TRUECRYPT

БЕСПЛАТНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ ДЛЯ ШИФРОВАНИЯ ИНФОРМАЦИИ “НА ЛЕТУ”

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

www.truecrypt.org

Информация о версии

Руководство пользователя TrueCrypt, версия 7.1a
Опубликовано TrueCrypt Foundation, 7 февраля 2012 г.

Уведомление

СОДЕРЖАНИЕ

ВВЕДЕНИЕ....6

РУКОВОДСТВО ДЛЯ НОВИЧКОВ....7

Как создать и использовать контейнер TrueCrypt....7
Как создать и использовать раздел/устройство, зашифрованное TrueCrypt....25

ТОМ TRUECRYPT....26

Создание нового тома TrueCrypt....26
Алгоритм хеширования....26
Алгоритм шифрования....26
Быстрое форматирование....27
Динамический («резиновый») том....27
Размер кластера....28
Тома TrueCrypt на дисках CD / DVD....28
Аппаратный/программный RAID, динамические тома Windows....28
Примечания к созданию томов....28
Избранные тома....30
Системные избранные тома....32

ШИФРОВАНИЕ СИСТЕМЫ....34

Скрытая операционная система....35
Операционные системы, поддерживающие системное шифрование....35
Диск восстановления TrueCrypt (Rescue Disk)....35

ПРАВДОПОДОБНОЕ ОТРИЦАНИЕ ПРИЧАСТНОСТИ....38

Скрытый том....39
Защита скрытых томов от повреждений....41
Требования безопасности и меры предосторожности касательно скрытых томов....45
Скрытая операционная система....50
Создание скрытой операционной системы....52
Правдоподобное отрицание причастности и защита от утечки данных....53
Варианты объяснения наличия двух разделов TrueCrypt на одном диске....54
Требования безопасности и меры предосторожности касательно скрытых ОС....56

ГЛАВНОЕ ОКНО ПРОГРАММЫ....58

Файл....58
Устройство....58
Смонтировать....58
Автомонтирование....58
Размонтировать....59
Размонтировать все....59
Очистить кэш....59
Не сохранять историю....59
Выход....60

Операции с томами....60
Меню программы....61
Тома -> Автомонтирование всех томов на основе устройств....61
Тома -> Размонтировать все смонтированные тома....61
Тома -> Изменить пароль тома....61
Тома -> Установить алгоритм деривации ключа заголовка....62
Тома -> Добавить/удалить ключевые файлы в/из том(а)....62
Тома -> Удалить из тома все ключевые файлы....62
Избранное -> Добавить смонтированный том в список избранных томов....62
Избранное -> Упорядочить избранные тома....62
Избранное -> Смонтировать избранные тома....62
Избранное -> Добавить смонтированный том в список избранных системных томов 62
Избранное -> Упорядочить системные избранные тома....62
Система -> Изменить пароль....62
Система -> Смонтировать без дозагрузочной аутентификации....63
Сервис -> Очистить историю томов....63
Сервис -> Настройка переносного диска....63
Сервис -> Генератор ключевых файлов....63
Сервис -> Создать резервную копию заголовка тома....63
Сервис -> Восстановить заголовок тома....63
Настройки -> Параметры....65
Монтирование томов TrueCrypt....67
Кэшировать пароль в памяти драйвера....67
Параметры монтирования....67
РАСПАРАЛЛЕЛИВАНИЕ....68
КОНВЕЙЕРИЗАЦИЯ....69
АППАРАТНОЕ УСКОРЕНИЕ....69
ГОРЯЧИЕ КЛАВИШИ....70
КЛЮЧЕВЫЕ ФАЙЛЫ....70
Диалоговое окно ключевых файлов....71
Токены безопасности и смарт-карты....72
Путь поиска ключевых файлов....72
Пустой пароль и ключевой файл....73
Быстрый выбор....73
Тома -> Добавить/удалить ключевые файлы в/из том(а)....73
Тома -> Удалить из тома все ключевые файлы....74
Сервис -> Генератор ключевых файлов....74
Настройки -> Ключевые файлы по умолчанию....74
ТОКЕНЫ БЕЗОПАСНОСТИ И СМАРТ-КАРТЫ....75
ПОРТАТИВНЫЙ (ПЕРЕНОСНОЙ) РЕЖИМ....76
Сервис -> Настройка переносного диска....77

ЯЗЫКОВЫЕ ПАКЕТЫ....78
Установка....78
АЛГОРИТМЫ ШИФРОВАНИЯ....79
AES....79
Serpent....80
Twofish....80
AES-Twofish....80
AES-Twofish-Serpent....81
Serpent-AES....81
Serpent-Twofish-AES....81
Twofish-Serpent....81
АЛГОРИТМЫ ХЕШИРОВАНИЯ....82
RIPEMD-160....82
SHA-512....82
Whirlpool....82
ПОДДЕРЖИВАЕМЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ....83
ИСПОЛЬЗОВАНИЕ В РЕЖИМЕ КОМАНДНОЙ СТРОКИ....84
Синтаксис....86
Примеры....87
МОДЕЛЬ МЕХАНИЗМА ЗАЩИТЫ....88
ТРЕБОВАНИЯ БЕЗОПАСНОСТИ И МЕРЫ ПРЕДОСТОРОЖНОСТИ....91
Утечки данных....91
Файл подкачки....92
Файлы дампа памяти....93
Файл гибернации....93
Незашифрованные данные в ОЗУ....94
Физическая безопасность....95
Вредоносное ПО (malware)....96
Многопользовательское окружение....97
Аутентичность и целостность данных....97
Выбор/изменение паролей и ключевых файлов....98
Trim-операции....99
Равномерное распределение нагрузки на блоки (Wear-Leveling)....99
Перераспределённые сектора....100
Дефрагментация....101
Журналируемые файловые системы....101
Клонирование томов....101
Дополнительные требования безопасности и меры предосторожности....102
О БЕЗОПАСНОМ РЕЗЕРВИРОВАНИИ ДАННЫХ....103
Несистемные тома....103
Системные разделы....104

Общие замечания....105
РАЗНОЕ....106
Использование TrueCrypt без прав администратора....106
Совместное использование по сети....107
Работа TrueCrypt в фоновом режиме....108
Том, смонтированный как сменный носитель....109
Системные файлы TrueCrypt и программные данные....110
Как удалить шифрование....112
Удаление TrueCrypt....113
Цифровые подписи....114
УСТРАНЕНИЕ НЕПОЛАДОК....116
НЕСОВМЕСТИМОСТИ....125
ЗАМЕЧЕННЫЕ ПРОБЛЕМЫ И ОГРАНИЧЕНИЯ....126
Замеченные проблемы....126
Ограничения....126
ВОПРОСЫ И ОТВЕТЫ....129
ТЕХНИЧЕСКИЕ ПОДРОБНОСТИ....143
Система обозначений....143
Схема шифрования....144
Режимы операции....146
Деривация ключа заголовка, соль и подсчёт итераций....147
Генератор случайных чисел....148
Ключевые файлы....151
Спецификация формата томов TrueCrypt....153
Соответствие стандартам и спецификациям....155
Исходный код....156
ПЛАНЫ НА БУДУЩЕЕ....156
СВЯЗЬ С РАЗРАБОТЧИКАМИ....156
ПРАВОВАЯ ИНФОРМАЦИЯ....156
ИСТОРИЯ ВЕРСИЙ....157
БЛАГОДАРНОСТИ....157
ССЫЛКИ....158

ПРЕДИСЛОВИЕ

Обратите внимание, что хотя большинство разделов в этом документе в целом применимо ко всем версиям TrueCrypt, некоторые разделы адресованы, главным образом, пользователям версии TrueCrypt для Windows. Таким образом, информация в них может не соответствовать версиям TrueCrypt для Mac OS X и Linux.

Введение

TrueCrypt это программное обеспечение, предназначенное для создания томов (устройств хранения данных) и работы с ними с использованием шифрования на лету (on-the-fly encryption). Шифрование на лету означает, что данные автоматически зашифровываются непосредственно перед записью их на диск и расшифровываются сразу же после их загрузки, т. е. без какого-либо вмешательства пользователя. Никакие данные, хранящиеся в зашифрованном томе, невозможно прочитать (расшифровать) без правильного указания пароля/ключевых файлов или правильных ключей шифрования. Полностью шифруется вся файловая система (имена файлов и папок, содержимое каждого файла, свободное место, метаданные и др.).

Файлы можно копировать со смонтированного тома TrueCrypt и на него точно так же, как и при использовании любого обычного диска (например, с помощью перетаскивания). При чтении или копировании из зашифрованного тома TrueCrypt файлы автоматически на лету расшифровываются (в память/ОЗУ). Аналогично, файлы, записываемые или копируемые в том TrueCrypt, автоматически на лету зашифровываются в ОЗУ (непосредственно перед их сохранением на диск). Обратите внимание, это *не* означает, что перед шифрованием/дешифрованием в ОЗУ должен находиться *весь* обрабатываемый файл. Никакой дополнительной памяти (ОЗУ) для TrueCrypt не требуется. Иллюстрация того, как всё это работает, приведена в следующем абзаце.

Предположим, у нас есть видеофайл формата .avi, хранящийся в томе TrueCrypt (следовательно, этот видеофайл полностью зашифрован). Пользователь указывает правильный пароль (и/или ключевой файл) и монтирует (открывает) том TrueCrypt. Когда пользователь дважды щёлкает мышью по значку этого видеофайла, операционная система запускает приложение, ассоциированное с файлами такого типа – в данном случае это, как правило, мультимедийный проигрыватель. Затем мультимедийный проигрыватель начинает загружать маленькую начальную часть видеофайла из зашифрованного тома TrueCrypt в ОЗУ (память), чтобы приступить к воспроизведению. Во время загрузки части файла TrueCrypt автоматически расшифровывает её (в ОЗУ), после чего расшифрованная часть видео (хранящаяся в ОЗУ) воспроизводится медиапроигрывателем. Пока эта часть воспроизводится, медиапроигрыватель начинает считывать сдругую небольшую часть видеофайла из зашифрованного тома TrueCrypt в ОЗУ (память), и процесс повторяется. Данная операция называется шифрованием/дешифрованием на лету, она работает для файлов любых типов (не только видео).

Обратите внимание: TrueCrypt никогда не сохраняет на диске никаких данных в незашифрованном виде – такие данные временно хранятся только в ОЗУ (оперативной памяти). Даже когда том смонтирован, хранящиеся в нём данные по-прежнему остаются зашифрованными. При перезагрузке Windows или выключении компьютера том будет размонтирован, а хранящиеся в нём файлы станут недоступными (и зашифрованными). Даже в случае непредвиденного перебоя питания (без правильного завершения работы системы), хранящиеся в томе файлы останутся недоступными (и зашифрованными). Чтобы

получить к ним доступ вновь, нужно смонтировать том (и правильно указать пароль и/или ключевой файл).

Руководство для новичков

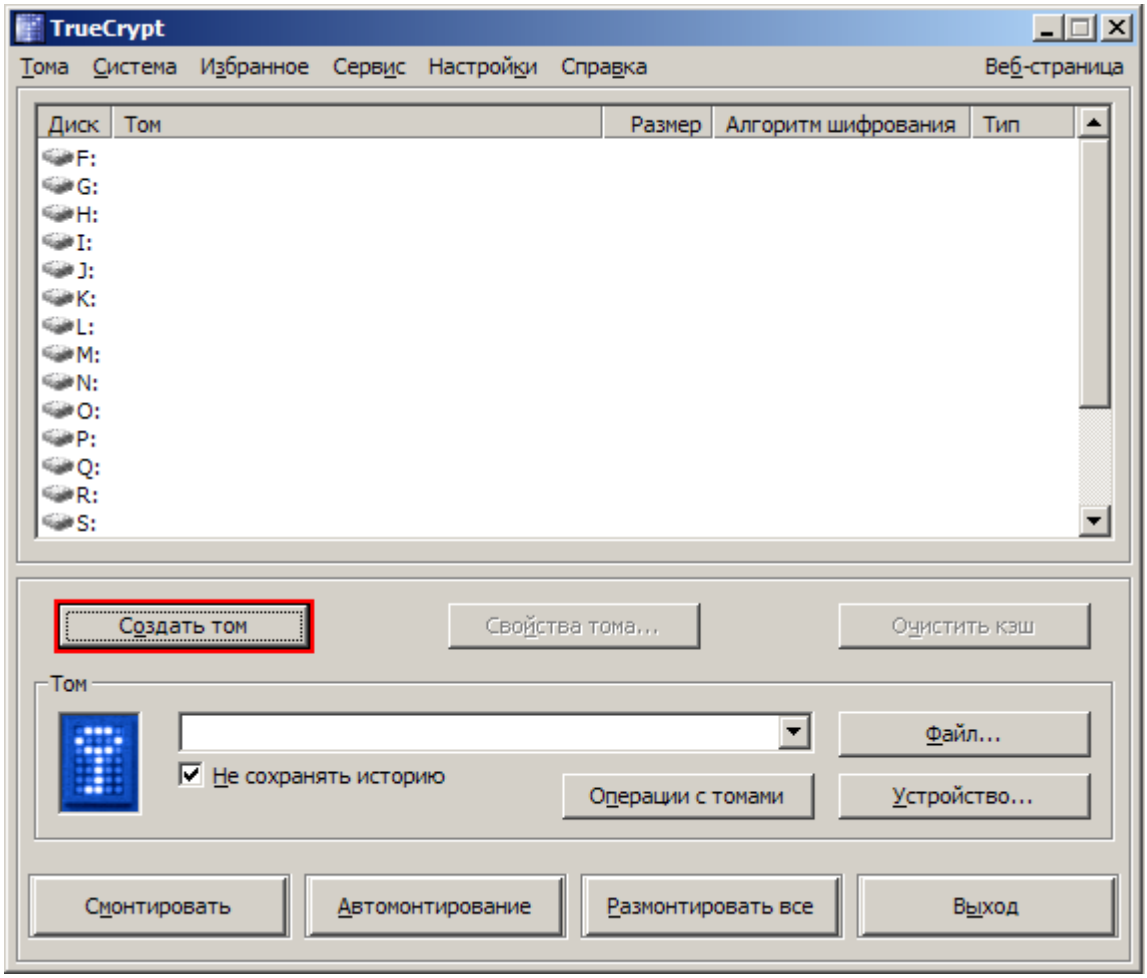
Как создать и использовать контейнер TrueCrypt

В этой главе содержатся пошаговые инструкции о том, как создавать, монтировать и использовать том TrueCrypt. Мы настоятельно вам рекомендуем также ознакомиться с другими разделами данного руководства, так как они содержат важную информацию.

Этап 1:

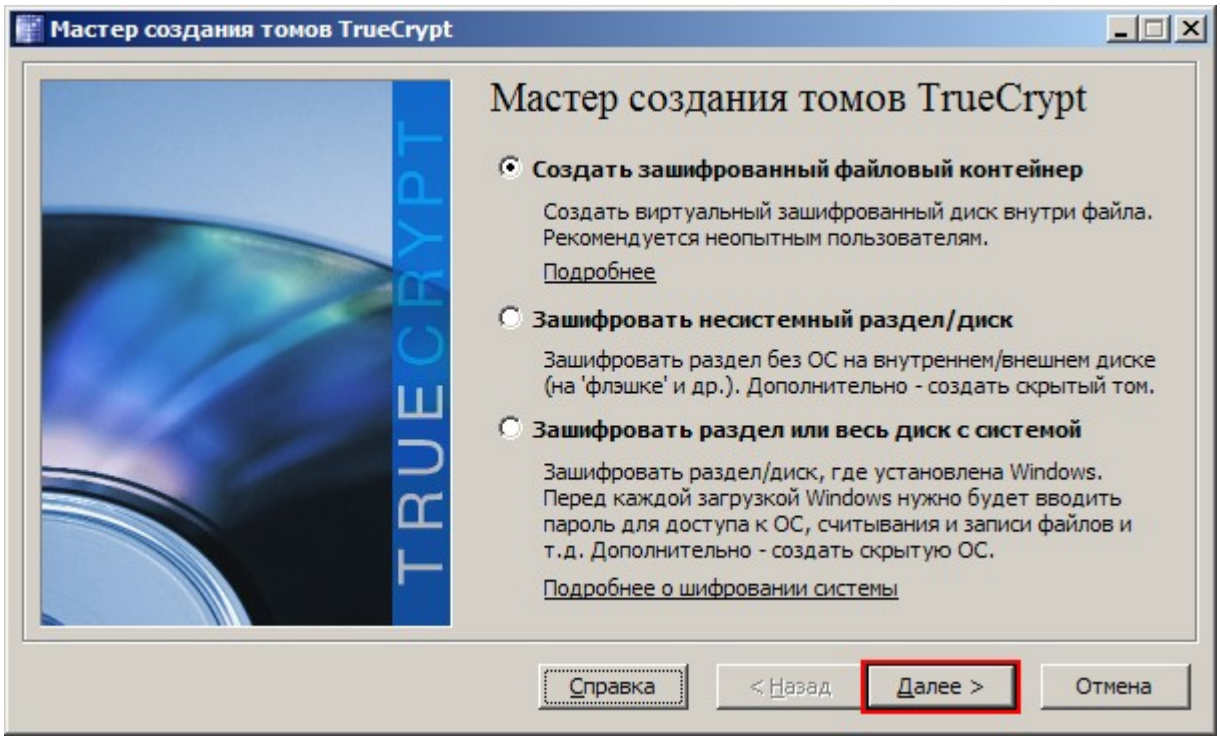
Если вы этого ещё не сделали, загрузите и установите TrueCrypt. Затем запустите TrueCrypt, дважды щёлкнув по файлу TrueCrypt.exe или по ярлыку TrueCrypt в меню «Пуск» в Windows.

Этап 2:



Должно появиться главное окно TrueCrypt. Нажмите кнопку **Создать том** (на иллюстрации она выделена красным).

Этап 3:



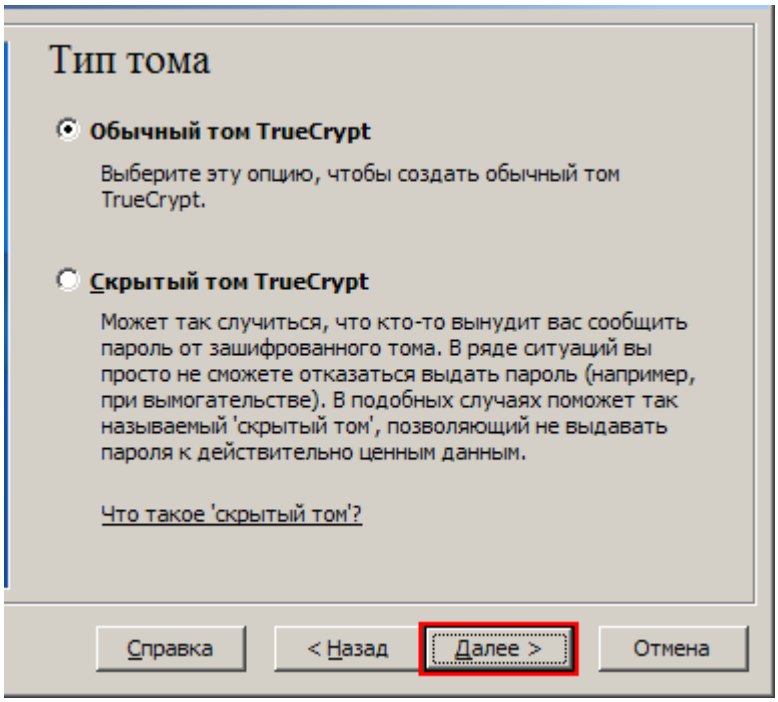
Должно появиться окно мастера создания томов TrueCrypt.

На этом этапе нам нужно выбрать место, где будет создан том TrueCrypt. Том TrueCrypt может находиться в файле (также именуемом контейнером), в разделе или на диске. В этом примере мы выберем первый вариант и создадим том TrueCrypt внутри файла.

Поскольку эта опция выбрана по умолчанию, просто нажимаем кнопку **Далее**.

Примечание: на иллюстрациях следующих этапов показана только правая часть окна мастера.

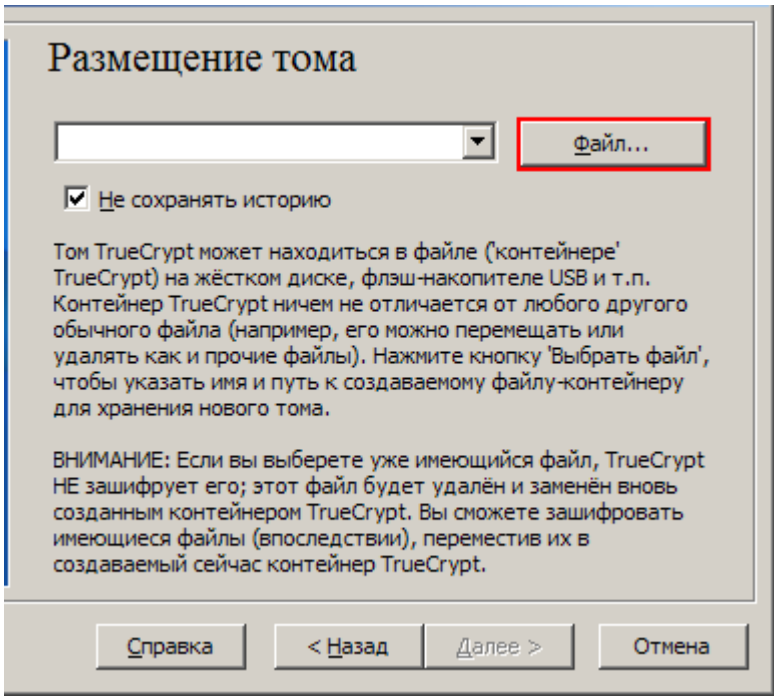
Этап 4:



Сейчас нам нужно выбрать, какой том TrueCrypt мы хотим создать – обычный или скрытый. В этом примере мы выберем первый вариант и создадим обычный том TrueCrypt.

Поскольку эта опция выбрана по умолчанию, просто нажимаем кнопку **Далее**.

