но если очень надо, т. е. данные весьма ценные, то можно извлечь из накопителя чипы памяти и с помощью специального оборудования эти данные считать. Да, это сложно, да, из-за фрагментации данных — очень сложно, но такую задачу решить все же можно.

Если подытожить, то с SSD ситуация складывается следующим образом:

- ❑ примерно 10% (в некоторых накопителях — чуть меньше) емкости SSD отводится под резервный неадресуемый пул. В теории ячейки этого пула должны очищаться, но на практике это происходит не всегда, и из-за многочисленных особенностей реализации и банальных ошибок в прошивке данные из этого пула можно достать;
- ❑ мгновенно удалить данные с SSD с включенным TRIM можно путем форматирования раздела как NTFS — TRIM пометит блоки как неиспользуемые, а контроллер постепенно удалит из них информацию;
- ❑ если все прошло правильно, восстановить информацию будет невозможно. И даже если подключить SSD к другому компьютеру или специальному стенду, контроллер продолжит затирать информацию;
- ❑ если же из SSD извлечь микросхемы памяти, то данные можно будет считать.

Как надежно уничтожить содержимое твердотельного диска? Если нужно быстро уничтожить информацию на SSD, то единственный правильный выход — физическое уничтожение его микросхем. Если же погубить SSD в планы не входит, тогда нужно заранее отформатировать диск и ждать некоторое время (в надежде, что времени хватит), пока контроллер очистит ячейки памяти. Естественно, все это время на SSD должно подаваться питание.

### **ВНИМАНИЕ!**

Поведение SSD существенно затрудняет восстановление данных в случае каких-либо сбоев. Именно поэтому я бы рекомендовал использовать SSD только для системы и программ, чтобы ускорить их загрузку. Поскольку при записи/стирании данных возможны нюансы, которые мы здесь обсудили, восстановить файлы с SSD обычному пользователю будет очень непросто (я не говорю о специальных лабораториях, способных снять чипы памяти и прочитать с них информацию непосредственно). Именно поэтому лучшая защита от случайного удаления/изменения файла — его резервная копия. Периодически создавайте резервные копии всех важных данных — желательно на обычный HDD. Жесткие диски больших размеров (1 Тбайт и выше) сейчас вполне доступны, и не нужно на этом экономить. В Windows также можно включить опцию История файлов (сама «история» тоже пусть хранится на HDD, а не на SSD) — так вы защититесь от некорректного изменения файла, когда файл физически не удален, но перезаписан другим содержимым, и без проблем сможете восстановить его предыдущую версию.





## ГЛАВА 12



# Ошибки, ведущие к утрате анонимности

## 12.1. Как не совершать ошибок?

Очень легко нечаянно себя рассекретить — достаточно один раз без анонимизации зайти под своим «анонимным именем» на ресурс, на который вы обычно заходили анонимно. Это самая распространенная ошибка — просто зашли на сайт из другого браузера, не настроенного на Тог или на другой анонимный прокси, или же не обратили внимание на невключенный Тог.

Поэтому очень важно разобраться, в каких случаях вы будете использовать анонимизацию трафика, а в каких — нет. Причем принять решение нужно до того, как вы станете заниматься деятельностью, требующей анонимности.

Полностью анонимизировать всю свою деятельность в Интернете нельзя — сеть Тог не выдержит таких нагрузок (если вы станете, например, смотреть видео онлайн, слушать онлайн-радио и скачивать огромные файлы), а сеть I2P<sup>1</sup> еще не настолько популярна на наших просторах. Впрочем, в последнее время скорость передачи информации через Тог выросла, и все зависит от построенной цепочки: в некоторых случаях комфортно посмотреть то же видео просто невозможно, в некоторых — приходится снижать качество, чтобы избежать задержек при воспроизведении.

Так что выберите направления деятельности, которые хотите анонимизировать. Например, вы собрались вести свой блог, но при этом желаете остаться анонимным. Тут важно анонимизировать весь процесс ведения блога, начиная с его регистрации. При создании сайта (блога) вы можете самостоятельно зарегистрировать доменное имя и купить хостинг или зарегистрировать сайт (блог) на одной из бесплатных платформ (например, для блога — на LiveJournal).

С одной стороны, блог-платформа — более анонимный способ регистрации, поскольку при создании блога требуется указать только e-mail, который до этого сле-

---

<sup>1</sup> I2P (от англ. Invisible Internet Project, ИП, или I2P — проект «Невидимый Интернет») — анонимная компьютерная сеть. В этой книге не рассматривается ввиду сложности реализации.

дует зарегистрировать также анонимно — для этого не требуются ни паспортные, ни платежные данные.

### **ВНИМАНИЕ!**

Не указывайте при регистрации на блог-платформе свой основной e-mail.

С другой стороны, во всех громких делах против блогеров как раз фигурируют блог-платформы, т. к. они по первому запросу передают всю информацию о вас следственным органам — это вам не швейцарский банк. Но другого выхода вообще-то и нет, ведь при покупке платного хостинга придется указать свои реальные данные, что тем более нежелательно.

### **ПРИМЕЧАНИЕ**

Как правило, для анонимизации своей деятельности лучше использовать Тог, нежели VPN-сервисы, поскольку последние по запросу правоохранительных органов (или в судебном порядке) будут вынуждены сообщить ваши данные (по крайней мере, большинство из них). С сетью Тог все гораздо сложнее — для деанонимизации ее пользователя придется обратиться к владельцам всех узлов цепочки, что дает огромную фору во времени.

Вот несколько советов, которые помогут вам сохранить анонимность:

- ☐ придумайте себе псевдоним — нет никакого смысла использовать анонимность, если вы будете на каждом углу сообщать свое имя;
- ☐ заранее создайте себе один или два почтовых ящика — их нужно зарегистрировать анонимно с помощью Тог. Эти ящики вы будете использовать для конфиденциальной переписки и для регистрации различных интернет-ресурсов: сайтов, блогов и т. п.;
- ☐ регистрируйте интернет-ресурсы только в анонимном режиме — убедитесь, что Тог включена, и только после этого регистрируйте блог или сайт. Можно для регистрации использовать и доступ из интернет-кафе, но учтите, что там вас могут легко вычислить — во многих интернет-кафе установлены видеокамеры, да и выбирается интернет-кафе чаще всего ближайшее к дому. Вот если бы уехать в другой город... (напомню также, что в России выход в Интернет через публичные сети Wi-Fi кафе, аэропортов, вокзалов, библиотек и т. п. мест осуществляется только с регистрацией номера мобильного телефона, что равносильно регистрации по паспорту). Все зависит от информации, которую вы собираетесь анонимно публиковать;
- ☐ никогда не ведите свой блог в открытую (не анонимно) — некоторые блогеры комбинируют анонимные и неанонимные сессии, что ведет к их рассекречиванию.

## **12.2. Как не попасть под лингвистический анализ?**

С помощью так называемого *лингвистического анализа* можно легко установить, кому принадлежит написанный текст. А посему становится ясно — если вы будете комбинировать анонимные и неанонимные сессии для публикации разного рода кон-

тента, вас могут легко вычислить. Представим, что вы — журналист или писатель и публикуетесь в основном не анонимно. Но есть ряд интересующих вас тем, на которые вы бы хотели писать анонимно, поскольку опасаетесь преследований и репрессий в той или иной форме. В этом случае вам нужно изменить свой стиль изложения, иначе эксперты по лингвистическому анализу очень быстро установят, кто есть кто.

Посоветовать изменить стиль, конечно, проще всего. Но не всегда понятно, как это сделать. Чтобы знать, на что обратить внимание, следует ознакомиться с тем, как производится лингвистический анализ, т. е. самому превратиться в специалиста по такому анализу.

Вот на что аналитики обращают больше всего внимания:

- ☐ средняя длина предложения в знаках;
- ☐ средняя длина диалога в знаках;
- ☐ соотношение диалогов и предложений в тексте;
- ☐ использование уникальных слов (как словарных, так и выдуманных автором);
- ☐ частота использования уникальных слов;
- ☐ использование одних и тех же уникальных слов в открытых и анонимных публикациях;
- ☐ активный словарный запас (количество уникальных словарных слов в тексте);
- ☐ активный несловарный запас (количество уникальных выдуманных слов в тексте);
- ☐ статистика использования частей речи: процент существительных, глаголов, прилагательных и т. п.;
- ☐ биграммы частей речи, т. е. частота употребления пар «существительное-глагол», «наречие-прилагательное» и т. п.;
- ☐ позиции частей речи в предложении (по всем частям речи);
- ☐ биграммы буквенных пар (подсчет по всем алфавитным парам «аа», «аб», «ав» и т. п.).

Для лингвистического анализа текста специалисты используют набор различных методов. С некоторыми из них вы можете познакомиться по адресу: <http://filologia.su/metody>. В Интернете также можно найти программы для лингвистического анализа текста — например, Лингвистический анализатор 2.0, который можно скачать бесплатно по адресу: <http://softok.org/science/naukateh/7776prog.html>. Программа не заменит вам опытного аналитика, но все же это лучше, чем ничего.

В общем, информации в Интернете по этой теме — очень много, но наша книга посвящена анонимности в Интернете, а не лингвистике. Главное, чтобы вы знали, что такой способ деанонимизации существует, а предупрежден — значит вооружен.

## 12.3. Наиболее частые ошибки

Исходя из всего ранее сказанного, выделим основные ошибки, совершаемые желающими быть анонимными пользователями:

- ❑ использование анонимных и неанонимных сессий для одного и того же вида деятельности — например, при регистрации e-mail и блога вы не анонимизировали трафик, но начали это делать при ведении блога. Понятно, что легко запросить у администратора блога IP-адреса, которые были зафиксированы при регистрации блога, чтобы понять, кто вы;
- ❑ элементарная забывчивость — забыли включить Tor, забыли перенастроить браузер (например, сначала отменили включение прокси-сервера Tor, чтобы скачать фильм, а затем забыли и продолжили работу, но уже не в анонимном режиме). Чтобы хоть как-то помочь себе, установите два браузера: один вы будете использовать в анонимном режиме, второй — для обычного серфинга;
- ❑ публикация больших текстов сходного стиля написания под своим обычным именем. Или ничего не публикуйте под своим именем, или же измените стиль написания перед публикацией анонимного контента;
- ❑ доступ к анонимному почтовому ящику без шифрования — всегда используйте шифрование трафика для доступа к своему анонимному почтовому ящику;
- ❑ отказ от анонимизации трафика при работе с чужого компьютера — самая распространенная ошибка. Некоторые пользователи почему-то думают, что если они используют чужой компьютер (например, компьютер друга, родственника, соседа и т. п.), то уже анонимны. Это не так, и анонимизация трафика обязательна и в этом случае. Иначе вас очень легко будет выследить — придут к тому, у кого вы были, и спросят, он ли заходил на тот или иной ресурс. Он ответит, что не он, но что вы были у него в гостях в то время.