Этап 5:

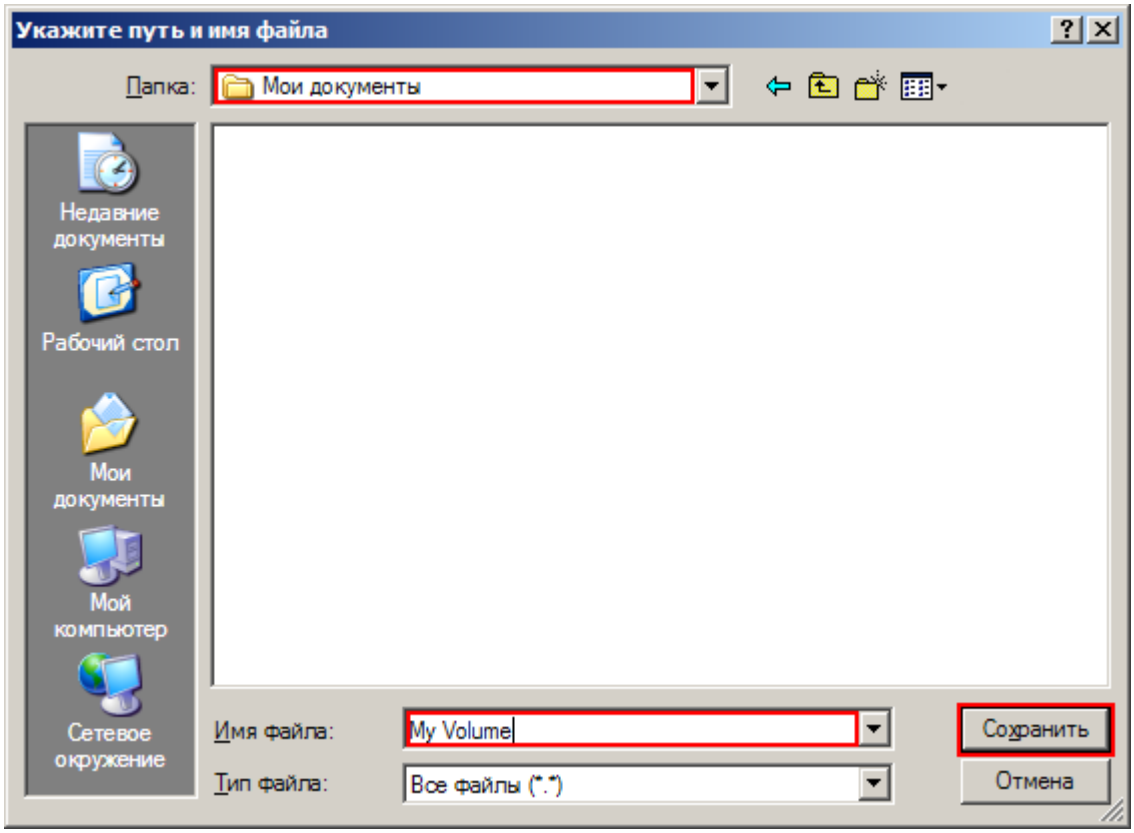


На этом этапе требуется указать место создания тома (файлового контейнера) TrueCrypt. Обратите внимание: контейнер TrueCrypt ничем не отличается от любого другого обычного файла. Например, его можно переместить или удалить как любой другой обычный файл. Также ему потребуется имя файла, которое мы выберем на следующем этапе.

Нажмите кнопку **Файл**.

Появится стандартное диалоговое окно выбора файлов Windows (при этом окно мастера создания томов останется открытым в фоне).

Этап 6:



В этом руководстве мы создадим наш том TrueCrypt в папке *D:\My Documents* и присвоим тому (файлу-контейнеру) имя *My Volume* (как показано на иллюстрации выше). Разумеется, вы можете выбрать любое другое имя и размещение файла (например, поместив его на флэш-брелок USB). Обратите внимание, что файла *My Volume* пока не существует – TrueCrypt его создаст.

ВАЖНО: Имейте в виду, что TrueCrypt *не* будет шифровать никаких имеющихся файлов (при создании файла-контейнера TrueCrypt). Если на данном этапе выбрать какой-либо уже существующий файл, он будет перезаписан и заменён новым созданным томом (т. е. перезаписанный файл будет *уничтожен*, а *не* зашифрован). Зашифровать имеющиеся файлы вы сможете позднее путём перемещения их в том TrueCrypt, который мы сейчас создаём.[1]

Выберите в файловом окне желаемый путь (место, где вы хотите создать контейнер).

В поле **Имя файла** введите имя, которое вы хотите дать файлу-контейнеру.

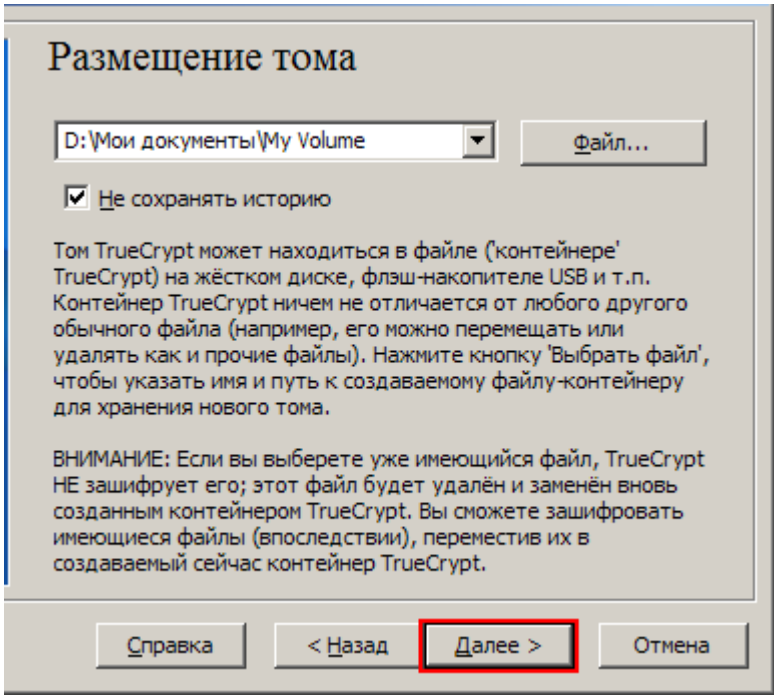
Нажмите кнопку **Сохранить**.

Файловое окно должно исчезнуть.

[1] Обратите внимание: после копирования имеющихся незашифрованных файлов в том TrueCrypt исходные файлы следует надёжно удалить (затереть) с помощью специализированных утилит (многие из них бесплатны).

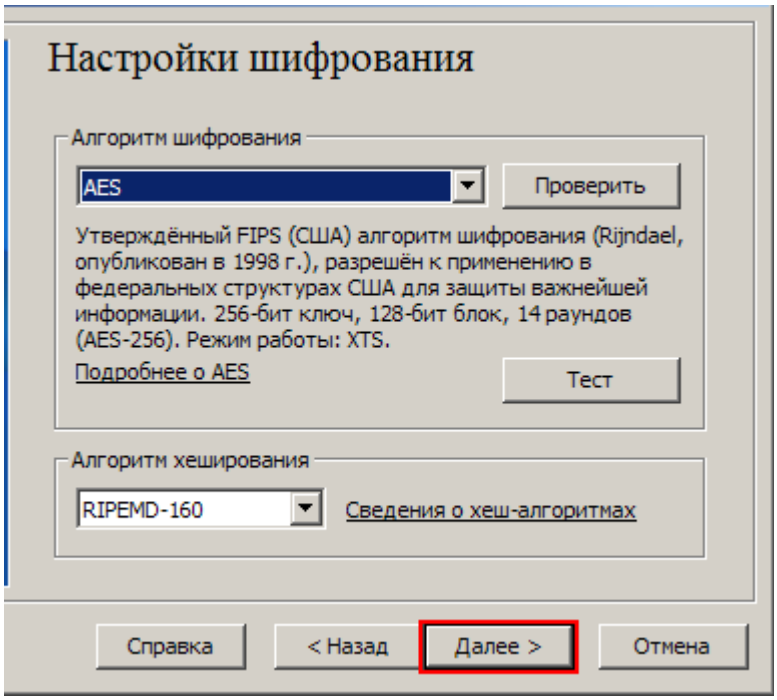
На следующих этапах мы вернёмся в окно мастера создания томов TrueCrypt.

Этап 7:



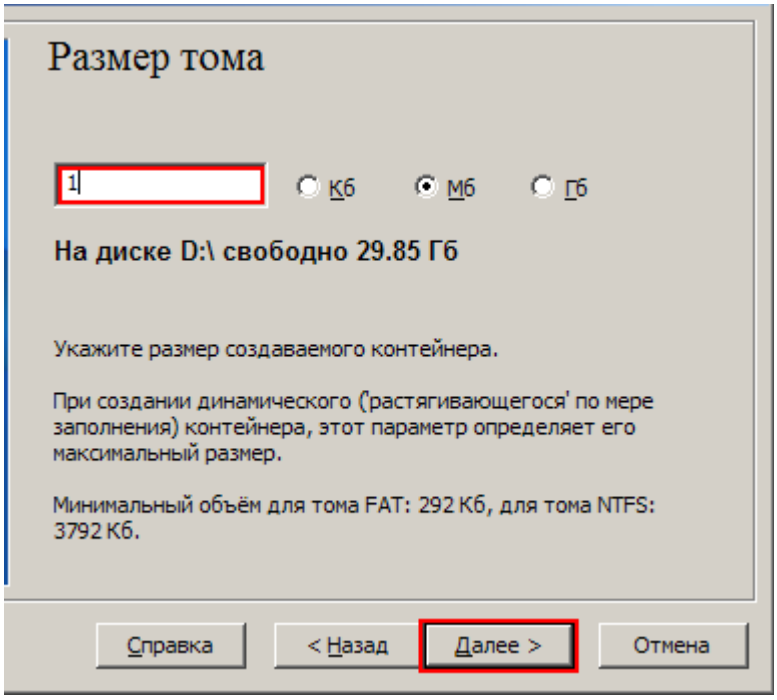
В окне мастера создания томов нажмите **Далее**.

Этап 8:



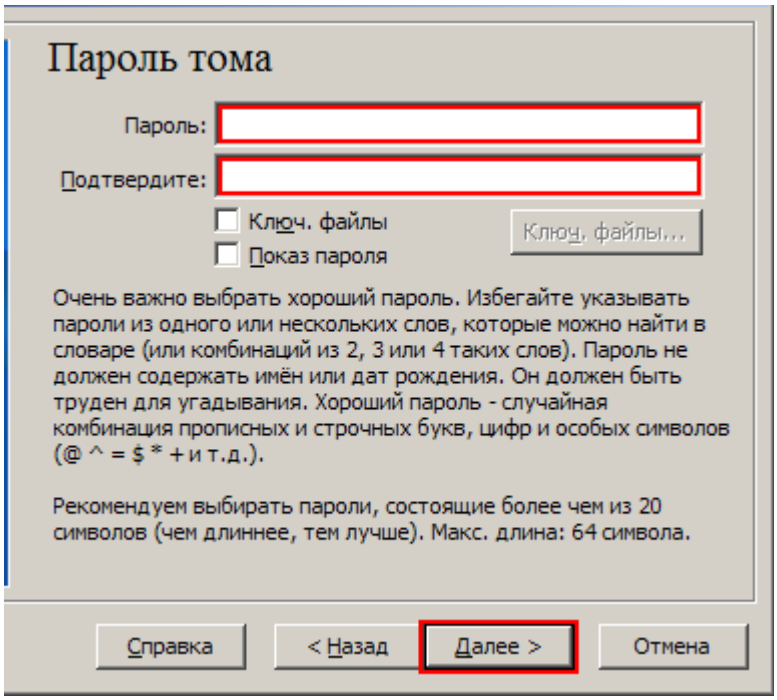
Здесь можно выбрать для тома алгоритмы шифрования и хеширования. Если вы не знаете, что лучше выбрать, просто оставьте предложенные значения и нажмите **Далее** (см. подробности в главах Алгоритмы шифрования и Алгоритмы хеширования).

Этап 9:



Здесь мы укажем, что хотим создать контейнер TrueCrypt размером 1 мегабайт. Разумеется, вы можете указать любой другой размер. После того, как вы введёте нужный вам размер в поле ввода (оно выделено красным), нажмите кнопку **Далее**.

Этап 10:



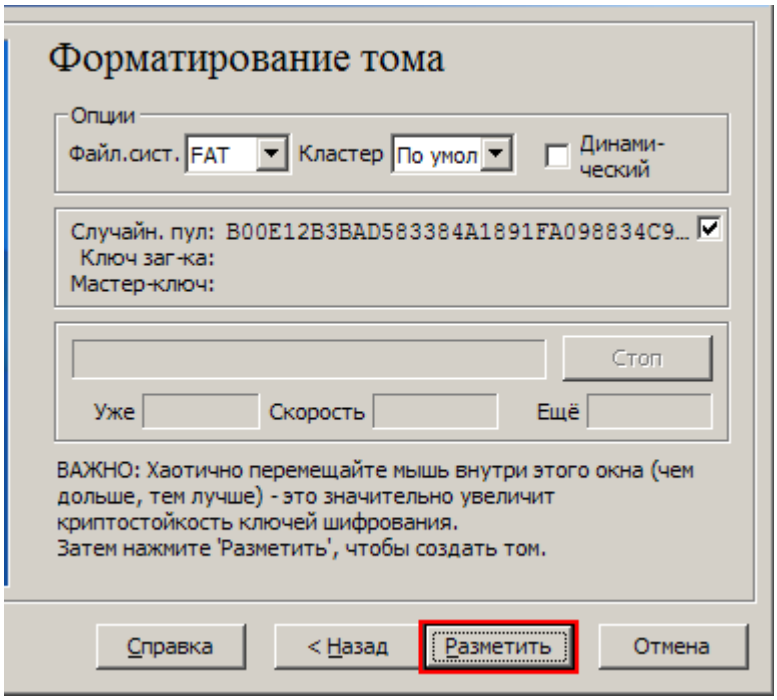
Мы подошли к одному из самых важных этапов: нам нужно выбрать для тома хороший пароль.

Какой пароль следует считать хорошим, написано в этом окне мастера. Внимательно прочитайте данную информацию.

После того, как вы определитесь с хорошим паролем, введите его в первое поле ввода. Затем введите тот же самый пароль в расположенное ниже второе поле ввода и нажмите кнопку **Далее**.

Примечание: кнопка **Далее** будет недоступна до тех пор, пока в полях ввода не будут введены одинаковые пароли.

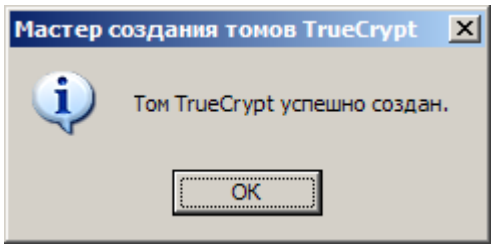
Этап 11:



Перемещайте мышь произвольным образом в окне мастера создания томов в течение хотя бы 30 секунд. Чем дольше вы будете перемещать мышь, тем лучше – этим вы значительно повысите криптостойкость ключей шифрования (что увеличит их надёжность).

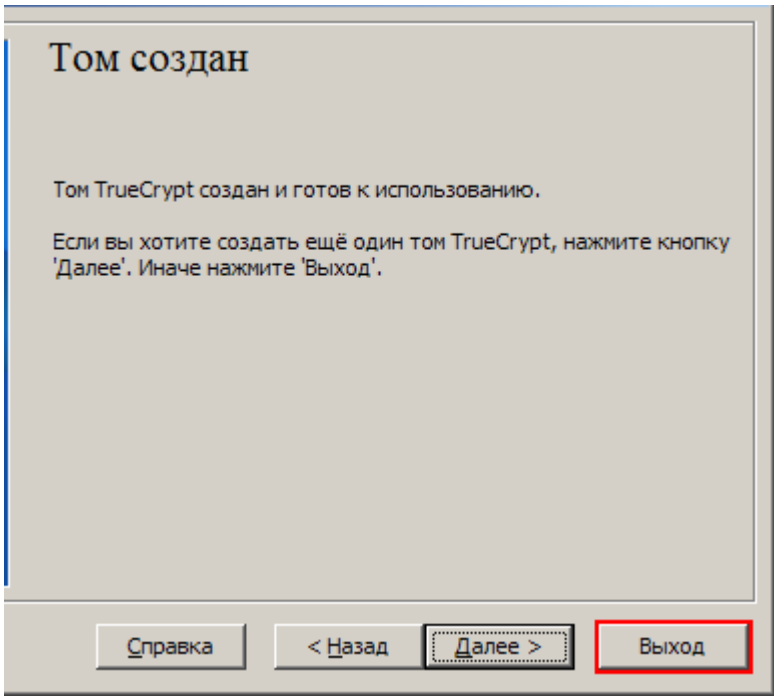
Нажмите кнопку **Разметить**.

Сейчас должно начаться создание тома. TrueCrypt создаст файл с именем *My Volume* в папке *D:\Мои документы* (как мы указали на этапе 6). Этот файл станет контейнером TrueCrypt (т. е. он будет содержать зашифрованный том TrueCrypt). В зависимости от размера тома, операция создание тома может длиться довольно долго. По окончании появится следующее диалоговое окно:



Нажмите **OK**, чтобы закрыть это окно.

Этап 12:



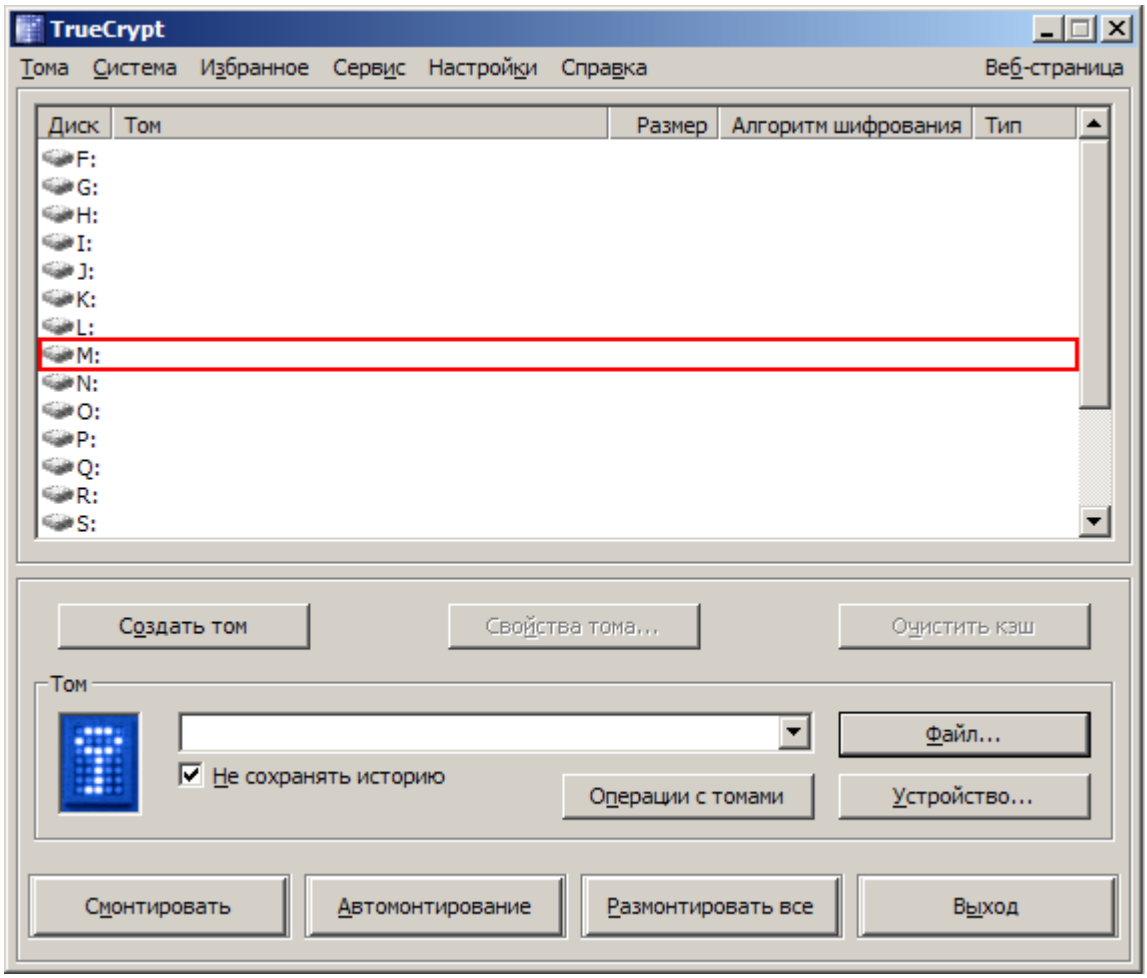
Итак, только что мы успешно создали том TrueCrypt (файл-контейнер).

Нажмите кнопку **Выход** в окне мастера создания томов TrueCrypt.

Окно мастера должно исчезнуть.

На следующих этапах мы смонтируем том, который только что создали. Сейчас мы должны были вернуться в главное окно TrueCrypt (которое должно быть всё ещё открыто, в противном случае выполните заново этап 1, чтобы запустить TrueCrypt, а затем перейдите к этапу 13).