В *главе 13* вы узнаете, какие программы нужно использовать, чтобы остаться анонимным. Ведь иногда все старания идут насмарку, если программы для работы с Интернетом сами сообщают, куда нужно, всю информацию о вас...

## ГЛАВА 13



# Программы с «сюрпризами» и без...

## 13.1. Программы с открытым кодом

Для обеспечения большей анонимности вы должны использовать программы с открытым исходным кодом (так называемые OpenSource-программы). Исходный код таких программ свободно доступен на сайтах их разработчиков.

Возникает вопрос: почему именно OpenSource? У этих программ есть одно большое преимущество — их исходный код открыт, а это означает, что в коде программы нет «черных ходов» (backdoors), и эти программы не передают информацию о передаваемых с их помощью данных своим разработчикам или кому-либо еще. Ведь если бы это было так, общественность очень быстро бы об этом узнала. В мире много энтузиастов, исследующих исходный код программ на наличие всевозможных ошибок. Если в исходном коде того же Firefox будет найдена «черная дверь», через пару минут об этом узнает весь мир.

Программное обеспечение, исходный код которого закрыт, называется *проприетарным*. Проприетарное программное обеспечение не обязательно является платным. Наоборот, в мире есть множество программ, распространяемых бесплатно (freeware), но исходный код этих программ закрыт. Взять ту же «Оперу» (браузер Opera) — ее исходный код никому не доступен, то же самое можно сказать и об IE. Да, Internet Explorer может скачать любой желающий с сайта Microsoft, но сама Microsoft до сих пор не открыла его исходного кода.

Исходный код проприетарных программ — тайна за семью замками, и он редко когда бывает выложен в Интернете. Разве что произойдет утечка информации внутри компании, и чем-то обиженный сотрудник возьмет да и выложит «исходники» на каком-то сайте.

Поскольку исходный код проприетарного ПО закрыт, никто не может с абсолютной уверенностью сказать, что такие программы не передают данные (например, информацию о посещаемых вами узлах или содержимое заполняемых вами форм) разработчикам или третьим лицам.

Есть у OpenSource и еще одно преимущество — по сути, над разработкой программ с открытым кодом работает весь мир. Представьте обычную компанию, разрабаты-

вающую проприетарную программу. Сколько человек работает над ее исходным кодом? 10, 20, 50, 100, 500, пусть даже 1000. Так, общее число сотрудников Oracle Software (не только программистов, а всех сотрудников и во всех офисах по всем странам) составляет всего 840 человек. Размер относительно небольшого заводика на постсоветском пространстве. А в разработке OpenSource-программ косвенно принимают участие тысячи разработчиков. Да, пусть команда разработчиков какого-то OpenSource-проекта составляет всего несколько десятков человек. Зато к ним с легкостью присоединяются энтузиасты по всему миру, помогающие отлаживать программу, ищущие в ней «баги» и подсказывающие, как сделать так, чтобы программа работала лучше.

Но везде есть пятна — даже на Солнце. У программ OpenSource имеются свои недостатки, и вы должны знать об этом:

- ☐ недостаток финансирования — именно поэтому закрываются многие OpenSource-проекты, и ваша любимая программа сначала останется без поддержки (никто не будет исправлять «баги»), а в скором времени устареет и станет неактуальной. А как же энтузиасты? Они есть, пока существует основная команда разработчиков... Конечно, таких гигантов, как Firefox или FileZilla, это не коснется, но все же...
- ☐ доступность исходного кода всем — главное преимущество открытых программ является и главным их недостатком. Ведь любой желающий может скачать исходники программы, встроить в них backdoor или другой вредоносный код, а потом выложить свое произведение на «файлопомойках», на своем сайте (под видом «улучшенной» версии программы) и т. д. Но этот недостаток легко преодолеть — просто возьмите себе за правило качать программы только с их официальных сайтов, а не с произвольных источников.

## 13.2. Выбор программ

Программ для работы в Интернете очень много: браузеры, почтовые клиенты, FTP-клиенты и т. п. Вы должны знать, какие программы являются программами с открытым кодом, а какие — нет.

Сначала определимся, какие программы понадобятся для работы в Интернете:

- ☐ браузер — куда же без него;
- ☐ почтовый клиент — электронная почта была, есть и будет;
- ☐ программы для закачки файлов, FTP-клиенты — загружать файлы из Интернета приходится достаточно часто, и нужно позаботиться о подборе таких программ;
- ☐ клиенты для мгновенного обмена сообщениями. Электронная почта — это хорошо, но иногда хочется пообщаться, так сказать, в реальном времени, поэтому без клиентов для быстрого обмена сообщениями никак не обойтись.

### ПРИМЕЧАНИЕ

В главе 4 был рассмотрен выбор программы для мгновенного обмена сообщениями, поэтому в этой главе мы не рассматриваем такие программы.

### 13.2.1. Выбор браузера

Начнем с браузеров. В табл. 13.1 приведены OpenSource-браузеры и интернет-адреса официальных сайтов проектов, чтобы вы знали, откуда можно загружать программу.

*Таблица 13.1. Свободные браузеры*

Название	Сайт	Описание
Mozilla Firefox	<a href="https://www.mozilla.org/ru/firefox/">https://www.mozilla.org/ru/firefox/</a>	Самый популярный OpenSource-браузер. Его используют сотни тысяч пользователей по всему миру, он включен в состав практически всех дистрибутивов операционной системы Linux. Но не загружайте Firefox с файлообменников и сайтов всевозможных сообществ!
Mozilla SeaMonkey	<a href="http://mozilla-russia.org/products/seamonkey/">http://mozilla-russia.org/products/seamonkey/</a>	Проект в 2006 году пришел на смену популярному проекту Mozilla Suite, а разработка самого Suite была прекращена. В набор ПО входят: браузер, компоновщик страниц, почтовый клиент, адресная книга, IRC-чат — все, что нужно для работы в Интернете. Установив этот набор ПО, вам в 90% случаев больше не понадобятся еще какие-либо программы (если не считать программ для мгновенного обмена сообщениями). На сайте также можно скачать portable-версию продукта (для запуска с флешки без установки на компьютер)
Google Chromium	<a href="http://www.chromium.org/">http://www.chromium.org/</a>	Браузер с открытым кодом от сообщества The Chromium Authors и компании Google. Не стоит путать с браузером Google Chrome, исходный код которого закрыт! Об отличиях этих двух браузеров вы можете прочитать в Википедии по адресу: <a href="https://ru.wikipedia.org/wiki/Chromium">https://ru.wikipedia.org/wiki/Chromium</a>

Неужели в мире есть всего три браузера с открытым исходным кодом? Конечно же нет! Но остальные браузеры не могу вам порекомендовать по разным причинам:

- ☐ некоторые из них рассчитаны только на Linux. Конечно, если вы — опытный программист, то можете портировать один из таких браузеров в Windows. Но, как правило, игра не стоит свеч. Потратите уйму времени и не факт, что у вас получится;
- ☐ функциональность остальных программ не радует — если вы привыкли к тому же Firefox, то работать, скажем, с Konqueror вам будет непривычно. Я бы не стал рекомендовать вам такие программы.

Еще раз отмечу, что не нужно путать бесплатные (freeware) программы с OpenSource-программами. Да, популярный браузер Opera, каким бы удобным он ни был, не является OpenSource-программой, хотя распространяется бесплатно.



Хочется сказать несколько слов о Firefox. Этот браузер в последнее время обновляется весьма часто. Во время работы над своей книгой «Анонимность и безопасность в Интернете. От "чайника" к пользователю»<sup>1</sup>, вышедшей в 2012 году, я использовал 7-ю версию Firefox. Открываю сегодня в этом браузере окно **О Firefox**, чтобы узнать номер версии, и вижу, что Firefox версии 67.0 сейчас как раз обновляется (рис. 13.1), а после перезапуска браузера наблюдаю уже версию 67.0.2 (рис. 13.2).



Рис. 13.1. Firefox обновляется

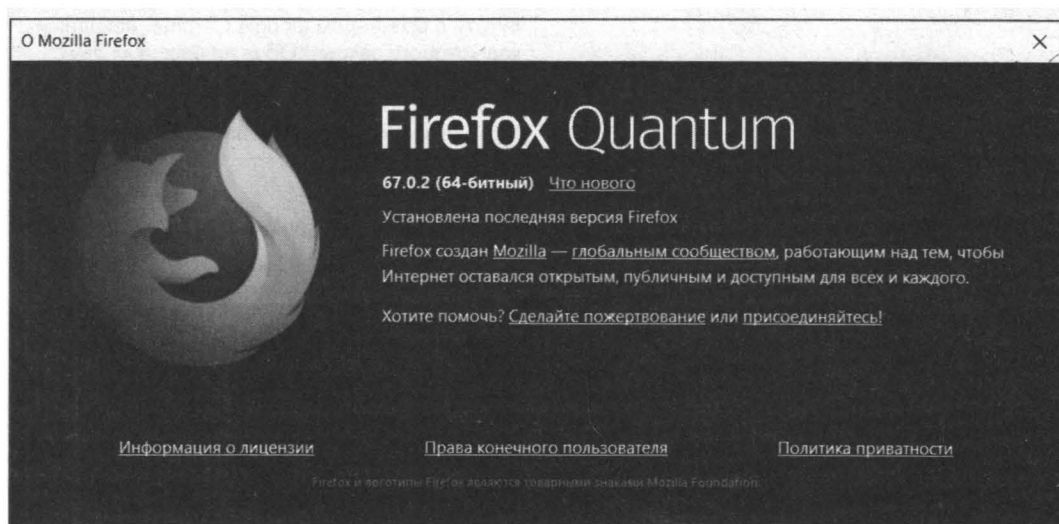


Рис. 13.2. Самая последняя версия на момент подготовки книги — 67.0.2

<sup>1</sup> См. <http://bhv.ru/books/book.php?id=189715>.

Постоянные обновления — это неплохо, значит разработчики ведут работу над исправлением ошибок. С другой стороны, разработчики сторонних расширений, которые вы используете, могут не поспевать за разработчиками браузера, и может оказаться, что ваше любимое расширение в последней версии браузера работать не будет. В настройках браузера (рис. 13.3) предусмотрена возможность отключить автоматические обновления. Если вы не используете сторонних расширений, можно оставить все как есть — пусть себе обновляется. Но если у вас много сторонних расширений, которые вы активно используете, имеет смысл отключить автоматические обновления. А обновляться уже по такой схеме: создаете контрольную точку средствами Windows, выполняете обновление браузера и проверяете работоспособность необходимых расширений. Если какой-нибудь плагин не работает, всегда можно выполнить восстановление из контрольной точки.