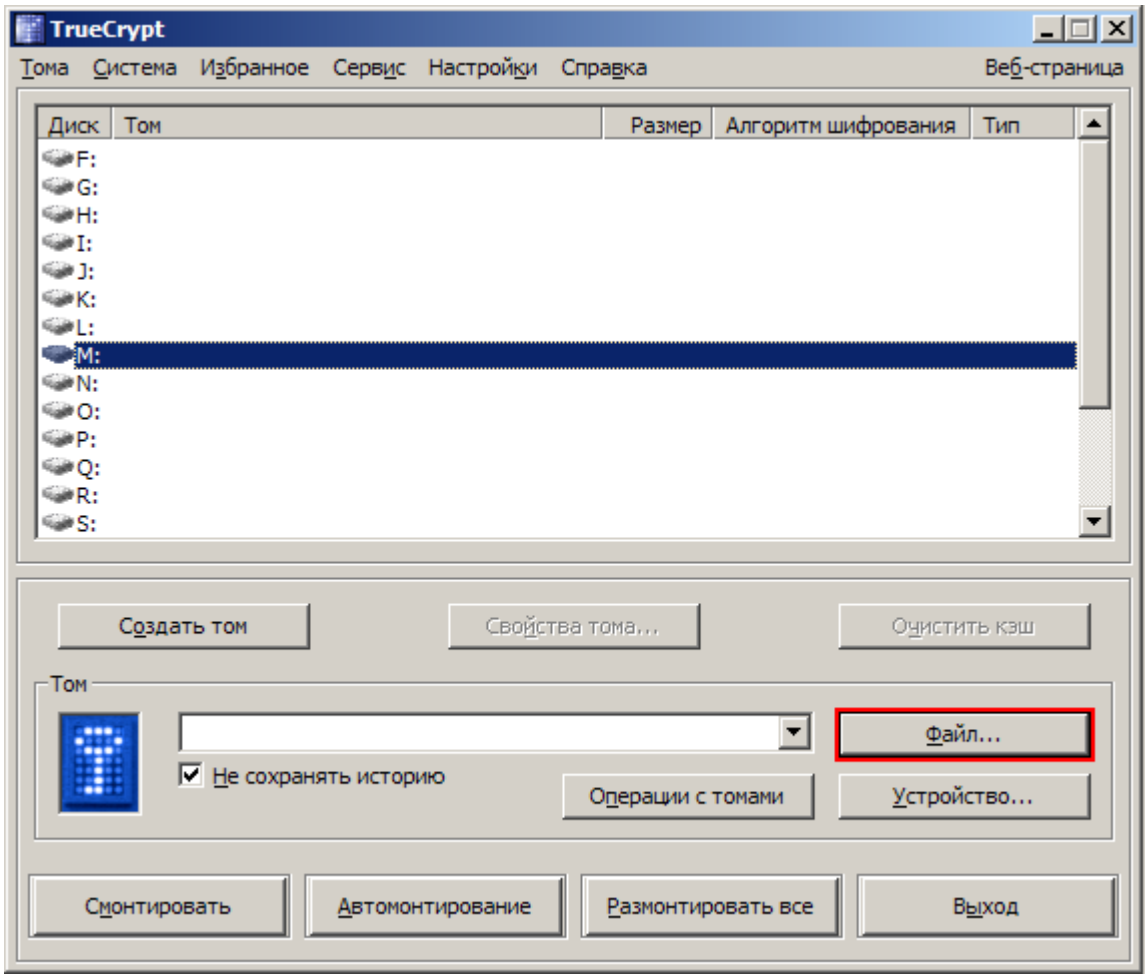
Этап 13:



Выберите в списке букву диска (на иллюстрации она помечена красным). Она станет буквой диска со смонтированным контейнером TrueCrypt.

Примечание: в нашем примере мы выбрали букву диска M, но вы, разумеется, можете выбрать любую другую доступную букву.

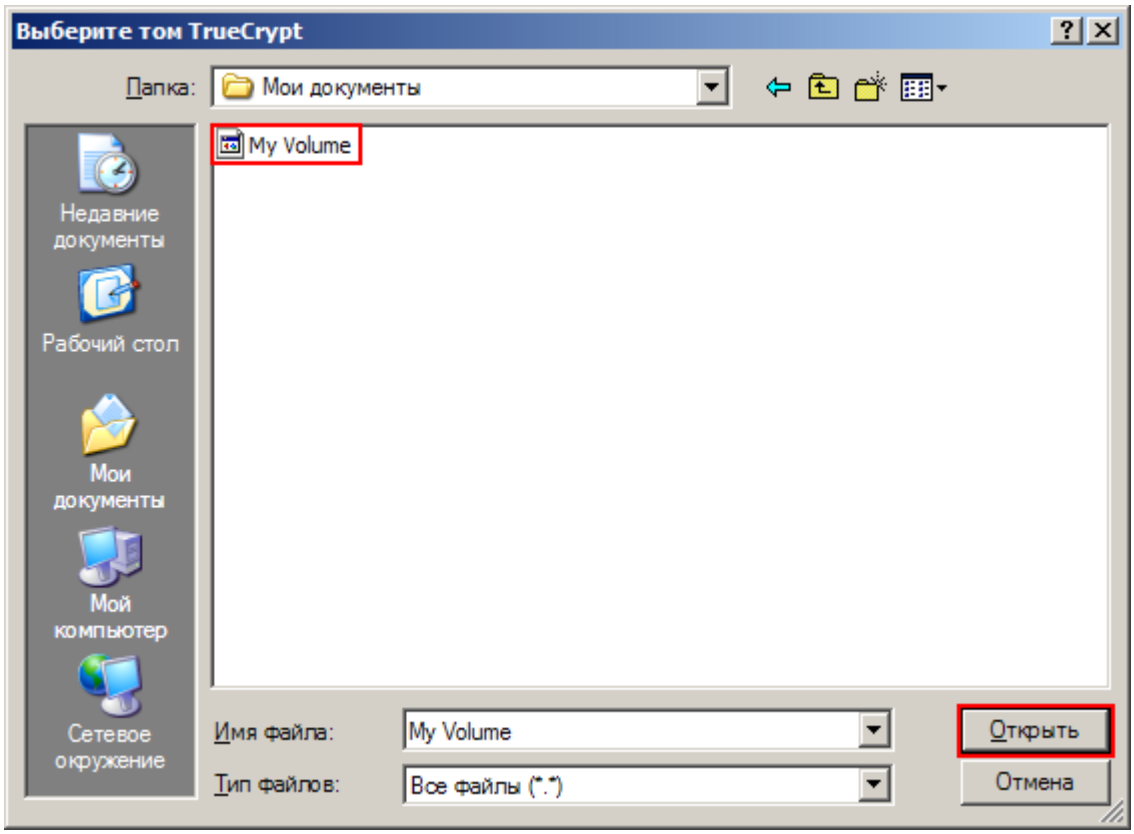
Этап 14:



Нажмите кнопку **Файл**.

Появится стандартное окно выбора файлов.

Этап 15:



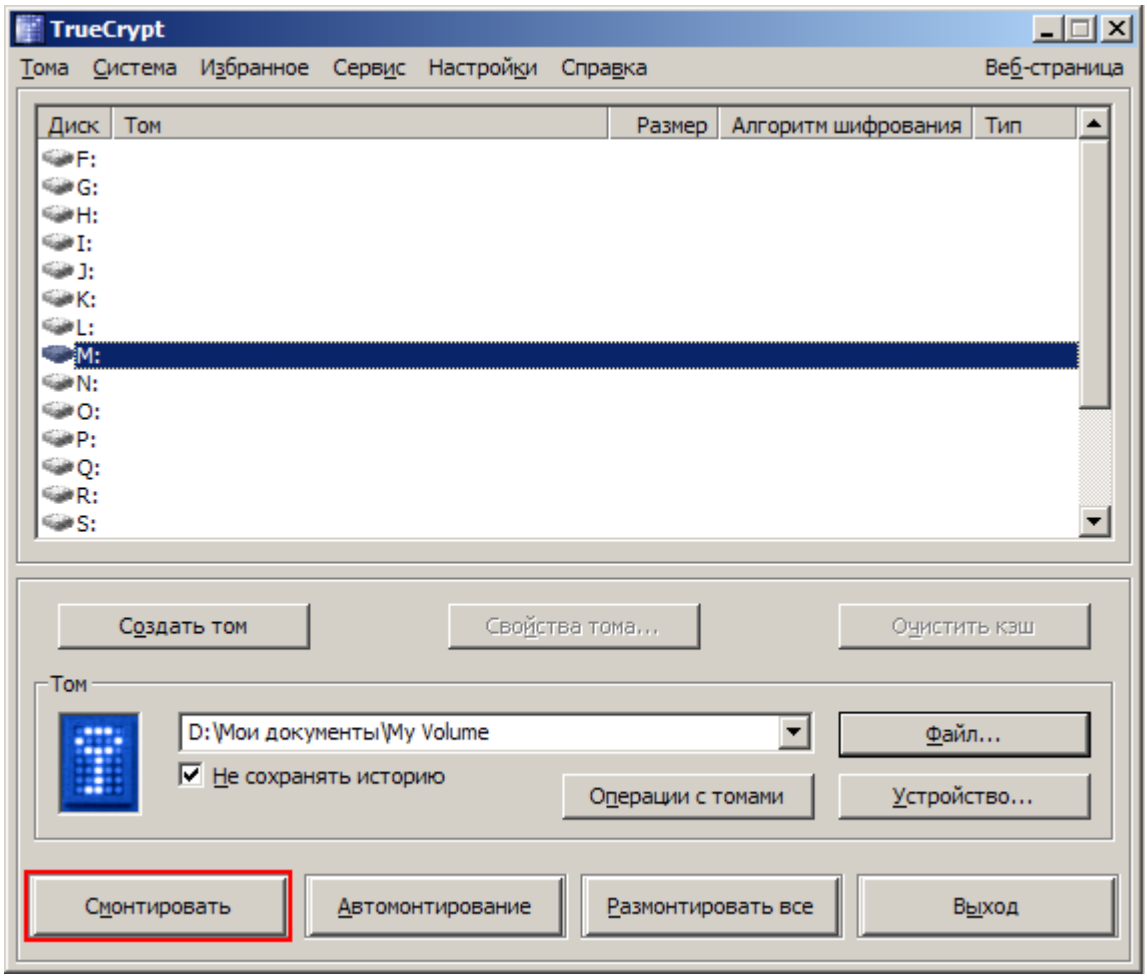
В окне выбора файлов найдите и укажите файл-контейнер (который мы создали на этапах 6-11).

Нажмите кнопку **Открыть** (в окне выбора файлов).

Окно выбора файлов должно при этом исчезнуть.

На следующих этапах мы вернёмся в главное окно TrueCrypt.

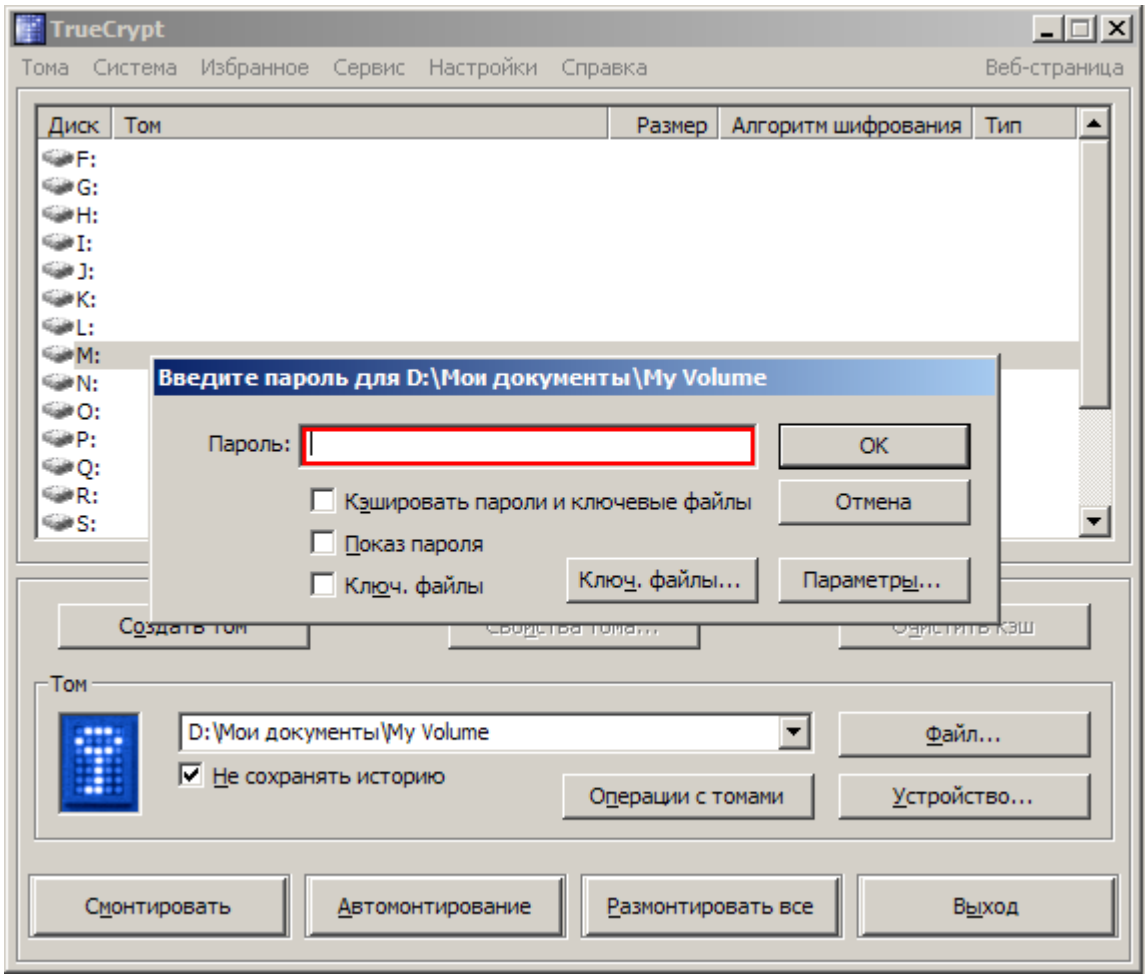
Этап 16:



В главном окне TrueCrypt нажмите кнопку **Смонтировать**.

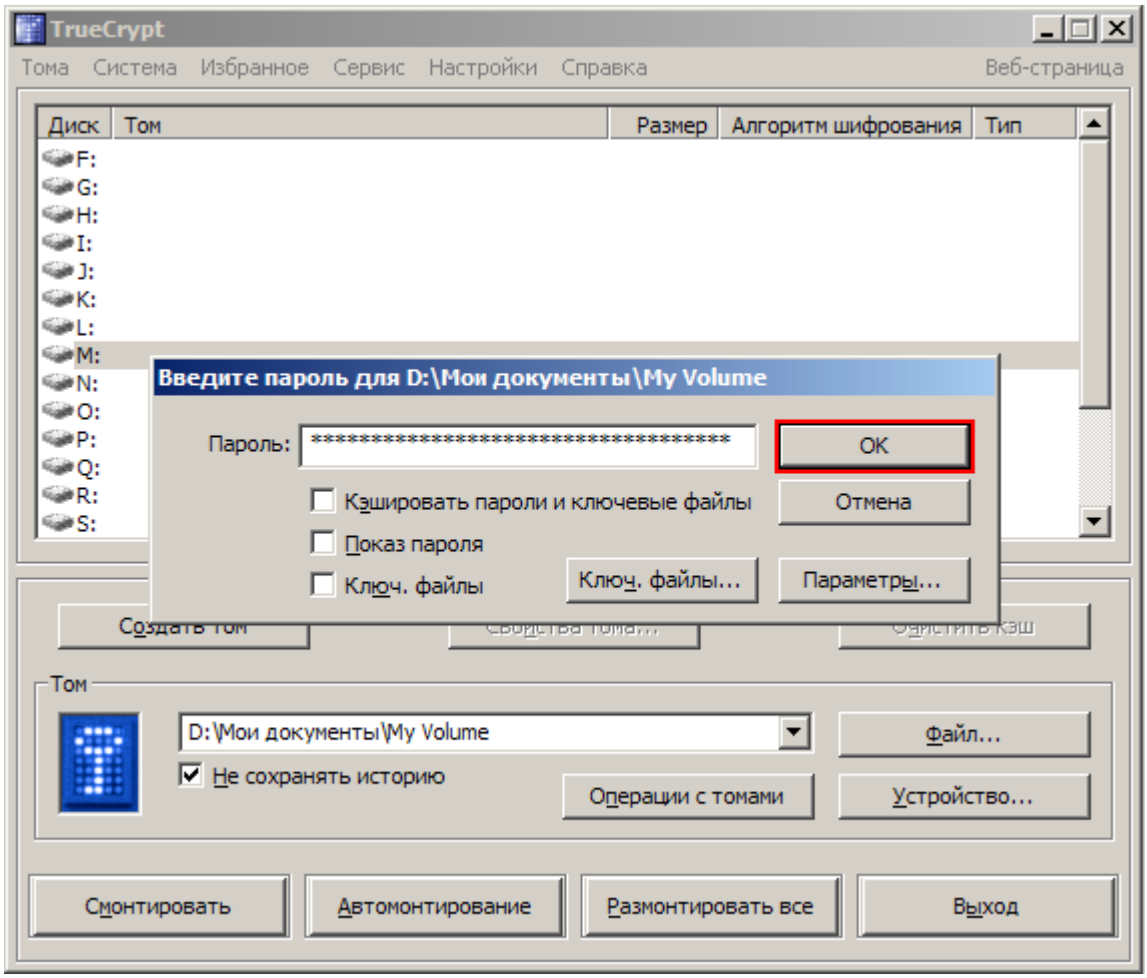
Появится диалоговое окно ввода пароля.

Этап 17:



Укажите пароль (который мы задали на этапе 10) в поле ввода (на иллюстрации оно помечено красным).

Этап 18:

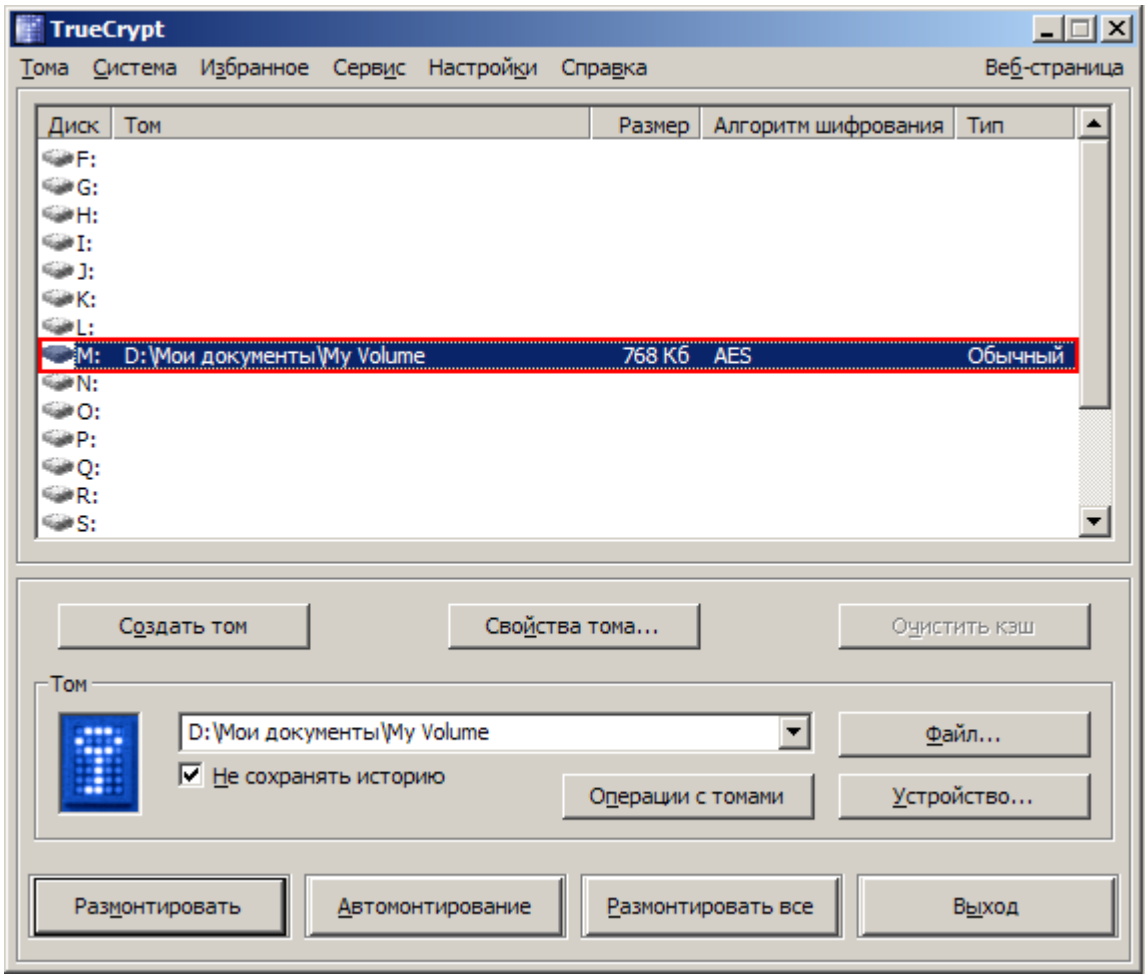


Нажмите **OK** в окне ввода пароля.

Сейчас TrueCrypt попытается смонтировать наш том. Если пароль указан неправильно (например, вы ошиблись при вводе), TrueCrypt известит вас об этом, и потребуется повторить предыдущий этап (снова ввести пароль и нажать **OK**). Если пароль правильный, то том будет смонтирован.

(См. продолжение на следующей странице.)

Заключительный этап:



Итак, мы только что успешно смонтировали контейнер как виртуальный диск M:

Этот виртуальный диск полностью зашифрован (в том числе зашифрованы имена файлов, таблицы распределения, свободное место и т.д.) и ведёт себя как настоящий диск. Вы можете сохранять (или копировать, перемещать и т.д.) файлы на этом виртуальном диске, они будут шифроваться на лету в момент записи.

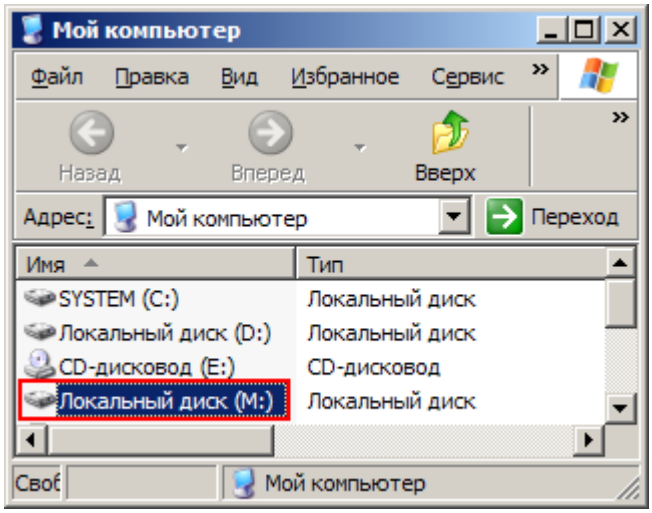
Например, если вы откроете файл, хранящийся в томе TrueCrypt, в медиапроигрывателе, этот файл будет автоматически расшифровываться в памяти (в ОЗУ) непосредственно в момент считывания, т. е. на лету.

ВАЖНО: Обратите внимание, что когда вы открываете файл, хранящийся в томе TrueCrypt (или когда сохраняете/копируете файл в томе TrueCrypt), повторный ввод пароля не запрашивается. Правильный пароль нужно указать только один раз – при монтировании тома.

Открыть смонтированный том можно, например, двойным щелчком по элементу, выделенному на иллюстрации красным цветом.

(См. продолжение на следующей странице.)