Прочитать о нововведениях в текущей версии Firefox можно или в Википедии, или на официальной странице проекта: <https://www.mozilla.org/ru/firefox/features/>.

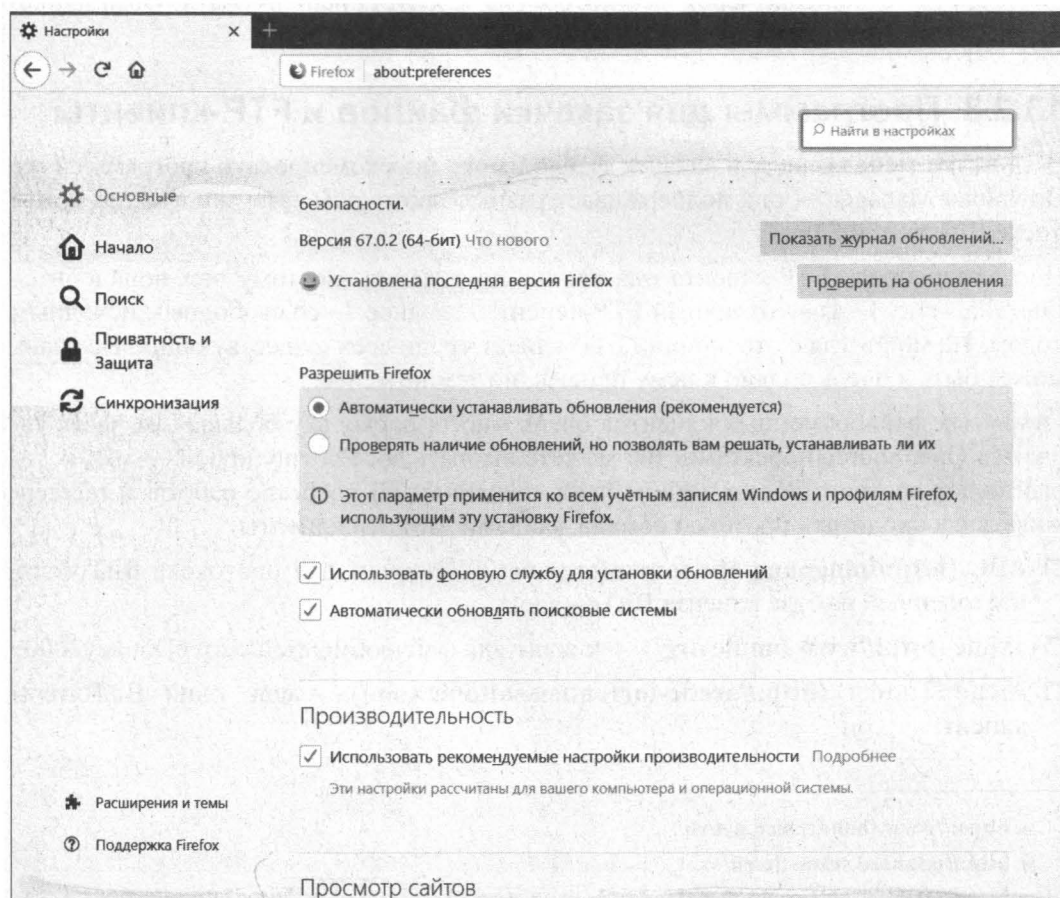


Рис. 13.3. Окно настроек Firefox: раздел Основные

### 13.2.2. Выбор почтового клиента

Теперь перейдем к открытым почтовым клиентам. Честно говоря, я вижу пока только один серьезный OpenSource-проект: Mozilla Thunderbird<sup>1</sup>. Так что, выбрав эту программу, вы не будете обделены.

Впрочем, можно порекомендовать и почтовый клиент Sylpheed<sup>2</sup>. Только используйте его последнюю версию — не следует загружать старые версии (ветка 2.x), поскольку в них пароли почтовых аккаунтов хранились в открытом виде. Выглядит, конечно, эта программа как привет из 2000-х. Очень архаично.

Более современный вариант — Mailspring<sup>3</sup>. Этот почтовый клиент с открытыми исходниками доступен для Windows, Linux и macOS. Поддерживает несколько почтовых ящиков, множество тем оформления, управление контактами и т. д.

С другой стороны, никто не запрещает работать с почтой через веб-интерфейс — популярные почтовые сервисы вроде Gmail.com обладают удобным интерфейсом, который ничем не хуже, чем интерфейс обычной почтовой программы. Разумеется, для работы с почтой через веб-интерфейс следует использовать OpenSource-браузер, а для еще большей уверенности — VPN-сервис.

### 13.2.3. Программы для загрузки файлов и FTP-клиенты

В качестве менеджера для загрузок файлов могу порекомендовать программу Free Download Manager<sup>4</sup> — она поддерживает разные протоколы загрузки файлов, в том числе BitTorrent и FTP.

Но полноценного FTP-клиента она все же не заменит. Поэтому вам понадобится FileZilla<sup>5</sup> (рис. 13.4) — отличный FTP-клиент, а главное — со свободным исходным кодом. На мой взгляд, это лучший FTP-клиент среди всех существующих. Не знаю, может быть я очень сильно к нему привык, но тем не менее...