Просматривать содержимое смонтированного тома можно точно так же, как содержимое любого другого диска. Например, открыть ‘*Компьютер*’ (или ‘*Мой компьютер*’) и дважды щёлкнуть по соответствующей букве диска (в нашем случае это буква M).

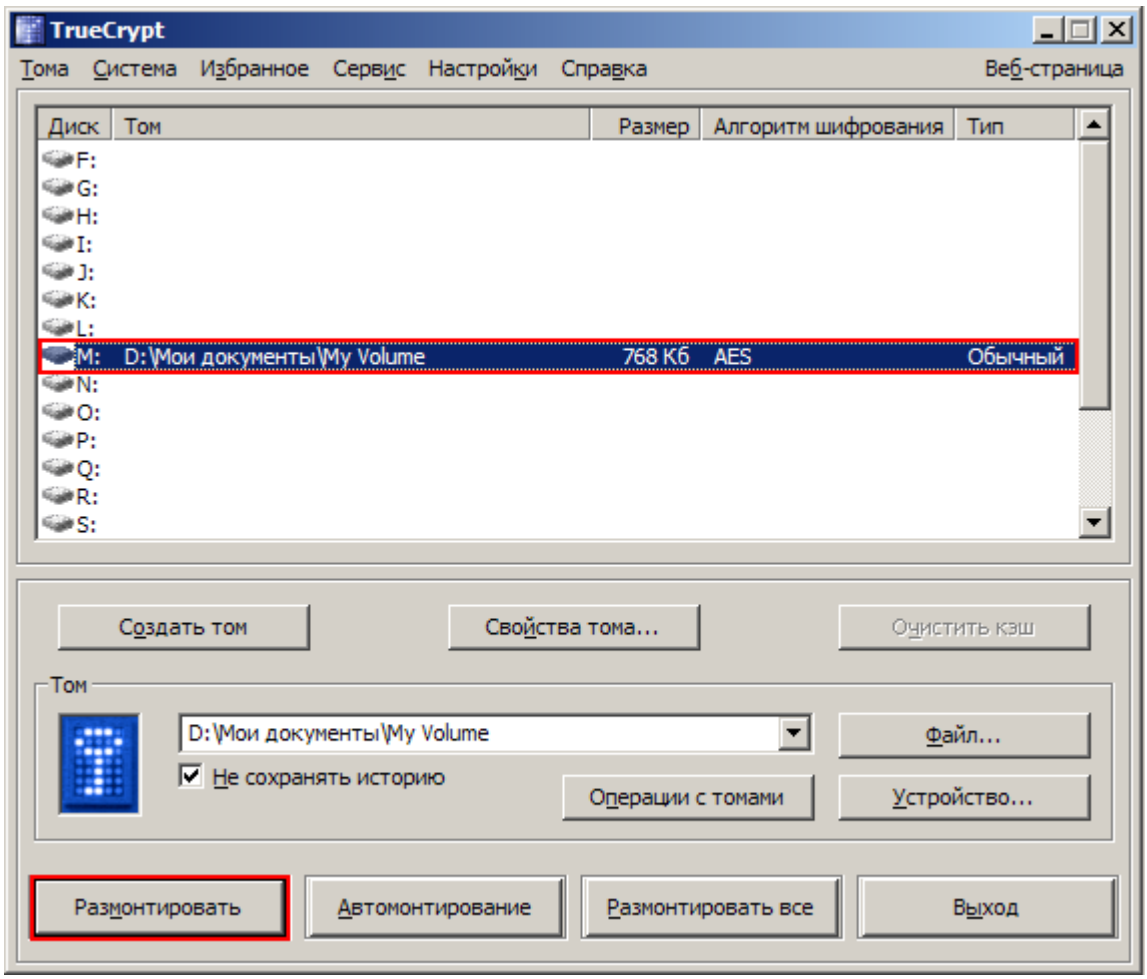


Вы можете копировать файлы (или папки) в/из том(а) TrueCrypt, как если бы вы копировали их в любой другой обычный диск (например, с помощью перетаскивания). Файлы, считываемые или копируемые из зашифрованного тома TrueCrypt, автоматически на лету расшифровываются в ОЗУ (в памяти). Аналогично, файлы, записываемые или копируемые в том TrueCrypt, автоматически зашифровываются на лету в ОЗУ (непосредственно перед их записью на диск).

Обратите внимание: TrueCrypt никогда не сохраняет на диске данные в незашифрованном виде – незашифрованные данные хранятся лишь временно в ОЗУ (памяти). Даже при смонтированном томе данные в этом томе остаются зашифрованными. При перезагрузке Windows или выключении компьютера том будет размонтирован, а все находящиеся в нём файлы станут недоступными (и зашифрованными). Даже в случае случайного перебоя электропитания (т. е. при некорректном завершении работы системы) все хранящиеся в томе файлы будут недоступными (и зашифрованными). Чтобы снова получить к ним доступ, потребуется смонтировать том. Как это сделать, описано на этапах 13-18.

(См. продолжение на следующей странице.)

Если вам нужно закрыть том, сделав его содержимое недоступным, можно либо перезагрузить операционную систему, либо размонтировать том. Чтобы это сделать, проделайте следующее:



Выберите нужный том из списка смонтированных томов в главном окне TrueCrypt (на иллюстрации он помечен красным) и нажмите кнопку **Размонтировать** (на иллюстрации она также помечена красным). Чтобы снова получить доступ к хранящимся в томе файлам, потребуется смонтировать том. Как это сделать, описано на этапах 13-18.

Как создать и использовать раздел/устройство, зашифрованное TrueCrypt

Вместо создания файлов-контейнеров вы можете воспользоваться шифрованием физических разделов или дисков (т. е. создавать тома TrueCrypt на основе устройств). Чтобы это сделать, повторите этапы 1-3, но на этапе 3 выберите второй или третий параметр и следуйте инструкциям мастера. При создании тома TrueCrypt на основе устройства внутри *несистемного* раздела/диска, монтирование этого тома выполняется кнопкой *Автомонтирование* в главном окне TrueCrypt. Сведения о зашифрованных *системных* разделах/дисках см. в главе *Шифрование системы*.

ВАЖНО: ***Настоятельно рекомендуем ознакомиться с другими главами этого руководства, так как они содержат важную информацию, которая здесь опущена из соображений простоты объяснения азов.***

Том TrueCrypt

Существует два типа томов TrueCrypt:

- на основе файла (контейнер)
- на основе раздела/устройства (несистемного)

Примечание: помимо создания виртуальных томов указанных выше типов, TrueCrypt также может шифровать физический раздел/диск, на котором установлена Windows (подробности см. в главе *Шифрование системы*).

Том TrueCrypt на основе файла представляет собой обычный файл, который может находиться на любом устройстве хранения данных. Он содержит полностью независимое зашифрованное виртуальное дисковое устройство.

Раздел TrueCrypt это раздел на жёстком диске, зашифрованный с помощью TrueCrypt. Также можно шифровать целиком жёсткие диски (в том числе подключаемые по USB), флэш-накопители USB («флэшки») и устройства хранения данных других типов.

Создание нового тома TrueCrypt

Чтобы создать том TrueCrypt на основе файла или чтобы зашифровать раздел/устройство (для этого требуются права администратора), нажмите кнопку ‘Создать том’ в главном окне программы. Появится окно мастера создания томов TrueCrypt. Сразу за этим мастер начнёт сбор данных для генерирования мастер-ключа, вторичного ключа (режим XTS) и соли для нового тома. В сборе данных, которые должны носить как можно более случайный характер, участвуют перемещения мыши, нажатие на клавиши и другая получаемая из системы информация (см. подробности в главе *Генератор случайных чисел*). При создании тома TrueCrypt мастер предоставляет необходимые подсказки, однако некоторые моменты требуют пояснения.

Алгоритм хеширования

Этот параметр позволяет указать хеш-алгоритм, который будет применять TrueCrypt. Выбранный алгоритм используется генератором случайных чисел (как функция псевдослучайного смешивания) для генерирования мастер-ключа, вторичного ключа (режим XTS) и соли (см. подробности в главе *Генератор случайных чисел*). Также он используется в получении (деривации) ключа заголовка тома и вторичного ключа заголовка (см. главу *Деривация ключа заголовка, соль и подсчёт итераций*).

Сведения о доступных хеш-алгоритмах приведены в главе *Алгоритмы хеширования.*

Обратите внимание: вывод хеш-функции *никогда* не используется непосредственно как ключ шифрования. Дополнительные сведения см. в главе *Технические подробности*.

Алгоритм шифрования

Этот параметр позволяет указать алгоритм шифрования, который будет применяться в новом томе. Обратите внимание, что выбранный алгоритм шифрования после создания тома изменить уже нельзя. Дополнительные сведения см. в главе *Алгоритмы шифрования*.

Быстрое форматирование

Если этот параметр выключен, форматированию подвергается каждый сектор нового тома. Это означает, что новый том будет *целиком* заполнен случайными данными. Быстрое форматирование занимает гораздо меньше времени, но оно менее надёжно, так как пока весь том не будет заполнен файлами, существует вероятность определить, как много данных он содержит (если свободное пространство не было предварительно заполнено случайными данными). Если вы не уверены, нужно ли вам включать или выключать быстрое форматирование, рекомендуем оставить этот параметр выключенным. Обратите внимание, что параметр 'Быстрое форматирование' доступен только при шифровании разделов/устройств.
ВАЖНО: При шифровании раздела/устройства, внутри которого вы планируете затем создать скрытый том, оставьте этот параметр выключенным.

Динамический («резиновый») том

Динамический контейнер TrueCrypt представляет собой предраспределённый разрежённый (sparse) файл NTFS, чей физический размер (реально занимаемое место на диске) увеличивается по мере добавления в контейнер новых данных. Обратите внимание, что физический размер контейнера (реально занимаемое контейнером место на диске) не уменьшается при удалении файлов из тома TrueCrypt. Физический размер контейнера может только *увеличиваться* до максимального значения, указанного пользователем при создании этого тома. По достижении указанного максимального значения физический размер тома будет оставаться постоянным.

Учтите, что разрежённые файлы можно создавать только в файловой системе NTFS. При создании контейнера в файловой системе FAT, параметр *Динамический* будет недоступен (“затенён”).

Имейте в виду, что размер динамического (на основе разрежённого файла) тома TrueCrypt, сообщаемый Windows и TrueCrypt, будет всегда равен его максимальному размеру (который был указан при создании этого тома). Чтобы узнать текущий физический размер контейнера (действительно занимаемое им место на диске), щёлкните правой кнопкой по файлу-контейнеру (в Проводнике Windows, не в TrueCrypt) и выберите пункт *Свойства* – в поле *На диске* будет указано реальное значение.

ВНИМАНИЕ: Скорость выполнения операций у динамических (на основе разрежённых файлов) томов TrueCrypt значительно ниже, чем у обычных томов. Кроме того, динамические тома TrueCrypt менее безопасны, так как они позволяют определить количество незанятых секторов в томе. Более того, если при записи данных на динамический том окажется, что в файловой системе, где находится файл-контейнер с данным томом, недостаточно свободного места, это может привести к повреждению зашифрованной файловой системы.

Размер кластера

Кластер это единица хранения данных. Например, один распределённый кластер в файловой системе FAT это однобайтовый файл. Когда файл увеличивается и превосходит границу кластера, распределяется ещё один кластер. В теории это означает, что чем больше размер кластера, тем больше тратится места на диске и тем выше производительность. Если вы не знаете, какой размер выбрать, используйте значение, предложенное по умолчанию.

Тома TrueCrypt на дисках CD/DVD

Если вы хотите сохранить том TrueCrypt на CD или DVD, сначала создайте на жёстком диске контейнер TrueCrypt на основе файла, а затем запишите («прожгите») его на CD/DVD с помощью любой программы для записи CD/DVD (в среде Windows XP и более новых версий Windows для этого можно воспользоваться средством записи CD, входящим в комплект поставки этой ОС). Имейте в виду, что если вы собираетесь монтировать том TrueCrypt, хранящийся на носителе, допускающим только чтение (таком, как CD/DVD), в среде Windows 2000, том TrueCrypt должен иметь формат FAT. Причина этого в том, что Windows 2000 не может монтировать файловую систему NTFS на носителях только для чтения (в отличие от Windows XP и более новых версий Windows).

Аппаратный/программный RAID, динамические тома Windows

TrueCrypt поддерживает аппаратные/программные массивы RAID, а также динамические тома Windows.

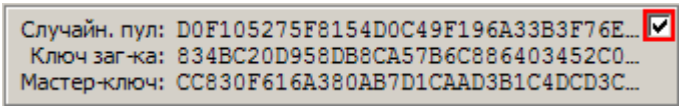
Windows Vista и новее: динамические тома отображаются в диалоговом окне выбора устройства
как `\Device\HarddiskVolume`*N*.

Windows XP/2000/2003: если вы намереваетесь отформатировать динамический том Windows как том TrueCrypt, помните, что после того, как вы создадите динамический том Windows (с помощью Windows-средства «Управление дисками»), нужно перезагрузить операционную систему, чтобы том стал доступен/виден в диалоговом окне выбора устройства в мастере создания томов TrueCrypt. Также учтите, что в диалоговом окне выбора устройства динамический диск Windows *не* отображается как одно устройство (элемент). Вместо этого выводятся *все* тома, из которых состоит динамический том Windows, и вы можете выбрать *любой* из них, чтобы отформатировать *весь* динамический том Windows.

Примечания к созданию томов

После нажатия кнопки ‘Разметить’ в окне мастера создания томов (последний этап), последует небольшая задержка, в течение которой система собирает дополнительные случайные данные. Затем для нового тома генерируются мастер-ключ, ключ заголовка, вторичный ключ (режим XTS) и соль с показом содержимого мастер-ключа и ключа заголовка.

Для большей безопасности можно отключить вывод на экран частей содержимого пула случайных чисел, мастер-ключа и ключа заголовка, сняв отметку в правом верхнем углу соответствующего поля:



Примечание: отображаются только первые 128 бит пула/ключей (а не всё содержимое).

Можно создавать тома FAT (стандартов FAT12, FAT16 и FAT32 или определяемые автоматически по количеству кластеров) или NTFS (однако нужно иметь в виду, что тома NTFS могу создавать только пользователи с правами администратора). Смонтированные тома TrueCrypt можно в любое время переформатировать в FAT12, FAT16, FAT32 или в NTFS. Они ведут себя точно так же, как стандартные дисковые устройства, поэтому можно щёлкнуть правой кнопкой мыши по значку смонтированного тома TrueCrypt (например, в окне ‘*Компьютер*’ или ‘*Мой компьютер*’) и выбрать команду ‘Форматировать’.

Более подробные сведения о создании томов TrueCrypt см. в разделе *Скрытый том*.

Избранные тома

Избранные тома удобны во многих случаях. Например, если у вас есть:

- том, который всегда должен **монтироваться на конкретную букву диска**;
- том, который нужно **автоматически монтировать при подключении к компьютеру устройства с этим томом** (скажем, контейнер, находящийся на флэш-накопителе USB или внешнем жёстком диске, подключаемом по шине USB);
- том, который нужно **автоматически монтировать при входе в вашу учётную запись** в операционной системе;
- том, который нужно всегда **монтировать только для чтения** или **как сменный носитель**.

Чтобы сконфигурировать том TrueCrypt как избранный, проделайте следующее:

1. Смонтируйте том (на ту букву диска, на которую вы хотите его монтировать всегда).
2. В главном окне TrueCrypt щёлкните правой кнопкой мыши по смонтированному тому и выберите команду *Добавить в избранные*.
3. В появившемся окне упорядочивания избранных томов выберите нужные параметры для этого тома (см. ниже).
4. Нажмите кнопку *OK*.

Избранные тома можно монтировать несколькими разными способами. Чтобы смонтировать все избранные тома, в меню *Избранное* выберите команду *Смонтировать избранные тома* или нажмите горячую клавишу монтирования избранных томов (*Настройки* > *Горячие клавиши*). Если нужно смонтировать только один из избранных томов, выберите его из списка в меню *Избранное*. При этом вам будет нужно ввести для данного тома пароль (и/или ключевые файлы) (если только он не находится в кэше). В случае правильного ввода том будет смонтирован и открыт в окне Проводника.

Избранные тома (только указанные или все) можно автоматически монтировать при каждом входе в Windows. Чтобы настроить это, проделайте следующее:

1. Смонтируйте том, который должен автоматически монтироваться при вашем входе в свою учётную запись Windows (на ту букву, на которую нужно, чтобы он монтировался всегда).
2. В главном окне TrueCrypt щёлкните правой кнопкой мыши на смонтированном томе и выберите команду *Добавить в избранные*.
3. В появившемся окне упорядочивания избранных томов включите параметр *Монтировать выбранный том при входе в систему* и нажмите *OK*.

Теперь при каждом входе в Windows вам будет нужно указывать для тома пароль (и/или ключевые файлы), и если данные введены правильно, том будет смонтирован.

Примечание: TrueCrypt не будет спрашивать пароль, если у вас включено кэширование

(запоминание) пароля дозагрузочной аутентификации (*Настройки* > *Шифрование системы*), а пароль у тома такой же, как и у системного раздела/диска.
Избранные тома (только указанные или все) можно автоматически монтировать при подключении к компьютеру устройства, на котором они расположены. Чтобы настроить это, проделайте следующее:

1. Смонтируйте том (на ту букву, на которую нужно, чтобы он монтировался всегда).
2. В главном окне TrueCrypt щёлкните правой кнопкой мыши на смонтированном томе и выберите команду *Добавить в избранные*.
3. В появившемся окне упорядочивания избранных томов включите параметр *Монтировать выбранный том при подключении устройства, на котором он расположен* и нажмите *OK*.

Теперь всякий раз, когда вы будете, например, вставлять в USB-порт компьютера флэш-накопитель USB с томом TrueCrypt, вам будет выдаваться запрос пароля (и/или ключевых файлов) (если только он не кэширован), и если данные введены правильно, том будет смонтирован.

Примечание: TrueCrypt не будет спрашивать пароль, если у вас включено кэширование (запоминание) пароля дозагрузочной аутентификации (*Настройки* > '*Шифрование системы*'), а у тома такой же пароль, как и у системного раздела/диска.

Каждому избранному тому можно присвоить особую метку. Эта метка – не то же самое, что метка тома в файловой системе, она отображается внутри интерфейса TrueCrypt вместо пути тома. Чтобы присвоить тому метку, проделайте следующее:

1. В меню *Избранное* выберите команду *Упорядочить избранные тома*.
2. В появившемся окне упорядочивания избранных томов выберите том, метку которого вы хотите отредактировать.
3. Введите метку в поле *Метка выбранного избранного тома* и нажмите *OK*.

Обратите внимание, что в окне упорядочивания избранных томов (*Избранное* > *Упорядочить избранные тома*) можно **настроить ряд других параметров для каждого избранного тома**. Например, любой том можно монтировать как доступный только для чтения или как сменный носитель. Чтобы это сделать, выполните следующее:

1. В меню *Избранное* выберите команду *Упорядочить избранные тома*.
2. В появившемся окне упорядочивания избранных томов выберите том, параметры которого вы хотите настроить.
3. Выберите нужные вам установки и нажмите *OK*.

Системные избранные тома отображаются в окне упорядочивания избранного (*Избранное* > *Упорядочить избранные тома*) в **порядке их монтирования**, когда вы выбираете команду *Избранное* > *Смонтировать избранные тома* или нажимаете соответствующую горячую клавишу (*Настройки* > *Горячие клавиши*). Чтобы изменить порядок отображения томов, используйте кнопки *Выше* и *Ниже*.

Обратите внимание, что избранный том может также быть **разделом внутри области действия ключа шифрования системы, смонтированного без дозагрузочной аутентификации** (пример: раздел на зашифрованном системном диске с другой операционной системой, которая сейчас не загружена). Когда вы монтируете такой том и добавляете его в избранные, больше не нужно выбирать команду *Система* > *Смонтировать без дозагрузочной аутентификации* или включать параметр монтирования

раздела с шифрованием системы без дозагрузочной аутентификации. Вы можете просто смонтировать избранный том (как объяснено выше) без установки каких-либо параметров, поскольку режим монтирования тома сохранён в конфигурационном файле со списком ваших избранных томов.

ВНИМАНИЕ: Если присвоенная избранному тому (сохранённая в конфигурационном файле) буква диска занята, данный том не будет смонтирован, при этом сообщение об ошибке не выводится.

Чтобы **удалить том из списка избранных**, в меню *Избранное* выберите команду *Упорядочить избранные тома*, выделите нужный том, нажмите кнопку *Убрать* и затем нажмите *OK*.

Системные избранные тома

Системные избранные тома удобны, например, в следующих ситуациях:

- у вас есть тома, которые нужно **монтировать до загрузки системы и служб приложений и перед входом пользователей в систему**;
- у вас есть совместно используемые в сети папки, расположенные в томах TrueCrypt; настроив такие тома как системные избранные, вы тем самым гарантируете, что **совместно используемые по сети ресурсы будут автоматически восстанавливаться** операционной системой при каждой перезагрузке;
- вам нужно, чтобы такой том монтировался на **одну и ту же букву диска** при каждой загрузке операционной системы.

Обратите внимание, что в отличие от обычных (несистемных) избранных томов, **системные избранные тома используют пароль дозагрузочной аутентификации**, поэтому необходимо, чтобы системный раздел/диск был зашифрован (также примите к сведению, что включать кэширование пароля дозагрузочной аутентификации не требуется).

Системные избранные тома можно настроить так, чтобы они были **доступны из TrueCrypt только пользователям с правами администратора** (выберите *Настройки* > *Системные избранные тома* > *Просматривать/размонтировать системные избранные тома могут лишь администраторы*). Этот параметр следует включать при использовании на серверах, чтобы предотвратить возможность размонтирования системных избранных томов пользователями без административных привилегий. На не-серверных системах этот параметр можно использовать для того, чтобы системные избранные тома не влияли на действия с обычными томами (такими, как *Размонтировать все*, авторазмонтирование и т.д.). Кроме того, в случае запуска TrueCrypt без прав администратора (а это стандартное поведение в Windows Vista и более новых версиях Windows) системные избранные тома не отображаются в списке букв дисков в главном окне TrueCrypt.

Чтобы сконфигурировать том **TrueCrypt** как системный избранный, проделайте следующее**:**

1. Смонтируйте том (на ту букву, на которую нужно, чтобы он монтировался всегда).
2. В главном окне TrueCrypt щёлкните правой кнопкой мыши на смонтированном томе и выберите команду *Добавить в системные избранные*.
3. В появившемся окне упорядочивания системных избранных томов включите параметр *Монтировать системные избранные тома при старте Windows* и нажмите *OK*.