Открытых файлообменных клиентов очень много, поскольку большая их часть являются OpenSource-проектами. Вы можете выбрать абсолютно любой — тот, который будет соответствовать вашим представлениям об удобстве работы и поддерживать необходимый протокол обмена файлами. Вот эти клиенты:

- ❑ ABC (<http://pingpong-abc.sourceforge.net/>) — клиент для протокола BitTorrent, построенный на базе клиента BitTornado;
- ❑ aMule (<http://www.amule.org/>) — клиент для файлообменной сети eDonkey2000;
- ❑ Arctic Torrent (<http://arctic-torrent.en.softonic.com/>) — еще один BitTorrent-клиент;

---

<sup>1</sup> См. <https://www.thunderbird.net/ru/>.

<sup>2</sup> См. <http://sylpheed.sraoss.jp/en/>.

<sup>3</sup> См. <https://getmailspring.com/download>.

<sup>4</sup> См. <https://www.freedownloadmanager.org/ru/download.htm>.

<sup>5</sup> См. <https://filezilla.ru/>.

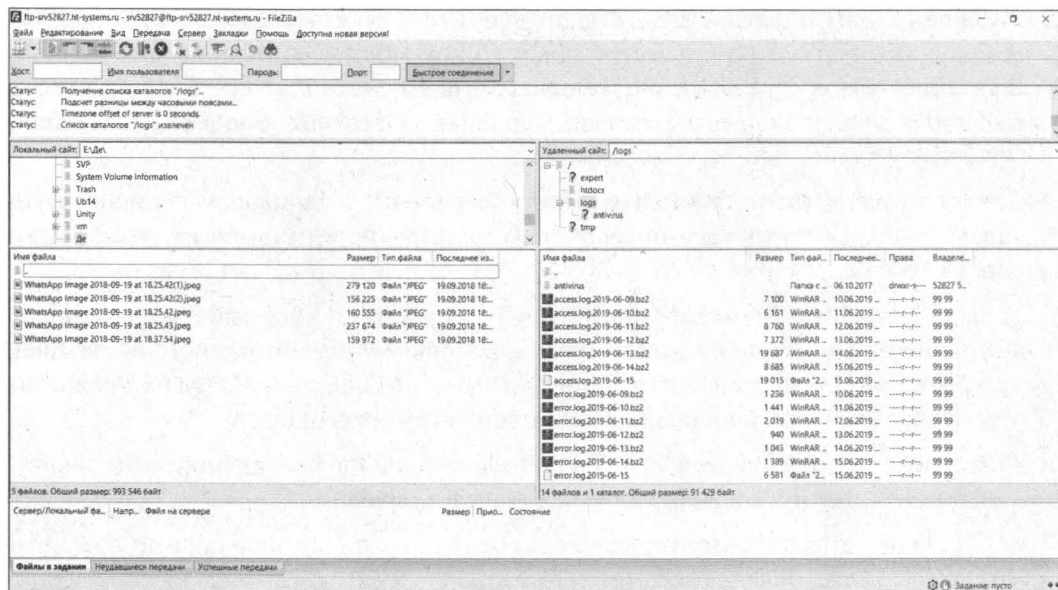


Рис. 13.4. Программа FileZilla: подключение с FTP-сервером установлено

- ❑ BitTornado (<https://bittornado.com/>) — Torrent-клиент, который был взят за основу при создании других клиентов для BitTorrent, в частности ABC;
- ❑ BitTyrant (<http://bittyrant.cs.washington.edu/>) — разработка Университета Вашингтона по созданию эффективного BitTorrent-клиента. Этот клиент основан на Azureus 2.5.x и обладает практически таким же интерфейсом. Но основное отличие — это механизм загрузки раздачи, увеличивающий скорость загрузки на 70% по сравнению с Azureus;
- ❑ DC++ (<http://dcplusplus.sourceforge.net/>) — свободный и открытый клиент файлообменной сети Direct Connect для Windows. Разработан как замена стандартному клиенту NeoModus Direct Connect;
- ❑ Deluge (<https://deluge-torrent.org/>) — клиент-сервер для передачи данных по протоколу BitTorrent, поддерживает множество плагинов;
- ❑ EMule (<https://www.emule-project.net/home/perl/general.cgi?l=34>) — свободный клиент файлообменной сети ed2k. Изначально был разработан как замена проприетарному клиенту eDonkey2000. В EMule встроен IRC-клиент, поэтому его можно также использовать для общения по протоколу IRC;
- ❑ FlyLinkDC++ (<http://www.flylinkdc.ru/>) — свободный и открытый клиент файлообменной сети Direct Connect. Был создан на DC++;
- ❑ G3 Torrent (<http://g3torrent.sourceforge.net/>) — еще один Torrent-клиент, находится на стадии разработки. Ознакомиться с основными возможностями можно на сайте разработчика;
- ❑ KCeasy (<http://www.kceasy.com/>) — свободный файлообменный клиент. Поддерживает обмен файлами и поиск в сетях Gnutella, Ares и OpenFT;

- ❑ **MLDonkey** (<http://mldonkey.sourceforge.net/>) — кроссплатформенный файлообменный клиент с открытым исходным кодом. Поддерживает большое количество протоколов и P2P-сетей: eDonkey, FileTP (HTTP, FTP, SSH), Overnet, Kademlia, Direct Connect, Gnutella, Gnutella2, OpenNap, Souleseek, BitTorrent, FastTrack, OpenFT, DC++;
- ❑ **Torrent Swapper** (<http://bit-torrent.sourceforge.net/>) — социальный пиринговый клиент. Обладает удобным интерфейсом пользователя и удобным механизмом поиска файлов;
- ❑ **Transmission** (<https://transmissionbt.com/>) — простой и удобный Torrent-клиент, в отличие от других подобных программ использует совсем немного системных ресурсов. Возможностей у этого клиента тоже меньше, чем у других аналогичных программ, но их вполне достаточно для загрузки файлов;
- ❑ **Vuze** (<http://www.vuze.com/>) — Torrent-клиент, поддерживающий сети анонимизации I2P, Tor и Nodezilla. Ранее назывался Azureus;
- ❑ **XBT Client** (<http://xbtt.sourceforge.net/client/>) — клиент для пиринговой сети BitTorrent. Также обладает веб-интерфейсом.

Сравнение этих и некоторых других клиентов можно найти по адресу:

[http://en.wikipedia.org/wiki/Comparison\\_of\\_BitTorrent\\_clients](http://en.wikipedia.org/wiki/Comparison_of_BitTorrent_clients).

Как видите, при желании можно найти OpenSource-клиент практически для каждой файлообменной сети.

## 13.3. Плагины

Многие программы, в том числе и OpenSource, поддерживают всевозможные плагины (расширения), расширяющие функциональность основной программы. Вот только помните — перед установкой плагина нужно почитать о нем отзывы в Интернете. Ведь плагины зачастую пишутся не разработчиками основной программы, а сторонними программистами. Нечестные на руку разработчики могут написать плагины, сливающие конфиденциальную информацию. А внешне это будет совсем безобидный плагин, например, демонстрирующий погоду.

Есть и такие плагины, которые могут вас рассекретить. По ним можно вычислить ваш IP-адрес — и никакие анонимайзеры не помогут.

А есть плагины, наоборот, позволяющие сохранить анонимность. Например, для Firefox вы можете использовать следующие плагины:

- ❑ **Adblock Plus** — блокирует рекламу и контент, загружаемый со сторонних сайтов;
- ❑ **FireX Proxy** — позволяет быстро сменить IP-адрес, выбрав один из анонимных прокси. Однако выбор прокси здесь весьма ограничен, поэтому я бы рекомендовал найти списки прокси и настраивать для работы с ними браузер вручную;
- ❑ **NoScript** — позволяет разрешать использование JavaScript и другие интерактивные элементы: аудио, видео, Flash только доверенным сайтам;

- ☐ CookieSafe — разрешает использование Cookies только доверенным сайтам;
- ☐ Flashblock — блокирует нежелательные Flash-объекты на страницах;
- ☐ BetterPrivacy — позволяет контролировать особые Cookies Flash-объектов;
- ☐ HTTPS Everywhere — включает принудительное использование протокола шифрования для популярных веб-сайтов. Работает не для всех сайтов. Поддерживает браузеры Firefox, Opera, Chrome.

Правда, не все эти плагины работают с последней версией Firefox. Тут выбирать вам: или использовать тот или иной плагин и обеспечить дополнительную анонимность, или же использовать последнюю версию Firefox. На мой взгляд, не следует жертвовать безопасностью в погоне за последней версией браузера.

# Заключение

По традиции вместо скучного заключения привожу список интересных ресурсов, связанных с безопасностью и анонимностью работы в Интернете:

- ❑ <https://www.psc.ru/sergey/bgtraq/ARTICLES/wwwseq/www-security-faq.html> — часто задаваемые вопросы, связанные с безопасностью в Сети;
- ❑ <https://wos.anho.org/security/> — еще один полезный ресурс, который поможет вам сохранить анонимность и безопасность в Интернете;
- ❑ <https://nordrus.info/security/> — руководство по защите информации;
- ❑ <http://malpaso.ru/gpg-keysigning-party/> — правила обмена ключами для зашифрованного обмена информацией;
- ❑ <https://pgpru.com/> — сайт проекта OpenPGP в России.



# Предметный указатель

## A

Acronis 122  
AES 179  
AOMEI Partition Assistant 122  
APK-файл 171  
App Lock 176

## B

BitLocker 130  
♦ поддерживаемые файловые системы 131

## C

Crypto Plugin 184  
CrystalDiskMark 163  
Cybersafe Top Secret 109

## D

DarkComet RAT 89

## E

E4M 144  
eCryptfs 140  
EDS 125  
EDS Lite 179  
EFS 127  
EFS Recovery Agent 128  
Encrypted File System 126

## F

File Encryption Key 128  
Folder Lock 165  
FTP-клиенты 250

## G

Google: проверка безопасности 200  
GPS-модуль 189

## I

IP-адрес 175  
IP-адрес маршрутизатора 225

## L

LUKS Manager 179

## M

MailDroid 186

## O

OpenPGP 106  
OpenSSL 107  
Orbot 174

## P

PFX-файл 113  
PGP 106  
PGP Desktop 107  
PKI 105  
public key 106

## S

S/MIME 105  
SecurityKISS 173  
Signal Protocol 72, 73, 74, 77  
SMTP: список серверов 100