Системные избранные тома отображаются в окне упорядочивания избранного (*Избранное* > *Упорядочить системные избранные тома*) в **порядке их монтирования**. Чтобы изменить порядок отображения томов, используйте кнопки *Выше* и *Ниже*.

Каждому системному избранному тому можно присвоить особую метку. Эта метка – не то же самое, что метка тома в файловой системе, она отображается внутри интерфейса TrueCrypt вместо пути тома. Чтобы присвоить тому метку, проделайте следующее:

1. В меню *Избранное* выберите команду *Упорядочить системные избранные тома*.
2. В появившемся окне упорядочивания системных избранных томов выберите том, метку которого вы хотите отредактировать.
3. Введите метку в поле *Метка выбранного избранного тома* и нажмите *OK*.

Обратите внимание, что в окне упорядочивания системных избранных томов (*Избранное* > *Упорядочить системные избранные тома*) можно **настроить ряд других параметров для каждого системного избранного тома**. Например, любой том можно монтировать как доступный только для чтения или как сменный носитель.

ВНИМАНИЕ: Если присвоенная системному избранному тому (сохранённая в конфигурационном файле) буква диска занята, данный том не будет смонтирован, при этом сообщение об ошибке не выводится.

Обратите внимание, что Windows требуется использовать ряд файлов (например, файлы подкачки, файлы Active Directory и др.) до того, как будут смонтированы системные избранные тома. Поэтому такие файлы нельзя хранить на системных избранных томах. Тем не менее, их *можно* хранить на любом разделе, который входит в область действия шифрования системы (например, на системном разделе или на любом разделе системного диска, целиком зашифрованного с помощью TrueCrypt).

Чтобы **удалить том из списка системных избранных**, в меню *Избранное* выберите команду *Упорядочить системные избранные тома*, выделите нужный том, нажмите кнопку *Убрать* и затем нажмите *OK*.

Шифрование системы

TrueCrypt позволяет на лету шифровать системный раздел или весь системный диск, т. е. раздел или диск, где установлена Windows и с которого она загружается.

Шифрование системы обеспечивает наивысший уровень надёжности и безопасности, так как все файлы, включая любые временные файлы, создаваемые Windows и приложениями в системном разделе (как правило, без вашего ведома и согласия), файлы гибернации, файлы подкачки и т. д., всегда остаются зашифрованными (даже при случайном пропадании питания). Кроме того, Windows записывает множество данных, которые потенциально могут нести конфиденциальную нагрузку, например, имена и пути открываемых вами файлов, запускаемые вами программы и др. Все такие файлы-протоколы и записи в реестре также всегда остаются зашифрованными.

Шифрование системы включает в себя дозагрузочную аутентификацию,означающую, что любому пользователю для получения доступа, возможности работы в зашифрованной системе, чтения и записи файлов на системном диске и т. д. будет нужно вводить правильный пароль перед каждой загрузкой (стартом) Windows. Дозагрузочную аутентификацию обеспечивает загрузчик TrueCrypt (Boot Loader), расположенный в первой дорожке загрузочного диска и на диске восстановления TrueCrypt (Rescue Disk, см. далее).

Обратите внимание, что TrueCrypt выполняет шифрование имеющегося незашифрованного системного раздела/диска «на месте», т. е. прямо при работе операционной системы (во время шифрования системы можно продолжать пользоваться компьютером как обычно, без каких-либо ограничений). Аналогично, зашифрованный с помощью TrueCrypt системный раздел/диск можно дешифровать «на месте», во время работы операционной системы. Процесс шифрования/дешифрования можно прервать в любой момент, оставить раздел/диск частично незашифрованным, перезагрузить или выключить компьютер, а затем возобновить операцию с той точки, в которой она была остановлена.

При шифровании системы применяется режим XTS (см. раздел *Режимы операции*). Технические детали шифрования системы см. в разделе *Схема шифрования* в главе *Технические подробности*.

Чтобы зашифровать системный раздел или весь системный диск, в меню *Система* выберите команду *Зашифровать системный раздел/диск* и следуйте инструкциям мастера. Чтобы дешифровать системный раздел/диск, в меню *Система* выберите команду *Перманентно расшифровать системный раздел/диск*.

Примечание: Windows 7 и более новые версии Windows по умолчанию загружаются с особого маленького раздела. Этот раздел содержит файлы, необходимые для загрузки системы. Право записи в этот раздел Windows даёт только приложениям с административными привилегиями (при работе системы). TrueCrypt выполняет шифрование этого раздела, только если вы выбрали шифрование всего системного диска (а не шифрование только раздела, в котором установлена Windows).

Скрытая операционная система

Возможны ситуации, когда кто-то вынудит вас расшифровать операционную систему. Зачастую вы просто не сможете этому воспротивиться (например, при вымогательстве). На этот случай TrueCrypt позволяет создать скрытую операционную систему, наличие которой должно быть невозможно доказать (при условии соблюдения некоторых правил). Таким образом, вам не потребуется расшифровывать скрытую операционную систему или сообщать от неё пароль. Подробности см. в разделе *Скрытая операционная система* в главе *Правдоподобное отрицание причастности*.

Операционные системы, поддерживающие системное шифрование

Примечание: после того как была выпущена эта версия TrueCrypt, могла появиться новая версия операционной системы, проверенная на полную совместимость с TrueCrypt. Поэтому если это самая новая стабильная версия TrueCrypt, вам следует ознакомиться с онлайн-вариантом данной главы по адресу:
http://www.truecrypt.org/docs/?s=sys-encryption-supported-os

В настоящий момент TrueCrypt может зашифровывать следующие операционные системы:

- Windows 7 (32- и 64-разрядная версии)
- Windows Vista (SP1 и новее)
- Windows Vista x64 (64-разрядная версия) (SP1 и новее)
- Windows XP
- Windows XP x64 (64-разрядная версия)
- Windows Server 2008 R2 (64-разрядная версия)
- Windows Server 2008
- Windows Server 2008 x64 (64-разрядная версия)
- Windows Server 2003
- Windows Server 2003 x64 (64-разрядная версия)

Примечание
Помимо прочих, не поддерживаются следующие операционные системы: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, а также встраиваемые/планшетные версии Windows.

См. также раздел *Операционные системы, поддерживающие системное шифрование*.

Диск восстановления TrueCrypt (Rescue Disk)

При подготовке к шифрованию системного раздела/диска TrueCrypt требует, чтобы вы создали так называемый диск восстановления TrueCrypt (на CD/DVD). Он нужен в следующих случаях:

- Если экран загрузчика TrueCrypt не появляется при старте компьютера (или если не загружается Windows), **возможно повреждение загрузчика TrueCrypt**. С помощью диска восстановления TrueCrypt загрузчик можно восстановить и, таким образом, вернуть доступ к зашифрованной системе и данным (при этом, однако, вам всё равно будет нужно ввести правильный пароль). На экране диска восстановления выберите

Repair Options > *Restore TrueCrypt Boot Loader*. Затем нажмите ‘Y’ для подтверждения действия, извлеките диск восстановления из CD/DVD-накопителя и перезагрузите компьютер.

- Если **загрузчик TrueCrypt часто повреждается** (например, из-за неаккуратно написанного ПО активации) или если **нужно, чтобы на жёстком диске не было загрузчика TrueCrypt** (например, если вы хотите использовать альтернативный загрузчик/диспетчер для других операционных систем), в этом случае можно загружаться непосредственно с диска восстановления TrueCrypt (поскольку он также содержит загрузчик TrueCrypt) без восстановления загрузчика на жёстком диске. Просто вставьте диск восстановления в CD/DVD-накопитель и введите на его экране пароль.

- Если вы вводите правильный пароль, но TrueCrypt говорит, что пароль неверный, возможно **повреждение мастер-ключа или других важных данных**. Диск восстановления TrueCrypt позволяет их восстановить и, таким образом, вернуть доступ к зашифрованной системе и данным (разумеется, при этом вам будет нужно ввести правильный пароль). На экране диска восстановления выберите *Repair Options* > *Restore key data*. Затем введите пароль и нажмите ‘Y’ для подтверждения действия, извлеките диск восстановления из CD/DVD-накопителя и перезагрузите компьютер.

  Примечание: данную функцию нельзя использовать для восстановления заголовка скрытого тома, находящегося внутри скрытой операционной системы (см. раздел *Скрытая операционная система*). Чтобы восстановить заголовок такого тома, нажмите кнопку *Устройство*, выберите раздел, следующий за разделом с обманной системой, нажмите *OK*, выберите *Сервис -> Восстановить заголовок тома* и следуйте инструкциям.

  ВНИМАНИЕ: При восстановлении ключевых данных с помощью диска восстановления TrueCrypt также происходит восстановление пароля, который был действителен на момент создания диска восстановления TrueCrypt. Поэтому при каждой смене пароля необходимо уничтожать ранее созданный диск восстановления TrueCrypt и создавать новый (для этого нужно выбрать *Система -> Создать диск восстановления*). В противном случае, если неприятель знает ваш старый пароль (например, он получил его с помощью одной из клавиатурных программ-перехватчиков) и найдёт ваш старый диск восстановления TrueCrypt, он сможет воспользоваться им для восстановления ключевых данных (мастер-ключа, зашифрованного старым паролем) и, следовательно, расшифровать ваш системный раздел/диск.

- Если **Windows повреждена и не может загрузиться**, с помощью диска восстановления TrueCrypt можно перманентно расшифровать раздел/диск до начала загрузки Windows. На экране диска восстановления выберите *Repair Options* > *Permanently decrypt system partition/drive*. Введите правильный пароль и дождитесь завершения операции дешифрования. После этого вы сможете, например, загрузиться с установочного CD/DVD-диска Windows, чтобы исправить установку системы. Обратите внимание, что эта функция неприменима для дешифрования скрытого тома внутри скрытой операционной системы (см. раздел *Скрытая операционная система*).

  Примечание: в случае повреждения Windows (невозможности загрузки) её также можно восстановить (или получить доступ к хранящимся в ней файлам), не прибегая

к дешифрованию системного раздела/диска. Для этого нужно проделать следующее. Если у вас в компьютере несколько операционных систем, загрузите ту, которая не требует дозагрузочной аутентификации. Если в компьютере всего одна операционная система, можно загрузиться с помощью CD/DVD-диска с WinPE или BartPE либо подключить системный диск как вторичный/внешний диск к другому компьютеру и загрузить операционную систему, установленную на том компьютере. После загрузки системы запустите TrueCrypt, нажмите кнопку *Устройство*, выберите интересующий вас системный раздел, нажмите *OK*, выберите *Система > Смонтировать без дозагрузочной аутентификации*, введите свой пароль дозагрузочной аутентификации и нажмите *OK*. Этот раздел будет смонтирован как обычный том TrueCrypt (т. е. данные будут расшифровываться/шифроваться на лету в ОЗУ, как и всегда).

- Ваш диск восстановления TrueCrypt содержит **резервную копию исходного содержимого первой дорожки диска** (сделанную до того, как туда был прописан загрузчик TrueCrypt) и позволяет в случае необходимости её восстановить. Первая дорожка обычно содержит системный загрузчик или диспетчер загрузок ОС. На экране диска восстановления выберите *Repair Options > Restore original system loader*.

*Обратите внимание, что даже если вы потеряете свой диск восстановления TrueCrypt, и его найдёт ваш неприятель, он/она всё равно **не** сможет расшифровать системный раздел или диск, не зная правильный пароль.*

Чтобы загрузиться с диска восстановления TrueCrypt, вставьте его в CD/DVD-накопитель и перезагрузите компьютер. Если экран диска восстановления TrueCrypt не появился (или если вы не видите на экране элемента ‘Repair Options’ в разделе ‘Keyboard Controls’), вероятно, BIOS вашего ПК настроен так, что сначала выполняется загрузка с жёсткого диска, и лишь потом с CD/DVD-накопителя. В этом случае перезагрузите компьютер, нажмите клавишу <F2> или <Delete> (сразу же, как появится информация BIOS) и дождитесь появления экрана настройки BIOS. Если экран настройки BIOS не появился, снова перезагрузите компьютер (нажмите кнопку Reset на корпусе ПК) и сразу же начните постоянно нажимать клавишу <F2> или <Delete>. Когда появится экран настройки BIOS, сконфигурируйте BIOS так, чтобы загрузка системы сначала происходила с CD/DVD-накопителя (о том, как это сделать, см. в документации на вашу системную плату/BIOS или проконсультируйтесь в службе техподдержки поставщика вашего ПК). Затем снова перезагрузите компьютер. Экран диска восстановления TrueCrypt теперь должен появиться. Примечание: чтобы выбрать *Repair Options* на экране диска восстановления TrueCrypt, можно нажать на клавиатуре клавишу <F8>.

В случае повреждения вашего диска восстановления вы можете создать новый, выбрав в меню *Система* команду *Создать диск восстановления*. Чтобы выяснить, повреждён или нет диск восстановления TrueCrypt, вставьте его в CD/DVD-накопитель и выберите *Система > Проверить диск восстановления*.

Правдоподобное отрицание причастности

На случай, если противник вынудит вас сообщить пароль, в TrueCrypt предусмотрено два вида правдоподобного отрицания причастности:

1. Скрытые тома (см. подробности ниже в разделе *Скрытый том*) и скрытые операционные системы (см. раздел *Скрытая операционная система*).

2. Пока не будет выполнено дешифрование, раздел/устройство TrueCrypt выглядит не более чем как набор случайных данных (никакого рода "сигнатур" в нём не содержится). Поэтому должно быть невозможно *гарантированно утверждать*, что раздел или устройство являются томом TrueCrypt или что они зашифрованы (при условии соблюдения требований, перечисленных в главе *Требования безопасности и меры предосторожности*). Правдоподобное объяснение наличия раздела/устройства, содержащего только случайные данные, может быть таким: вы уничтожили (стёрли с надёжным затиранием данных) содержимое раздела/устройства с помощью одной из программ, предназначенных для удаления информации с её перезаписью случайными данными (на самом деле TrueCrypt также можно использовать для надёжного стирания раздела/устройства – для этого нужно создать внутри него пустой зашифрованный раздел/том на основе устройства). При этом, однако, требуется предотвращать утечки данных (см. раздел *Утечки данных*) и также иметь в виду, что при шифровании системы первая дорожка диска содержит (незашифрованный) загрузчик TrueCrypt, идентификация которого не составляет труда (подробности см. в главе *Шифрование системы*). В случае шифрования системы правдоподобное отрицание причастности достигается созданием скрытой операционной системы (см. раздел *Скрытая операционная система*).

   Хотя тома TrueCrypt на основе файлов (контейнеры) и не содержат никакого рода "сигнатур" (до тех пор, пока не будет выполнено дешифрование, тома выглядят лишь как набор случайных данных), они не обеспечивают никакого правдоподобного отрицания причастности, так как практически невозможно правдоподобно объяснить наличие файла, содержащего только случайные данные. Тем не менее, правдоподобного отрицания причастности можно добиться и при использовании тома TrueCrypt на основе файла (контейнера), если создать внутри него скрытый том (см. ниже).

Примечания

- При форматировании раздела жёсткого диска как тома TrueCrypt (или шифрования раздела на месте), таблица разделов (включая тип раздела) *никогда* не изменяется (в таблицу разделов не вносится никаких “сигнатур” или “идентификаторов” TrueCrypt).

- Существуют методы обнаружения файлов и устройств, содержащих случайные данные (таких, как тома TrueCrypt). Тем не менее, это никаким образом *не* должно влиять на правдоподобность отрицания причастности. Если неприятель не может *гарантированно утверждать*, что раздел/устройство является томом TrueCrypt или что в файле, разделе или устройстве содержится скрытый том TrueCrypt (при условии, что вы соблюли все условия, описанные в главе *Требования безопасности и меры предосторожности* и в подразделе *Требования безопасности и меры*

предосторожности касательно скрытых томов).

Скрытый том

Возможны ситуации, когда кто-то заставит вас сообщить пароль от зашифрованного тома. Во многих случаях вы просто не сможете отказаться это сделать (например, при вымогательстве). Использование так называемого скрытого тома позволяет благополучно выходить из таких ситуаций, не сообщая пароль от тома с вашими данными.

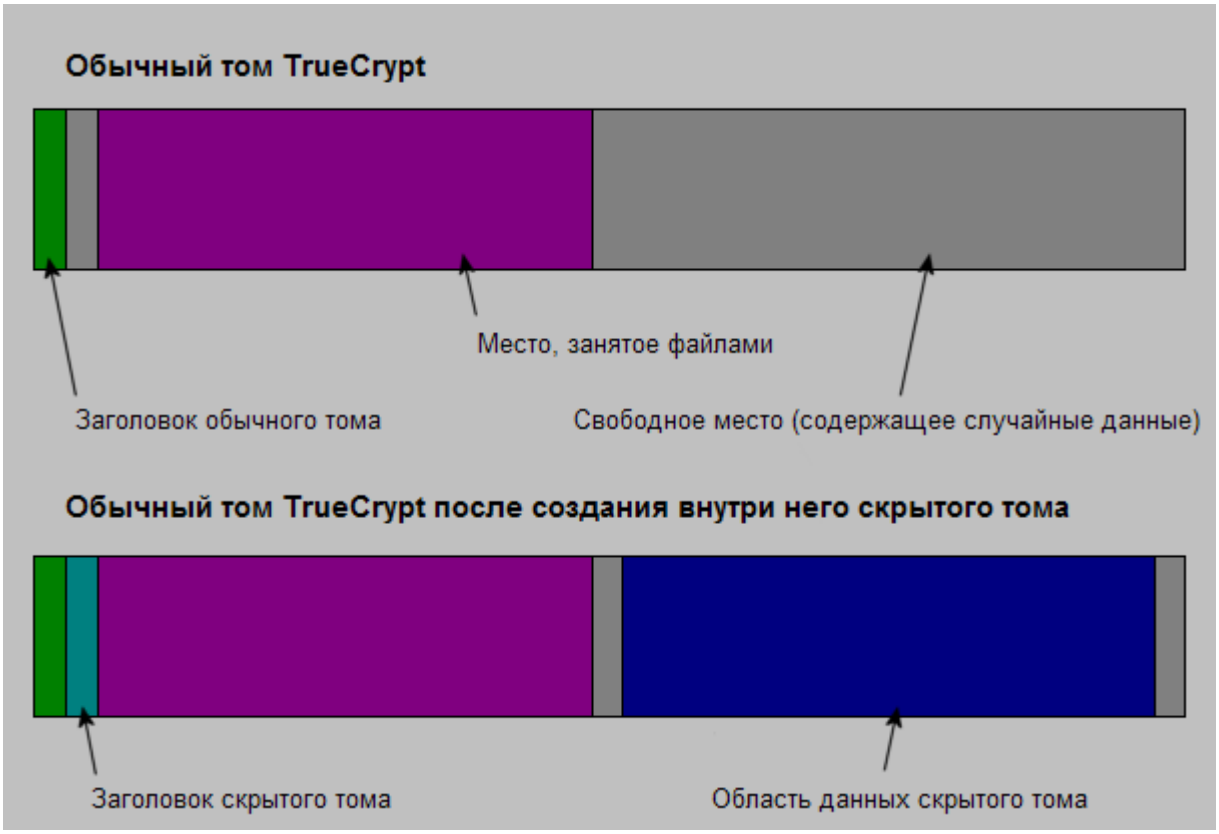


Схема обычного тома TrueCrypt до и после создания внутри него скрытого тома.

Принцип скрытого тома в том, что том TrueCrypt создаётся внутри другого тома TrueCrypt (в свободном месте тома). Даже при смонтированном внешнем томе невозможно гарантированно утверждать, есть внутри него скрытый том или нет[1], так как свободное место в *любом* томе TrueCrypt всегда заполняется случайными данными при создании[2] тома, и никакую часть (несмонтированного) скрытого тома нельзя отличить от случайных данных. Обратите внимание, что TrueCrypt никак не модифицирует файловую систему (информацию о свободном месте и т. д.) внутри внешнего тома.

[1] При условии соблюдения всех инструкций мастера создания томов TrueCrypt, а также требований, указанных в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов*.
[2] При условии, что были выключены параметры *Быстрое форматирование* и *Динамический*, и что том не содержит файловой системы, зашифрованной на месте (TrueCrypt не позволяет пользователю создавать скрытый том внутри такого тома). Сведения о методе заполнения свободного места в томе случайными данными см. в главе *Технические подробности*, раздел *Спецификация формата томов TrueCrypt*.

Пароль для скрытого тома должен существенно отличаться от пароля для внешнего тома. Перед созданием скрытого тома следует скопировать во внешний том некоторое количество осмысленно выглядящих файлов, которые на самом деле вам скрывать НЕ требуется. Эти файлы будут служить для введения в заблуждение того, кто вынудит вас сообщить пароль. Вы сообщите только пароль от внешнего тома, но не от скрытого. Файлы, действительно представляющие для вас ценность, останутся в неприкосновенности в скрытом томе.

Скрытый том монтируется так же, как обычный том TrueCrypt: нажмите кнопку *Файл* или *Устройство*, выберите внешний (хост) том (важно: убедитесь, что этот том *не* смонтирован). Затем нажмите кнопку *Смонтировать* и введите пароль для скрытого тома. Какой том будет смонтирован – скрытый или внешний – определяется только указанным паролем (т. е. если введён пароль для внешнего тома, то будет смонтирован внешний том, а если указать пароль для скрытого, то смонтируется скрытый том).

Используя введённый пароль, TrueCrypt сначала пытается расшифровать заголовок обычного тома. Если этого сделать не удаётся, выполняется загрузка области, где может находиться заголовок скрытого тома (т. е. байты 65536–131071, содержащие исключительно случайные данные, если внутри тома нет скрытого тома) в ОЗУ и попытка расшифровать её с помощью указанного пароля. Обратите внимание, что заголовки скрытых томов не могут быть идентифицированы, так как они выглядят как абсолютно случайные данные. Если заголовок успешно расшифрован (информацию о том, как TrueCrypt определяет, успешно ли он расшифрован, см. в разделе *Схема шифрования*), из расшифрованного заголовка (который по-прежнему находится в ОЗУ) извлекаются сведения о размере скрытого тома и выполняется монтирование скрытого тома (по его размеру также определяется его смещение).