SSID, имя сети 223  
Symantec Endpoint Encryption 164

## T

Tor для Android 174  
TPM 130  
TRIM 237  
TrueCrypt 144, 179

## V

VPN 55, 173  
VPN-сервисы 56, 61, 64  
VPN-соединение 56

## X

X.509 107  
XSS-уязвимость 101

## Z

Zeus 89

---

## A

Алгоритм  
♦ AES 145, 226  
♦ RSA 108  
♦ TKIP 226  
♦ Whirlpool 145  
Анонимайзер 13, 14, 15, 36, 37  
Анонимизация трафика 9  
Анонимный прокси-сервер 15, 16, 21, 36  
Аппаратный чип TPM 130  
Аутентификация 16

**Б**

Безлимитные пакеты 220  
 Беспроводной маршрутизатор 219  
 Беспроводные сети Wi-Fi 219  
 Блог-платформа 241  
 Браузеры 247

**В**

Включение  
 ◇ BitLocker 131  
 ◇ чипа TPM 140  
 Выбор VPN-сервиса 56

**Г**

Генератор паролей 196

**Д**

Двухфакторная аутентификация 193, 199  
 Демон gpsd 189

**И**

Изменение пароля BitLocker 136

**К**

Кейлоггер 94  
 ◇ SniperSpy 95  
 Ключ  
 ◇ FEK 128  
 ◇ восстановления 133  
 ◇ открытый, закрытый 105  
 Команда  
 ◇ fsutil 238  
 ◇ openssl 107  
 Криптоконтейнер 125  
 Критерии оценки мессенджеров 67  
 Кэш DNS  
 ◇ очистка 213  
 Кэширование страниц 16

**Л**

Лингвистический анализ 242

**Н**

Неизвестные источники 172

**О**

Очистка приватных данных  
 браузера 22

**П**

Параметр: неизвестные  
 источники 172  
 Персональные данные 191  
 Плагины 252  
 ◇ Torbutton 40, 45, 52  
 ◇ TorLauncher 45  
 Понижение мощность передачи 227  
 Почтовые клиенты 250  
 Программа  
 ◇ BCWipe 216  
 ◇ CCleaner 215  
 ◇ DBAN 235  
 ◇ DSX 235  
 ◇ KeePass Password Safe 198  
 ◇ Secure Data Manager 198  
 ◇ Secure Erase 235  
 ◇ Tor 34  
 ◇ USBDeview 208  
 ◇ USBOblivion 210  
 ◇ анализа Cookies CookieSpy 101  
 ◇ восстановления паролей  
 ▫ Mail PassView 95  
 ▫ WebBrowserPassView 96  
 ◇ подбора паролей  
 ▫ Brutus 103  
 ▫ THC-Hydra 103

**Программы**

◇ OpenSource 245  
 ◇ для шифрования данных 179  
 ▫ EDS Lite 179  
 ▫ LUKS Manager 179  
 ◇ шифрования 29  
 Прокси-сервер 15, 16, 17  
 Проникновение в сеть  
 ◇ последствия 220  
 Проприетарное ПО 245  
 Протокол  
 ◇ WEP 225  
 ◇ WPA 225  
 ◇ WPA2 225

**Р**

Разблокировка зашифрованного  
 диска 136  
 Распределенная сеть Tor 33, 61,  
 64, 65

**С**

Скрытая передача информации 104  
 Скрыть широковещание SSID 223  
 Снятие блокировки  
 с зашифрованного диска 131  
 Сохранение ключа  
 восстановления 133  
 Способы подбора пароля 194  
 Стандарт  
 ◇ BSI VSITR 235  
 ◇ DoD 5220.22-M 234  
 ◇ eMMC 237

**Т**

Троян 89

**У**

Управление BitLocker 139  
 Установка программ:  
 неизвестные источники 171  
 Утилита SYSKEY 128

**Ф**

Фильтрация MAC-адресов 226  
 ФСТЭК 167

**Х**

Хороший пароль 194  
 Хранение паролей 197

**Ш**

Шифрование  
 ◇ BitLocker 130  
 ◇ всего диска 121  
 ◇ прозрачное 126  
 ◇ производительность 163  
 ◇ раздела 122  
 ◇ файлов с помощью EFS 129

**Э**

ЭЦП 184

# Эта книга поможет вам!

Современный Интернет таит в себе множество опасностей: в нем обитают сетевые мошенники и распространяются вредоносные программы, а хранящаяся на компьютере и смартфоне информация представляет особый интерес для киберпреступников. Книга подробно рассказывает о том, как эти данные защитить, как скрыть информацию о себе, получить доступ к заблокированным сайтам и оставлять меньше следов своего присутствия в Интернете.

- Хотите посещать сайты с ограниченным доступом?
- Хотите общаться в социальных сетях анонимно?
- Хотите скрыть свой IP-адрес и местоположение в Интернете?
- Хотите безопасно пользоваться смартфоном?
- Хотите защититься от кражи паролей и персональных данных?

## Обеспечить безопасность и анонимность по силам каждому!



**Колисниченко Денис Николаевич** — инженер-программист и системный администратор. Автор более 70 книг компьютерной тематики, в том числе «Самоучитель системного администратора», «Linux. От новичка к профессионалу», «Безопасный Android: защищаем свои деньги и данные от кражи» и др.

«», «»,

191036, Санкт-Петербург,  
Гончарная ул., 20  
Тел.: (812) 717-10-50,  
339-54-17, 339-54-28  
E-mail: mail@bhv.ru  
Internet: www.bhv.ru

ISBN 978-5-9775-6605-6