Скрытый том можно создавать внутри тома TrueCrypt любого типа, т. е. внутри тома на основе файла или тома на основе устройства (для этого требуются права администратора). Чтобы создать скрытый том TrueCrypt, в главном окне программы нажмите кнопку *Создать том* и выберите *Создать скрытый том TrueCrypt*. В окне мастера будет предоставлена вся информация, необходимая для успешного создания скрытого тома TrueCrypt.
При создании скрытого тома для неопытного пользователя может быть весьма затруднительно или даже вообще невозможно установить размер скрытого тома так, чтобы тот не перекрывал данные во внешнем томе. Поэтому мастер создания томов автоматически сканирует карту кластеров внешнего тома (перед созданием внутри него скрытого тома) и определяет максимально возможный размер скрытого тома.[1]

В случае возникновения каких-либо проблем при создании скрытого тома, см. возможные решения в главе *Устранение неполадок*.

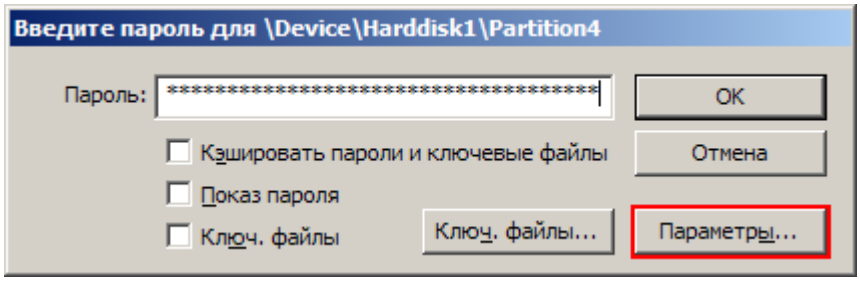
Обратите внимание, что также имеется возможность создавать и загружать операционную систему, располагающуюся в скрытом томе (см. раздел *Скрытая операционная система* в главе *Правдоподобное отрицание причастности*).

[1] Мастер сканирует карту кластеров с целью найти размер непрерывной свободной области (если таковая существует), конец которой выровнен по концу внешнего тома. Данная область предоставляется под скрытый том, поэтому максимально возможный размер скрытого тома ограничен её размером. В среде Linux и Mac OS X карта кластеров мастером не сканируется, но драйвер находит любые данные, записанные во внешнем томе, и использует их расположение, как описано ранее.

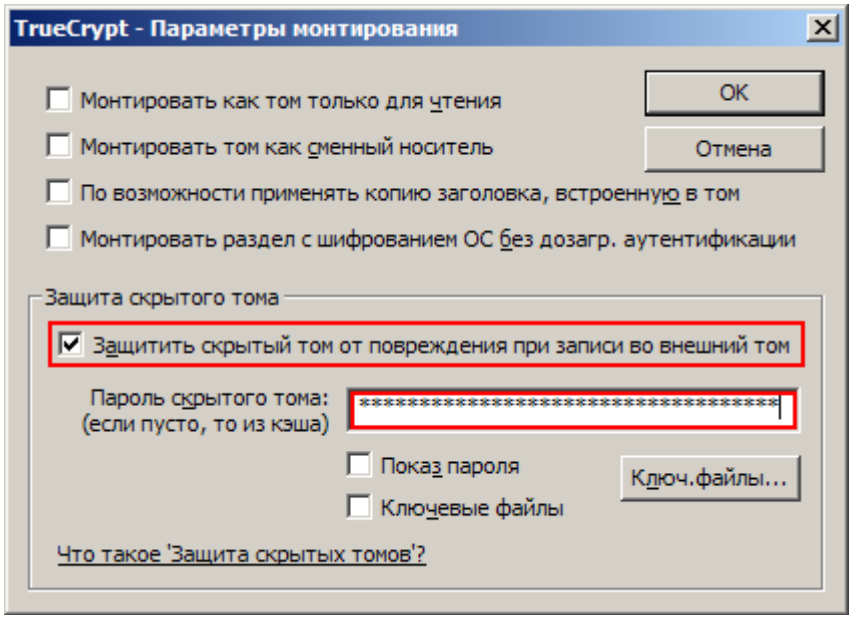
Защита скрытых томов от повреждений

Если вы монтируете том TrueCrypt, внутри которого находится скрытый том, то можете *считывать* данные из (внешнего) тома без всякого риска. Однако если вам (или операционной системе) потребуется *записать* данные во внешний том, есть риск повредить (перезаписать) скрытый том. Чтобы избежать подобной ситуации, скрытый том следует защитить, о чём и пойдёт здесь речь.

При монтировании внешнего тома введите его пароль и, прежде чем нажать *OK*, нажмите кнопку *Параметры*:



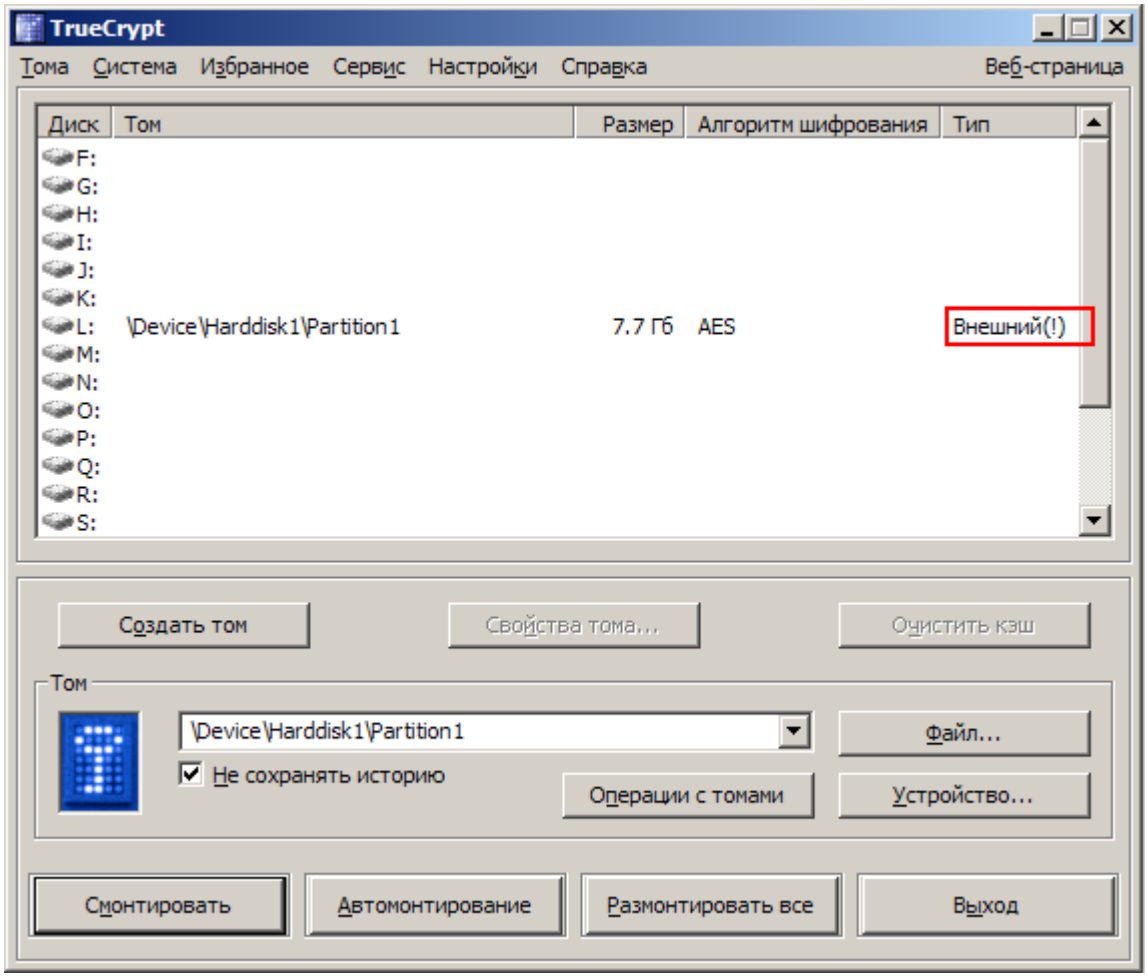
В появившемся диалоговом окне *Параметры монтирования* включите опцию *Защитить скрытый том от повреждения при записи во внешний том*. В поле *Пароль скрытого тома* введите пароль для скрытого тома. Нажмите *OK*, а затем нажмите *OK* в окне ввода основного пароля.



Оба пароля должны быть правильными; в противном случае внешний том не будет смонтирован. При включённой защите скрытого тома TrueCrypt на самом деле *не* монтирует скрытый том. Он только расшифровывает его заголовок (в ОЗУ) и получает информацию о

размере скрытого тома (из расшифрованного заголовка). Затем монтируется внешний том, а любые попытки записи данных в область скрытого тома отклоняются (пока внешний том не будет размонтирован). **Обратите внимание, что TrueCrypt *никогда и никак* не модифицирует файловую систему (например, сведения о распределённых кластерах, объём свободного пространства и т. д.) внутри внешнего тома. Как только том будет размонтирован, защита отключается. При повторном монтировании тома определить, применялась ли защита скрытого тома, *невозможно*. Защиту скрытого тома может включать только пользователь, указывающий правильный пароль (и/или ключевые файлы) для скрытого тома (при каждом монтировании внешнего тома).**

Как только будет отвергнута/предотвращена предпринятая операция записи в область, занимаемую скрытым томом (для защиты скрытого тома), весь хост-том (оба тома – внешний и скрытый) становится недоступным для записи до тех пор, пока он не будет размонтирован (при каждой попытке записи в этот том драйвер TrueCrypt передаёт системе ошибку ‘неверный параметр’). Таким образом, сохраняется возможность правдоподобного отрицания причастности (иначе некоторые несоответствия внутри файловой системы могли бы свидетельствовать о том, что для этого тома применялась защита скрытого тома). Когда предотвращается повреждение скрытого тома, об этом выдаётся предупреждающее сообщение (при условии, что включена работа TrueCrypt в фоновом режиме, см. главу *Работа TrueCrypt в фоновом режиме*). Кроме того, отображаемый в главном окне тип смонтированного внешнего тома изменяется на ‘*Внешний(!)*’:

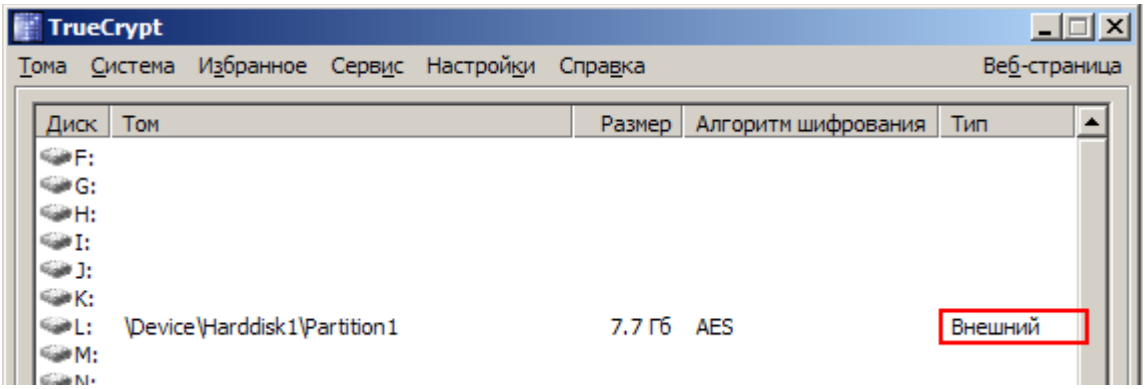


Также, в диалоговом окне *Свойства тома* в поле *Скрытый том защищён* выводится: '*Да (защита от повреждений!)*'.

Обратите внимание, что при предотвращении повреждения скрытого тома *никакая* информация об этом событии в том не записывается. После размонтирования и повторного монтирования внешнего тома в свойствах тома *не будет* строки "*защита от повреждений*".

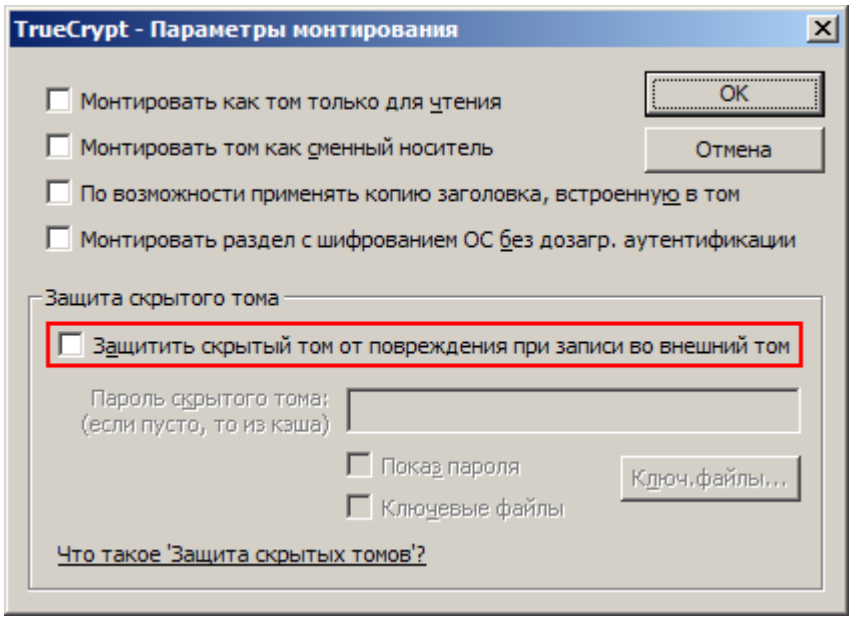
Проверить, защищён ли скрытый том от повреждений, можно несколькими способами:

1. После монтирования внешнего тома появляется окно с подтверждающим сообщением о том, что скрытый том защищён (если этого сообщения не появилось, скрытый том не защищён!).
2. В диалоговом окне *Свойства тома* у поле *Скрытый том защищён* выводится значение '*Да*'.
3. Тип смонтированного внешнего тома – *Внешний.*



ВАЖНО: Когда неприятель вынуждает вас смонтировать внешний том, вы, разумеется,* НЕ *должны монтировать внешний том с включённой защитой скрытого тома. Вы должны монтировать его как обычный том (после чего TrueCrypt будет показывать тип тома не "Внешний", а "Обычный"). Обратите внимание, что пока внешний том остаётся смонтированным с включённой защитой скрытого тома, неприятель* может *обнаружить наличие скрытого тома во внешнем томе (он/она сможет его найти до того момента, пока том не будет размонтирован).

ВНИМАНИЕ: Опция *Защитить скрытый том от повреждения при записи во внешний том* в диалоговом окне *Параметры монтирования* автоматически сбрасывается в выключенное состояние после завершённой попытки монтирования, неважно, успешной или нет (все уже защищённые скрытые тома, разумеется, остаются защищёнными). Поэтому эту опцию нужно включать *каждый* раз, когда вы пытаетесь смонтировать внешний том (если хотите, чтобы скрытый том был защищён от повреждений):



Если вы хотите смонтировать внешний том и защитить находящийся внутри него скрытый том, используя кэшированные пароли, выполните следующие шаги. Удерживая нажатой клавишу <Control> (<Ctrl>), щёлкните по кнопке *Смонтировать* (или выберите в меню *Тома* команду *Смонтировать том с параметрами*). Откроется диалоговое окно *Параметры монтирования*. Включите в нём опцию *Защитить скрытый том от повреждения при записи во внешний том* и оставьте поле ввода пароля пустым. Затем нажмите *OK*.

Если вам нужно смонтировать внешний том, и вы знаете, что в нём не потребуется сохранять никаких данных, тогда наиболее удобным способом защиты скрытого тома от повреждений будет монтирование внешнего тома как доступного только для чтения (см. Раздел *Параметры монтирования*).

Требования безопасности и меры предосторожности касательно скрытых томов

При использовании скрытого тома TrueCrypt нужно обязательно соблюдать описанные в этой главе требования безопасности и меры предосторожности. Отказ от ответственности: мы не гарантируем, что эта глава содержит список *всех* проблем, связанных с безопасностью, и атак, которые может предпринять ваш неприятель, чтобы получить доступ к данным, хранящимся в скрытом томе TrueCrypt, или ограничить возможность TrueCrypt надёжно хранить такие данные и обеспечивать правдоподобное отрицание причастности.

- Если неприятель имеет доступ к (размонтированному) тому TrueCrypt в нескольких точках в течение достаточно длительного времени, он может определить, какие сектора тома изменяются. Если вы изменяете содержимое скрытого тома (например, создаёте/копируете новые файлы в скрытый том или изменяете/удаляете/переименовываете/перемещаете файлы в скрытом томе, и т. п.), содержимое секторов (зашифрованный текст) в области, занимаемой скрытым томом, изменяется. Узнав пароль от внешнего тома, неприятель может потребовать объяснений, почему изменились эти сектора. Если вы не дадите правдоподобного объяснения, это может послужить поводом заподозрить наличие скрытого тома внутри внешнего тома.

Имейте в виду, что случаи, подобные вышеописанному, также могут возникать в следующих ситуациях:

  - Файловая система, в которой у вас хранится контейнер TrueCrypt на основе файла, была дефрагментирована, и копия контейнера TrueCrypt (или его фрагмента) остаётся в свободном пространстве хост-тома (в дефрагментированной файловой системе). Чтобы это предотвратить, сделайте одно из следующего:
    - вместо тома TrueCrypt на основе файла используйте том TrueCrypt на основе раздела/устройства;
    - надёжно очистите (затрите) свободное пространство в хост-томе (в дефрагментированной файловой системе) после дефрагментации;
    - не дефрагментируйте файловые системы, в которых у вас хранятся тома TrueCrypt.

  - Контейнер TrueCrypt на основе файла хранится в журналируемой файловой системе (например, в NTFS). При этом копия контейнера TrueCrypt (или его фрагмента) может оставаться в хост-томе. Чтобы это предотвратить, сделайте одно из следующего:
    - вместо тома TrueCrypt на основе файла используйте том TrueCrypt на основе раздела/устройства;
    - храните контейнер в нежурналируемой файловой системе (например, в FAT32).

  - Том TrueCrypt находится на устройстве или в файловой системе, где применяется механизм wear-leveling – равномерное распределение нагрузки на блоки (например, флэш-память SSD или флэш-накопитель USB). В таком устройстве может оставаться копия (или её фрагмент) тома TrueCrypt. Поэтому не храните скрытые тома в таких устройствах/файловых системах. Подробнее о wear-leveling см. в разделе *Требования безопасности и меры предосторожности* в главе *Равномерное распределение нагрузки на блоки*.

- Том TrueCrypt находится на устройстве или в файловой системе, где сохраняются данные (или на устройстве/в файловой системе под управлением или мониторингом системы/устройства, сохраняющих данные) (например, значение таймера или счётчика), которые можно использовать для того, чтобы определить, что один блок был записан раньше, чем другой, и/или чтобы определить, сколько раз блок был записан/считан. Поэтому не храните скрытые тома в таких устройствах/файловых системах. Выяснить, сохраняет ли устройство/система такие данные, можно в прилагаемой к устройству/системе документации или связавшись с поставщиком/производителем.

- Том TrueCrypt находится на устройстве, склонном к износу (где есть возможность определить, что один блок был записан/считан больше раз, чем другой). Поэтому не храните скрытые тома в таких устройствах/файловых системах. Выяснить, предрасположено ли устройство к износу, можно в документации на это устройство или у его поставщика/производителя.

- Вы делаете резервную копию содержимого скрытого тома, клонируя несущий его хост-том, или создаёте новый скрытый том, клонируя его хост-том. Поэтому так поступать нельзя. Следуйте инструкциям в главе *О безопасном резервировании данных* и в разделе *Клонирование томов*.

- При шифровании раздела/устройства, внутри которого вы намереваетесь создать скрытый том, убедитесь, что выключено *Быстрое форматирование*.

- В среде Windows убедитесь, что вы не удаляли никаких файлов в томе, внутри которого собираетесь создать скрытый том (при сканировании карты кластеров удалённые файлы не определяются).

- В среде Linux или Mac OS X, если вы собираетесь создать скрытый том внутри тома TrueCrypt на основе файла, убедитесь, что этот том – не на основе разрежённого (sparse) файла (Windows-версия TrueCrypt это проверяет самостоятельно, не позволяя создавать скрытые тома внутри разрежённых файлов).

- Когда скрытый том *смонтирован*, операционная система и сторонние приложения могут выполнять запись в не-скрытые тома (обычно в незашифрованный системный том) незашифрованной информации о данных, хранящихся в скрытом томе (например, имена и размещение файлов, к которым недавно было обращение, базы данных, созданные утилитами индексирования файлов, и др.), самих данных в незашифрованном виде (временные файлы и т. п.), незашифрованной информации о файловой системе в скрытом томе (что может быть использовано, например, для идентификации файловой системы и для определения, является ли файловая система той, что во внешнем томе), пароля/ключа для скрытого тома, или других конфиденциальных данных. Поэтому необходимо соблюдать следующие требования и предостережения:

    - *Windows*: Создайте скрытую операционную систему (о том, как это сделать, см. раздел *Скрытая операционная система*) и монтируйте скрытые тома только тогда, когда запущена скрытая операционная система.

    Примечание: когда работает скрытая операционная система, TrueCrypt гарантирует, что все локальные незашифрованные файловые системы и не-скрытые тома TrueCrypt доступны только для чтения (то есть никакие файлы не могут быть записаны в такие файловые системы или тома

TrueCrypt).[1] Запись данных в файловые системы разрешена внутри скрытых томов TrueCrypt.
В качестве альтернативного варианта, если использование скрытой операционной системы невозможно, можно воспользоваться "live-CD" с системой Windows PE (целиком хранящейся на CD/DVD и оттуда же загружающейся), гарантирующей, что все данные, записываемые в системный том, записываются в RAM-диск (диск в ОЗУ). Монтируйте скрытые тома только тогда, когда работает система с такого "live-CD" (если нельзя использовать скрытую операционную систему). Кроме того, в течение такого "live-CD"-сеанса в режиме чтения-записи можно монтировать только файловые системы, расположенные в скрытых томах TrueCrypt (внешние или незашифрованные тома/файловые системы необходимо монтировать в режиме только для чтения, либо они не должны монтироваться/быть доступными вовсе). В противном случае вы должны удостовериться, что во время "live-CD"-сеанса приложения и операционная система не выполняют запись никаких конфиденциальных данных (см. выше) в не-скрытые тома/файловые системы.

- *Linux*: Загрузите или создайте версию "live-CD" вашей операционной системы (т. е. "live"-систему Linux, целиком хранящуюся на CD/DVD и оттуда же загружающуюся), это гарантирует, что любые записанные в системный том данные записаны в RAM-диск (диск в ОЗУ). Монтируйте скрытые тома только тогда, когда запущена такая "live-CD"-система. В течение сеанса только файловые системы внутри скрытых томов TrueCrypt могут быть смонтированы в режиме чтения-записи (внешние или незашифрованные тома/файловые системы должны монтироваться как только для чтения или оставаться вовсе несмонтированными/недоступными). Если вы не можете соблюсти это требование и не в состоянии гарантировать, что приложения и операционная система не выполняют запись никаких конфиденциальных данных (см. выше) в не-скрытые тома/файловые системы, вы не должны монтировать или создавать скрытые тома TrueCrypt в среде Linux.

- *Mac OS X*: Если вы не в состоянии гарантировать, что приложения и операционная система не выполняют запись никаких конфиденциальных данных данных перечисленных выше критических типов в не-скрытые тома (или файловые системы), монтировать или создавать скрытые тома TrueCrypt в среде Mac OS X не следует.

- Когда смонтирован внешний том с включённой защитой скрытого тома от повреждения (см. раздел *Защита скрытых томов от повреждений*), необходимо следовать тем же требованиям и предостережениям, которые от вас требовались при монтировании скрытого тома (см. выше). Причина этого в том, что из операционной системы может "утечь" пароль/ключ для скрытого тома в не-скрытый или незашифрованный том.

- Если вы используете **операционную систему, находящуюся внутри скрытого тома** (см. раздел *Скрытая операционная система*), то в дополнение к вышесказанному необходимо соблюдать следующие требования безопасности и предостережения:

  - Следует использовать обманную операционную систему так часто, как вы пользуетесь своим компьютером. В идеале её следует использовать всегда, когда не требуется задействовать засекреченные данные. В противном случае

[1] Не относится к файловым системам на CD/DVD-подобных носителях и к нетипичным или нестандартным устройствам/носителям.

может пострадать правдоподобность отрицания наличия скрытой операционной системы (если вы сообщили неприятелю пароль от обманной операционной системы, он сможет выяснить, что эта система использовалась не слишком часто, что может навести на мысль о существовании в компьютере скрытой операционной системы). Обратите внимание, что вы можете сохранять данные в разделе с обманной системой в любой момент и без какого-либо риска повредить скрытый том (так как обманная система не установлена во внешнем томе).

- Если операционную систему требуется активировать, это нужно сделать до того, как она будет клонирована (клонирование это часть процесса создания скрытой ОС — см. раздел *Скрытая операционная система*), а скрытая операционная система (т. е. клон) никогда не должна быть активирована повторно. Причина этого в том, что скрытая операционная система создана путём копирования содержимого системного раздела в скрытый том (поэтому если операционная система не активирована, скрытая операционная система также будет неактивированной). В случае активации или повторной активации скрытой операционной системы, дата и время активации (и другая информация) могут быть зафиксированы на сервере Microsoft (и в скрытой операционной системе), но не в обманной операционной системе. Поэтому если неприятель получит доступ к сохранённым на сервере данным или перехватит ваш запрос серверу (и если вы сообщили ему пароль от обманной операционной системы), он сможет выяснить, что обманная операционная система была активирована (или повторно активирована) в другое время, а это способно навести на мысль о существовании в компьютере скрытой операционной системы.

По аналогичным причинам любое ПО, требующее активации, должно быть установлено и активировано до того, как вы приступите к созданию скрытой операционной системы.

- Когда вам нужно завершить работу скрытой операционной системы и запустить обманную систему, *не* перезагружайте компьютер. Вместо этого завершите работу системы или переведите её в состояние гибернации (сна), после чего оставьте компьютер выключенным в течение хотя бы нескольких минут (чем дольше, тем лучше), и только после этого включите его и загрузите обманную систему. Это требуется, чтобы очистить память, в которой могут содержаться конфиденциальные данные. Подробности см. в главе *Незашифрованные данные в ОЗУ*, раздел *Требования безопасности и меры предосторожности*.

- Компьютер может быть подключён к сети (в том числе к Интернету) только когда запущена обманная операционная система. Когда выполняется скрытая ОС, компьютер не следует подключать ни к какой сети, включая Интернет (один из самых надёжных способов гарантировать это – отключить от ПК сетевой кабель, если таковой имеется). Обратите внимание, что при загрузке данных с/на удалённый сервер, на сервере обычно фиксируются дата и время соединения и другая информация. Разного сорта данные также протоколируются и в операционной системе (например, данные автоматического обновления Windows, отчёты приложений, протоколы ошибок и т. п.). Таким образом, если неприятель получил доступ к хранящимся на сервере данным или перехватил ваш запрос серверу (и если вы сообщили ему пароль от обманной операционной системы), он сможет узнать, что соединение было выполнено не из обманной ОС, и это способно навести его на мысль о существовании в вашем компьютере скрытой операционной системы.

Также имейте в виду, что аналогичные проблемы возможны, если у вас в среде скрытой операционной системы есть какие-либо файловые системы с общим доступом через сеть (вне зависимости от того, удалённая файловая система или локальная). Поэтому во время работы скрытой операционной системы никаких файловых систем с общим доступом по сети (в любом направлении) быть не должно.

- Любые действия, которые могут быть обнаружены неприятелем (или любые действия, модифицирующие какие-либо данные вне смонтированных скрытых томов) должны выполняться только когда работает обманная операционная система (если только у вас нет альтернативного правдоподобного объяснения, например, использование системы на "live-CD" для выполнения таких действий). Скажем, параметр *Автоматический переход на летнее время и обратно* можно включать только в обманной операционной системе.

- Если BIOS, EFI или любой другой компонент протоколирует выключения питания или любые другие события, которые могут свидетельствовать об использовании скрытого тома/системы (например, путём сравнения таких событий с событиями в протоколе Windows), вы обязаны либо отключить подобное протоколирование, либо обеспечить надёжное удаление протокола после каждого сеанса (или иначе избежать подобной проблемы соответствующим образом).

В дополнение к вышесказанному необходимо соблюдать требования безопасности и меры предосторожности, перечисленные в следующих главах:

- *Требования безопасности и меры предосторожности*
- *О безопасном резервировании данных*

Скрытая операционная система

Если системный раздел или системный диск зашифрован с помощью TrueCrypt, то при каждом включении или при каждой перезагрузке компьютера требуется вводить пароль дозагрузочной аутентификации на экране загрузчика TrueCrypt. Может случиться, что кто-то вынудит вас расшифровать операционную систему или сообщить пароль от дозагрузочной аутентификации. Во многих ситуациях вы просто не сможете отказаться это сделать (например, при вымогательстве). TrueCrypt позволяет создать скрытую операционную систему, о существовании которой должно быть невозможно наверняка утверждать (при условии выполнения некоторых рекомендаций — см. ниже). Таким образом, вам не придётся расшифровывать скрытую операционную систему или сообщать от неё пароль.

Прежде чем продолжить чтение, вам следует ознакомиться с разделом *Скрытый том* и убедиться, что вы понимаете, что такое скрытый том TrueCrypt.

Скрытая операционная система это система (например, Windows 7 или Windows XP), установленная в скрытом томе TrueCrypt. Гарантированно утверждать, что существует скрытый том TrueCrypt, должно быть невозможно (при условии выполнения некоторых рекомендаций; подробности см. в разделе *Скрытый том*) и, следовательно, должно быть невозможно гарантированно утверждать, что существует скрытая операционная система.

Однако для загрузки системы, зашифрованной TrueCrypt, необходимо, чтобы незашифрованная копия загрузчика TrueCrypt (Boot Loader) находилась на системном диске или на диске восстановления TrueCrypt (Rescue Disk). Очевидно, что одно только присутствие загрузчика TrueCrypt свидетельствует о том, что в компьютере имеется система, зашифрованная с помощью TrueCrypt. Поэтому для обеспечения правдоподобного отрицания причастности при наличии загрузчика TrueCrypt, в течение процесса создания скрытой операционной системы мастер TrueCrypt поможет вам создать вторую зашифрованную ОС, так называемую **обманную операционную систему**. Обманная операционная система не должна содержать никаких конфиденциальных файлов. Её наличие не составляет секрета (она *не* установлена в скрытом томе). Пароль от обманной операционной системы можно без опасений сообщить любому, кто будет вынуждать вас раскрыть пароль от дозагрузочной аутентификации.[1]

Использовать обманную операционную систему следует так часто, как вы пользуетесь своим компьютером. В идеале её следует использовать всегда, когда не требуется задействовать засекреченные данные. В противном случае может пострадать правдоподобность отрицания наличия скрытой операционной системы (если вы сообщили

[1] Непрактично (и потому это не поддерживается) устанавливать операционные системы в два тома TrueCrypt, встроенных внутрь одного раздела, так как при использовании внешней операционной системы часто требуется записывать данные в область скрытой ОС (и в случае блокирования таких операций функцией защиты скрытого тома это по сути будет вызывать системные сбои, т. е. ошибки 'синего экрана смерти').

неприятелю пароль от обманной операционной системы, он сможет выяснить, что эта система использовалась не слишком часто, что может навести на мысль о существовании в компьютере скрытой операционной системы). Обратите внимание, что вы можете сохранять данные в разделе с обманной системой в любой момент и без какого-либо риска повредить скрытый том (так как обманная система *не* установлена во внешнем томе — см. ниже).

В вашем распоряжении будут два пароля дозагрузочной аутентификации — один для скрытой операционной системы, а другой для обманной системы. Если вы хотите загрузить скрытую систему, то просто вводите пароль для скрытой системы на экране загрузчика TrueCrypt (который появляется при включении или перезагрузке компьютера). Аналогично, если вам нужно загрузить обманную операционную систему (например, когда вас вынуждает это сделать неприятель), то на экране загрузчика TrueCrypt вы просто вводите пароль от обманной системы.

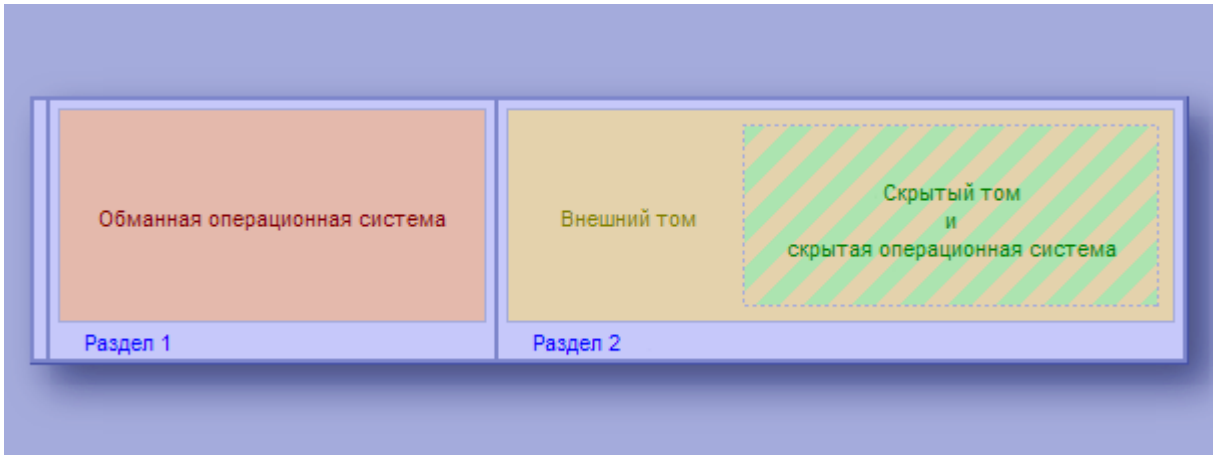
Примечание: когда вы вводите пароль дозагрузочной аутентификации, загрузчик TrueCrypt сначала пытается расшифровать (с помощью указанного пароля) последние 512 байт первой логической дорожки системного диска (где обычно хранятся зашифрованные данные мастер-ключа для не-скрытых системных разделов/дисков). Если это сделать не удаётся и если имеется раздел, следующий за активным разделом, загрузчик TrueCrypt (даже если на диске в действительности нет скрытого тома) автоматически пытается расшифровать (снова с помощью того же указанного пароля) область первого раздела, следующего за активным разделом[1], где может находиться зашифрованный заголовок возможного скрытого тома. Обратите внимание, что TrueCrypt никогда заранее не знает, имеется или нет скрытый том (идентифицировать заголовок скрытого тома невозможно, так как он выглядит как состоящий целиком из случайных данных). Если заголовок успешно расшифрован (о том, как TrueCrypt определяет, что он успешно расшифрован, см. *Схема шифрования*), из расшифрованного заголовка извлекается информация о размере скрытого тома (по-прежнему хранимая в ОЗУ) и монтируется скрытый том (его размер также определяет его смещение). Более подробные технические сведения см. в разделе *Схема шифрования*, глава *Технические подробности*.

Будучи запущенной, скрытая операционная система выглядит так, как будто она установлена в том же разделе, что и исходная ОС (обманная система). Однако в действительности она установлена внутри раздела, находящегося за ним (в скрытом томе). Все операции чтения/записи прозрачно перенаправляются из системного раздела в скрытый том. Ни операционная система, ни приложения не знают, что данные, записываемые в и считываемые из системного раздела, на самом деле записываются в и считываются из раздела, находящегося за ним (из/в скрытый том). Любые такие данные как обычно шифруются и расшифровываются на лету (с помощью ключа шифрования, отличного от того, который используется для обманной операционной системы).

Также обратите внимание на существование третьего пароля — пароля для **внешнего тома**. Это не пароль дозагрузочной аутентификации, а пароль для обычного тома TrueCrypt. Его можно без опаски сообщать любому, кто станет вынуждать вас выдать пароль от зашифрованного раздела, где находится скрытый том (содержащий скрытую операционную систему). Таким образом, наличие скрытого тома (и скрытой операционной системы) останется в тайне. Если вы не вполне понимаете, как такое возможно, или не знаете, что собой представляет внешний том, прочитайте раздел *Скрытый том*. Внешний том должен содержать некоторое количество осмысленно выглядящих файлов, которые на самом деле вам прятать *не* нужно.

[1] Если размер активного раздела меньше 256 Мбайт, то данные считываются из *второго* раздела, расположенного следом за активным (Windows 7 и новее по умолчанию не загружаются из раздела, в котором установлены).

Итак, всего будет три пароля. Два из них можно сообщать неприятелю (для обманной системы и для внешнего тома). Третий пароль, для скрытой системы, должен оставаться в тайне.



Пример макета системного диска, содержащего скрытую операционную систему

Создание скрытой операционной системы

Чтобы приступить к созданию скрытой операционной системы, выберите *Система* > *Создать скрытую ОС* и следуйте инструкциям мастера.

Вначале мастер проверяет наличие на системном диске раздела, подходящего для скрытой операционной системы. Обратите внимание, что прежде чем можно будет создать скрытую ОС, необходимо создать для неё раздел на системном диске. Этот раздел должен следовать сразу за системным и быть хотя бы на 5% больше, чем системный (системный раздел этот тот, где установлена выполняемая в данный момент операционная система). Однако если внешний том (не путайте его с системным разделом) отформатирован как NTFS, раздел для скрытой операционной системы должен быть, по крайней мере, на 110% (в 2,1 раза) больше, чем системный раздел (причина этого в том, что файловая система NTFS всегда сохраняет внутренние данные точно в центре тома, и потому скрытый том, который должен содержать клон системного раздела, может располагаться только во второй половине раздела).

На следующих этапах мастер создаст два тома TrueCrypt (внешний и скрытый) внутри раздела, следующего первым за системным разделом. Скрытый том будет содержать скрытую операционную систему. Размер скрытого тома всегда равен размеру системного раздела. Причина этого в том, что в скрытом томе должен находиться клон содержимого системного раздела (см. ниже). Обратите внимание, что клон будет зашифрован с помощью другого ключа шифрования, нежели оригинал. Прежде чем вы начнёте копировать во внешний том осмысленно выглядящие файлы, мастер сообщит вам максимально рекомендуемый размер дискового пространства, который могут занимать такие файлы, так чтобы во внешнем томе оставалось достаточно свободного места для скрытого тома.

Замечание: после того как вы скопируете некоторое количество осмысленно выглядящих файлов во внешний том, карта кластеров тома будет просканирована с целью определения размера непрерывной свободной области, конец которой выровнен по концу внешнего тома.

Эта область будет отведена под скрытый том, поэтому именно ею определяется его максимальный размер. При выяснении максимально возможного размера скрытого тома будет проверено, что он больше, чем системный раздел (что необходимо, так как в скрытый том нужно будет скопировать всё содержимое системного раздела — см. ниже). Таким образом, гарантируется, что никакие данные во внешнем томе не будут перезаписаны данными в области скрытого тома (например, при копировании в него системы). Размер скрытого тома всегда равен размеру системного раздела.

Затем TrueCrypt создаст скрытую операционную систему путём копирования в скрытый том содержимого системного раздела. Копируемые данные шифруются на лету с помощью ключа шифрования, отличного от того, который будет использоваться для обманной операционной системы. Процесс копирования системы выполняется в дозагрузочном окружении (до запуска Windows) и может занимать продолжительное время, измеряемое часами или даже днями (в зависимости от размера системного раздела и быстродействия компьютера). Вы сможете прервать процесс, выключить компьютер, загрузить операционную систему, а затем снова продолжить процесс. Однако в случае прерывания весь процесс копирования системы придётся начинать с начала (потому что содержимое системного раздела при клонировании должно оставаться неизменным). Скрытая операционная система будет изначально клоном операционной системы, из которой вы запустили мастер.

Windows создаёт (как правило, без вашего ведома или согласия) на системном разделе различные файлы-протоколы, временные файлы и т. п. Кроме того, в файлах гибернации (сна) и подкачки, также находящихся в системном разделе, сохраняется содержимое ОЗУ. Поэтому если неприятель проанализирует файлы в разделе, где находится исходная система (клоном которой является скрытая система), он сможет определить, что, например, вы использовали мастер TrueCrypt в режиме создания скрытой системы (что может навести на мысль о существовании в вашем ПК скрытой ОС). Чтобы избежать подобных проблем, TrueCrypt после создания скрытой системы надёжно удаляет (затирает) всё содержимое раздела, в котором находится исходная система. Затем, чтобы обеспечить возможность правдоподобного отрицания, TrueCrypt предложит вам установить в раздел новую систему и зашифровать её с помощью TrueCrypt. Таким образом, вы создадите обманную систему, и на этом весь процесс создания скрытой операционной системы будет завершён.

Правдоподобное отрицание причастности и защита от утечки данных

Во время работы скрытой операционной системы TrueCrypt из соображений безопасности гарантирует, что все локальные незашифрованные файловые системы и не-скрытые тома TrueCrypt доступны только для чтения (т. е. в такие файловые системы или тома TrueCrypt невозможно записать никаких файлов).[1] Запись данных разрешена в любую файловую систему, находящуюся внутри скрытого тома TrueCrypt (при условии, что этот скрытый том расположен не в контейнере, хранящемся в незашифрованной файловой системе или в любой другой файловой системе, доступной только для чтения).

Существует три главные причины введения таких контрмер:

1. Возможность создания безопасной платформы для монтирования скрытых томов TrueCrypt. Обратите внимание, что мы официально рекомендуем монтировать скрытые тома только в среде скрытой операционной системы. Подробности см. в

[1] Не относится к файловым системам на CD/DVD-подобных носителях и в нетипичных или нестандартных устройствах/носителях.

подразделе *Требования безопасности и меры предосторожности касательно скрытых томов*.

2. В ряде ситуаций существует возможность определить, что конкретная файловая система была смонтирована в некоторое время (или что конкретный файл в файловой системе был сохранён или считан не из неё) не в конкретной копии операционной системы (например, путём анализа и сравнения журналов файловых систем, времён файлов, протоколов приложений, отчётов об ошибках и т. д.). Это может навести на мысль о наличии в компьютере скрытой операционной системы. Контрмеры предотвращают подобные осложнения.

3. Предотвращение повреждения данных и возможность безопасной гибернации («сна»). Когда операционная система Windows выходит из режима гибернации, она подразумевает, что все смонтированные файловые системы находятся в том же состоянии, в котором они были на момент входа системы в режим гибернации. TrueCrypt обеспечивает это, защищая от записи любую файловую систему, доступную и из обманной, и из скрытой ОС. Без такой защиты файловая система может повредиться при монтировании одной системой в то время, когда другая находится в состоянии гибернации.

Если вам нужно безопасно перенести файлы из обманной системы в скрытую, выполните следующее:

1. Загрузите обманную систему.
2. Сохраните файлы в незашифрованном томе или во внешнем/обычном томе TrueCrypt.
3. Загрузите скрытую систему.
4. Если вы сохранили файлы в томе TrueCrypt, смонтируйте его (он будет автоматически смонтирован как доступный только для чтения).
5. Скопируйте файлы в раздел со скрытой операционной системой или в другой скрытый том.

Варианты объяснения наличия двух разделов TrueCrypt на одном диске

Неприятель может поинтересоваться, зачем вам понадобилось создавать на одном диске два зашифрованных TrueCrypt раздела (системный и несистемный), когда можно было бы вместо этого зашифровать весь диск с помощью одного ключа шифрования. На то может быть множество причин. Однако если вам не приходит в голову никакая (кроме создания скрытой операционной системы), вы можете воспользоваться, например, одним из следующих объяснений.

- Если на системном диске более двух разделов, и вам нужно зашифровать только два из них (системный раздел и раздел, следующий за ним), оставив другие разделы незашифрованными (например, чтобы обеспечить на этих незашифрованных разделах максимально возможную скорость чтения и записи данных, не нуждающихся в шифровании), единственный способ это сделать – зашифровать два раздела по-отдельности (обратите внимание, что с помощью одного ключа шифрования TrueCrypt может зашифровать весь системный диск и *все* находящиеся на нём разделы, но не может зашифровать только два из них — с помощью одного ключа можно зашифровать либо один, либо все разделы). В результате на системном диске будут два расположенных рядом раздела TrueCrypt (первый –

системный, второй – несистеменый), каждый зашифрованный своим собственным ключом (что также имеет место при создании скрытой операционной системы, и потому тоже может быть объяснено таким же образом).

Если вы не знаете ни одной веской причины, почему на системном диске может быть более одного раздела, примите к сведению следующее.

Как правило, несистемные файлы (документы) рекомендуется хранить отдельно от системных файлов. Один из наиболее простых и надёжных способов этого добиться – создать два раздела на системном диске: один раздел для операционной системы, а другой для документов (несистемных файлов). Такая практика рекомендуется по следующим причинам.

- Если повредится файловая система одного из разделов, файлы на этом разделе могут испортиться или стать недоступными, в то время как файлов на другом разделе это не коснётся.
- Так проще выполнить переустановку системы без потери документов (полная повторная установка ОС включает в себя форматирование системного раздела, что приводит к уничтожению всех хранящихся на нём файлов). В случае повреждения системы полная её переустановка это, зачастую, единственно возможный путь.

- Каскадное шифрование (например, AES-Twofish-Serpent) может быть во много раз медленнее, чем шифрование без каскадирования (например, AES). Однако каскадное шифрование более надёжно, чем некаскадное (например, вероятность взлома трёх разных алгоритмов шифрования, скажем, по причине развития криптоанализа, значительно ниже, чем только одного из них). Поэтому если вы зашифруете внешний том с применением каскадного алгоритма шифрования, а обманную систему с помощью некаскадного алгоритма, то сможете ответить, что вы хотели добиться максимальной производительности (и достаточной защиты) для системного раздела, а для несистемного раздела (т. е. для внешнего тома), где у вас хранятся самые конфиденциальные данные и куда вы обращаетесь не слишком часто (в отличие от операционной системы, которая используется очень часто и потому нуждается в наиболее высокой скорости), вам была нужна максимальная защита (хотя и ценой потери производительности). На системном разделе вы храните менее секретные данные (но которые вам нужны очень часто), чем данные на несистемном разделе (т. е. во внешнем томе).

- При условии, что внешний том у вас зашифрован с помощью каскадного шифрования (например, AES-Twofish-Serpent), а обманная система – некаскадным алгоритмом (скажем, AES), вы также можете ответить, что хотели избежать проблем, о которых предупреждает TrueCrypt, когда пользователь пытается выбрать каскадный алгоритм для шифрования системы (список проблем приведён ниже). Поэтому чтобы не осложнять себе жизнь такими проблемами, вы решили зашифровать системный раздел с помощью некаскадного алгоритма. Вместе с тем, для своих самых конфиденциальных данных вы по-прежнему захотели воспользоваться каскадным шифрованием (как более надёжным, чем некаскадный алгоритм), и потому решили создать второй раздел, которого эти проблемы *не* касаются (поскольку он несистемный). В системном разделе вы храните менее важные данные, чем те, которые хранятся в несистемном разделе (т. е. во внешнем томе).

  Примечание: если пользователь пытается зашифровать системный раздел, выбрав каскадный алгоритм шифрования, TrueCrypt предупреждает, что это может повлечь

за собой следующие проблемы (и, таким образом, рекомендует вместо этого выбрать некаскадный алгоритм шифрования):
    - При использовании каскадных алгоритмов шифрования размер загрузчика TrueCrypt больше, чем обычно, и потому на первой дорожке диска недостаточно места для его резервной копии. Следовательно, при *любом* повреждении загрузчика TrueCrypt (что часто случается, например, из-за неудачно реализованных антипиратских процедур активации некоторых программ) пользователю нужно прибегать к помощи диска восстановления TrueCrypt для починки загрузчика TrueCrypt или для загрузки системы.
    - На некоторых компьютерах выход из состояния гибернации («сна») занимает больше времени.

- В отличие от пароля для несистемного тома TrueCrypt, пароль дозагрузочной аутентификации требуется вводить при каждом включении или перезагрузке компьютера. Поэтому если пароль дозагрузочной аутентификации длинный (а он должен быть таковым в целях повышения надёжности защиты), вводить его так часто может быть очень утомительно. Следовательно, вы можете ответить, что вам было удобнее вводить короткий (и потому менее надёжный) пароль для системного раздела (т. е. для обманной системы), а более секретные документы (доступ к которым нужен не так часто) вы предпочли хранить в несистемном разделе TrueCrypt (т. е. во внешнем томе), для которого выбрали очень длинный пароль.

  Поскольку пароль для системного раздела не слишком надёжный (потому что он короткий), вы намеренно не храните важные конфиденциальные данные в системном разделе. Тем не менее, вы предпочитаете, чтобы системный раздел был зашифрован, так как храните на нём потенциально важные и умеренно конфиденциальные данные, с которыми работаете ежедневно (например, пароли от посещаемых вами интернет-форумов, автоматически запоминаемые браузером, историю посещаемых сайтов, запускаемых приложений и т. п.)

- Если неприятель завладеет вашим компьютером в тот момент, когда смонтирован том TrueCrypt (например, когда вы пользуетесь ноутбуком на улице), он в большинстве случаев сможет прочитать любые хранящиеся в томе данные (данные расшифровываются на лету при их считывании). Поэтому может быть разумным ограничить до минимума время, в течение которого том остаётся смонтированным. Очевидно, что это сделать невозможно или затруднительно, если конфиденциальные данные хранятся в зашифрованном системном разделе или на полностью зашифрованном системном диске (потому что при этом вам пришлось бы ограничить до минимума и время работы с компьютером). Следовательно, вы можете ответить, что для хранения особо важных данных вы создали отдельный раздел (зашифрованный другим ключом, нежели системный раздел), монтируете его только при необходимости, а затем как можно скорее размонтируете (поскольку время монтирования этого тома ограничено для минимума). В системном разделе вы храните данные менее важные (но которые вам часто нужны), чем на несистемном разделе (т. е. во внешнем томе).

Требования безопасности и меры предосторожности касательно скрытых ОС

Поскольку скрытая операционная система расположена в скрытом томе TrueCrypt, пользователь скрытой ОС должен соблюдать все правила и меры предосторожности, относящиеся к обычным скрытым томам TrueCrypt. Эти требования, а также дополнительные меры предосторожности, относящиеся именно к скрытым операционным

системам, приведены в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов*.

ВНИМАНИЕ: Если вы не защищаете скрытый том (о том, как это сделать, см. раздел *Защита скрытых томов от повреждений*), *не* записывайте ничего во внешний том (обратите внимание, что обманная операционная система установлена *не* во внешнем томе). В противном случае вы можете перезаписать и повредить скрытый том (и находящуюся внутри него скрытую ОС)!

Если выполнены все инструкции мастера и соблюдены меры предосторожности, указанные в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов*, гарантированно утверждать, что в ПК имеются скрытый том и скрытая операционная система, должно быть невозможно, даже если смонтирован внешний том или расшифрована/запущена обманная ОС.

Главное окно программы

Файл

Позволяет выбрать том TrueCrypt на основе файла. После выбора вы можете выполнить с ним различные операции (например, смонтировать том, нажав кнопку ‘Смонтировать’). Выбрать том также можно перетаскиванием его значка на значок ‘TrueCrypt.exe’ (при этом TrueCrypt будет автоматически запущен) или в главное окно программы.

Устройство

Позволяет выбрать раздел TrueCrypt или устройство хранения данных (например, флэш-накопитель USB). После выбора вы можете выполнить с ним различные операции (например, смонтировать том, нажав кнопку ‘Смонтировать’).

Примечание: монтировать разделы/устройства TrueCrypt можно и более удобным способом – см. подробности в разделе *Автомонтирование*.

Смонтировать

После того, как вы нажмёте кнопку ‘Монтировать’, TrueCrypt попытается смонтировать выбранный том, используя кэшированные (временно сохранённые в памяти) пароли (если таковые имеются), и если ни один из них не подойдёт, попросит вас ввести пароль. Если вы введёте правильный пароль (и/или укажете верные ключевые файлы), том будет смонтирован.
ВАЖНО: Обратите внимание, что когда вы закрываете программу TrueCrypt, драйвер TrueCrypt продолжает работать, и никакие тома TrueCrypt не размонтируются.

Автомонтирование

Эта функция позволяет монтировать разделы/устройства TrueCrypt без необходимости выбирать их вручную (нажатием кнопки *Устройство*). TrueCrypt поочерёдно сканирует заголовки всех доступных разделов/устройств в системе (за исключением накопителей DVD и аналогичных устройств) и пытается смонтировать каждый из них как том TrueCrypt. Обратите внимание, что ни том/устройство TrueCrypt, ни шифр, применявшийся при их шифровании, идентифицировать невозможно. По этой причине программа не может просто “найти” разделы TrueCrypt. Вместо этого она пытается выполнить монтирование каждого (даже незашифрованного) раздела/устройства с помощью всех алгоритмов шифрования и всех сохранённых в кэше паролей (если таковые имеются). Поэтому будьте готовы к тому, что на медленных компьютерах данный процесс может занять много времени.

Если введён неправильный пароль, TrueCrypt попытается выполнить монтирование с использованием кэшированных паролей (если таковые имеются). Если вы указали пустой пароль и не выбрали опцию *Ключ. файлы*, то при попытке автомонтирования

разделов/устройств будут использоваться только кэшированные пароли. Если вам не нужно указывать параметры монтирования, то можно избежать появления запроса пароля: для этого при нажатии кнопки *Автомонтирование* нужно удерживать нажатой клавишу <Shift> (при этом будут использоваться только кэшированные пароли, если таковые имеются).

Буквы дисков будут назначены начиная с той, которая была выбрана в списке дисков в главном окне TrueCrypt.

Размонтировать

Эта функция позволяет размонтировать том TrueCrypt, выбранный в списке дисков на главном окне программы. Размонтировать том TrueCrypt означает закрыть этот том и сделать недоступными операции чтения/записи с этим томом.

Размонтировать все

Примечание: сведения в этом разделе применимы ко всем элементам меню и кнопкам с таким же или похожим названием.

Эта функция позволяет размонтировать сразу несколько томов TrueCrypt. Размонтировать том TrueCrypt означает закрыть этот том и сделать недоступными операции чтения/записи с этим томом. Данная функция размонтирует все смонтированные тома TrueCrypt, за исключением следующих:

- разделы/диски внутри области действия ключа шифрования активной системы (например, системный раздел, зашифрованный TrueCrypt, или не-системный раздел, расположенный на системном диске, зашифрованном TrueCrypt, смонтированный во время работы зашифрованной операционной системы);

- тома TrueCrypt, не полностью доступные из-под учётной записи пользователя (например, том, смонтированный из-под другой учётной записи);

- тома TrueCrypt, не отображаемые в окне программы TrueCrypt, например, системные избранные тома, которые пытались размонтировать с помощью копии TrueCrypt без прав администратора при включённом параметре '*Просматривать/размонтировать системные избранные тома могут лишь администраторы*'.

Очистить кэш

Удаляет из памяти драйвера все кэшированные пароли (где также может находиться содержимое обработанных ключевых файлов). Если в кэше нет паролей, эта кнопка неактивна. О кэшировании паролей см. в разделе *Кэшировать пароли и ключевые файлы*.

Не сохранять историю

Если эта опция *не включена*, имена файлов и/или пути последних двадцати файлов/устройств, которые вы пытались смонтировать как тома TrueCrypt, будут

запоминаться в файле истории (его содержимое отображается при щелчке по стрелке у выпадающего списка “Том” в главном окне программы).

Если эта опция *включена*, TrueCrypt очищает записи в реестре, созданные диалоговыми окнами выбора файлов Windows для TrueCrypt и делает “текущей папкой” домашнюю папку пользователя (в переносном режиме – папку, из которой был запущен TrueCrypt) вне зависимости от того, что выбиралось в диалоговом окне выбора – контейнер или ключевой файл. Поэтому Windows-диалог выбора файлов не будет запоминать путь последнего смонтированного контейнера (или последнего выбранного ключевого файла). Учтите, однако, что описанные в этом разделе операции *не* гарантируют надёжность и безопасность (например, см. *Требования безопасности и меры предосторожности*), поэтому настоятельно рекомендуется на них не полагаться, а шифровать системный раздел/диск.

Более того, если включена эта опция, поле ввода пути к тому в главном окне TrueCrypt очищается при скрытии окна TrueCrypt.

Примечание: чтобы очистить историю томов, выберите в меню *Сервис* команду *Очистить историю томов*.

Выход

Завершает работу программы TrueCrypt. При этом драйвер продолжает работать, и никакие тома TrueCrypt не размонтируются. При работе в переносном (‘portable’) режиме драйвер TrueCrypt выгружается, если он больше не требуется (например, когда все копии главного приложения и/или мастера создания томов закрыты и нет смонтированных томов TrueCrypt). Однако если вы принудительно размонтируете том TrueCrypt, когда программа работает в переносном режиме, или смонтируете доступный для записи отформатированный как NTFS том в среде Windows Vista или более новых версиях Windows, в этом случае драйвер TrueCrypt *не* будет выгружен при выходе из TrueCrypt (он будет выгружен только при завершении работы системы или её перезагрузке). Таким образом предотвращаются различные проблемы, обусловленные ошибкой в Windows (например, был бы невозможен повторный запуск TrueCrypt в течение всего времени, пока есть какие-либо приложения, использующие размонтированный том).

Операции с томами

Изменить пароль тома

См. раздел *Тома -> Изменить пароль тома*.

Установить алгоритм деривации ключа заголовка

См. раздел *Тома -> Установить алгоритм деривации ключа заголовка*.

Создать резервную копию заголовка тома

См. раздел *Сервис -> Создать резервную копию заголовка тома*.

Восстановить заголовок тома

См. раздел *Сервис -> Восстановить заголовок тома*.

Меню программы

Примечание: в целях лаконичности в этой документации описаны только те элементы меню, которые в этом действительно нуждаются, а описание очевидных пунктов опущено.

Тома -> Автомонтирование всех томов на основе устройств

См. раздел *Автомонтирование.*

Тома -> Размонтировать все смонтированные тома

См. раздел *Размонтировать все.*

Тома -> Изменить пароль тома

Позволяет изменить пароль выбранного в данный момент тома TrueCrypt (неважно, скрытого или обычного). Изменяются только ключ заголовка и вторичный ключ заголовка (режим XTS) – мастер-ключ остаётся неизменным. Эта функция выполняет перешифровку заголовка тома с использованием ключа шифрования, полученного из нового пароля. Обратите внимание, что в заголовке тома содержится мастер-ключ шифрования, с помощью которого зашифрован этот том. Поэтому после применения этой функции хранящиеся в томе данные *не* потеряются (смена пароля длится несколько секунд).

Чтобы изменить пароль тома TrueCrypt, нажмите кнопку *Файл* или *Устройство*, затем выберите том и в меню *Тома* выберите команду *Изменить пароль тома*.

Примечание: о том, как изменить пароль для дозагрузочной аутентификации, см. в разделе *Система -> Изменить пароль*.

Также см.главу *Требования безопасности и меры предосторожности*.

PKCS-5 PRF

В этом поле можно выбрать алгоритм, который будет использоваться для деривации (получения) новых ключей заголовка тома (см. подробности в разделе *Деривация ключа заголовка, соль и подсчёт итераций*) и генерирования новой соли (см. подробности в разделе *Генератор случайных чисел*).

Примечание: когда TrueCrypt выполняет перешифрование заголовка тома, исходный заголовок сначала перезаписывается 256 раз случайными данными с целью не дать возможности неприятелю воспользоваться такими технологическими способами, как магнитно-силовая микроскопия или магнитно-силовая сканирующая туннельная

микроскопия [17] для восстановления перезаписанного заголовка (тем не менее, см. также главу *Требования безопасности и меры предосторожности*).

Тома -> Установить алгоритм деривации ключа заголовка

Эта функция позволяет перешифровать заголовок тома с другим ключом заголовка, полученным с помощью иной PRF-функции (например, вместо HMAC-RIPEMD-160 можно воспользоваться HMAC-Whirlpool). Обратите внимание, что в заголовке тома содержится мастер-ключ шифрования, с помощью которого зашифрован этот том. Поэтому после применения этой функции хранящиеся в томе данные *не* потеряются. Более подробные сведения см. в разделе *Деривация ключа заголовка, соль и подсчёт итераций*.

Примечание: когда TrueCrypt выполняет перешифрование заголовка тома, исходный заголовок сначала перезаписывается 256 раз случайными данными с целью не дать возможности неприятелю воспользоваться такими технологическими способами, как магнитно-силовая микроскопия или магнитно-силовая сканирующая туннельная микроскопия [17] для восстановления перезаписанного заголовка (тем не менее, см. также главу *Требования безопасности и меры предосторожности*).

Тома -> Добавить/удалить ключевые файлы в/из том(а)
Тома -> Удалить из тома все ключевые файлы

См. главу *Ключевые файлы.*

Избранное -> Добавить смонтированный том в список избранных томов
Избранное -> Упорядочить избранные тома
Избранное -> Смонтировать избранные тома

См. главу *Избранные тома*.

Избранное -> Добавить смонтированный том в список системных избранных томов
Избранное -> Упорядочить системные избранные тома

См. главу *Системные избранные тома*.

Система -> Изменить пароль

Изменяет пароль дозагрузочной аутентификации (см. главу *Шифрование системы*).

ВНИМАНИЕ: В случае повреждения ключевых данных их можно восстановить с помощью вашего диска восстановления TrueCrypt. При этом также будет восстановлен пароль, который был актуальным на момент создания диска восстановления TrueCrypt. Поэтому при каждой смене пароля следует уничтожать прежний диск восстановления TrueCrypt и

создавать его заново (выбрав *Система -> Создать диск восстановления*). В противном случае неприятель сможет расшифровать ваш системный раздел/диск с помощью старого пароля (если к нему в руки попадёт старый диск восстановления TrueCrypt, и он им воспользуется для восстановления ключевых данных). См. также главу *Требования безопасности и меры предосторожности*.

Более подробные сведения о смене пароля см. в разделе *Тома -> Изменить пароль тома* выше по тексту.

Система -> Смонтировать без дозагрузочной аутентификации

Выберите эту опцию, если вам нужно смонтировать раздел, находящийся в области действия шифрования системы, без дозагрузочной аутентификации. Пример: вы хотите смонтировать раздел, расположенный на зашифрованном системном диске с другой ОС, которая сейчас не запущена. Это может пригодиться, скажем, когда требуется создать резервную копию или восстановить операционную систему, зашифрованную с помощью TrueCrypt (из другой операционной системы).

Примечание: если нужно смонтировать сразу несколько разделов, нажмите кнопку *Автомонтирование*, затем нажмите *Параметры* и включите опцию *Монтировать раздел с шифрованием ОС без дозагрузочной аутентификации*.

Учтите, что эту функцию нельзя использовать для монтирования расширенных (логических) разделов, расположенных на полностью зашифрованном системном диске.

Сервис -> Очистить историю томов

Очищает список с именами файлов (если использовались тома на основе файлов) и путями последних двадцати успешно смонтированных томов.

Сервис -> Настройка переносного диска

См. главу *Портативный (переносной) режим.*

Сервис -> Генератор ключевых файлов

См. раздел *Сервис -> Генератор ключевых файлов* в главе *Ключевые файлы.*

Сервис -> Создать резервную копию заголовка тома
Сервис -> Восстановить заголовок тома

В случае повреждения заголовка тома TrueCrypt, такой том в большинстве случаев невозможно смонтировать. Поэтому каждый том, созданный с помощью TrueCrypt версии 6.0 и новее, содержит встроенную резервную копию заголовка, располагающуюся в конце тома. Ради дополнительной безопасности вы можете также создать внешние файлы с резервными копиями заголовка тома. Для этого нажмите кнопку *Устройство* или *Файл*,

укажите нужный вам том, выберите *Сервис -> Создать резервную копию заголовка тома* и следуйте инструкциям.

Примечание: резервная копия заголовка тома (встроенная или внешняя) это *не* копия исходного заголовка тома, так как тот зашифрован другим ключом заголовка, полученным с помощью другой соли (см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). При изменении пароля и/или ключевых файлов или при восстановлении заголовка из встроенной (или внешней) резервной копии выполняется повторное шифрование как заголовка тома, так и его резервной копии (встроенной в том) с помощью ключей заголовка, полученных посредством вновь сгенерированной соли (соль для заголовка тома отличается от соли для его резервной копии). Каждая соль создаётся TrueCrypt с помощью генератора случайных чисел (см. раздел *Генератор случайных чисел*).

Для восстановления повреждённого заголовка тома можно использовать резервные копии обоих типов (встроенную и внешнюю). Для этого нажмите кнопку *Устройство* или *Файл*, укажите нужный вам том, выберите *Сервис -> Восстановить заголовок тома* и следуйте инструкциям.
ВНИМАНИЕ: При восстановлении заголовка тома также восстанавливается пароль тома, который был действителен на момент создания резервной копии. Более того, если на момент создания резервной копии для монтирования тома требовались ключевые файлы, то после восстановления заголовка для монтирования тома снова потребуются те же ключевые файлы. Более подробную информацию см. в разделе *Схема шифрования*, глава *Технические подробности*.

Однажды создав резервную копию заголовка тома, вам потребуется создать её заново только тогда, когда вы измените пароль и/или ключевые файлы тома. В противном случае, поскольку заголовок тома остаётся неизменным, то и резервная копия заголовка тома тоже не требует обновления.

Примечание: помимо соли (последовательностью случайных чисел), внешние файлы с резервными копиями заголовка тома не содержат никакой незашифрованной информации, и их нельзя расшифровать, не зная правильный пароль и/или не предоставив правильные ключевые файлы. Более подробные сведения см. в главе *Технические подробности*.

При создании внешней резервной копии заголовка в неё помещаются как заголовок обычного тома, так и область, в которой может храниться заголовок скрытого тома, даже если внутри этого тома нет скрытого тома (для сохранения возможности правдоподобного отрицания наличия скрытых томов). Если в томе нет скрытого тома, область, зарезервированная под заголовок скрытого тома, будет заполнена в файле с резервной копией случайными данными (для сохранения возможности правдоподобного отрицания).

При *восстановлении* заголовка тома вам потребуется выбрать тип тома, заголовок которого вы хотите восстановить (обычный или скрытый том). За одну операцию можно восстановить только один заголовок тома. Чтобы восстановить оба заголовка, нужно выполнить операцию дважды (*Сервис -> Восстановить заголовок тома*). Вам будет нужно ввести правильный пароль (или предоставить правильные ключевые файлы), имевший силу на момент создания резервной копии заголовка тома. Паролем (и/или ключевыми файлами) будет также автоматически определяться тип заголовка тома для восстановления, т. е. обычный или скрытый (обратите внимание, что TrueCrypt определяет тип методом проб и ошибок).

Примечание: если при монтировании тома пользователь неправильно укажет пароль (и/или ключевые файлы) два раза подряд, TrueCrypt будет автоматически пытаться смонтировать том, используя встроенную резервную копию заголовка (вдобавок к попытке его монтирования с помощью основного заголовка), при каждой последующей попытке пользователя смонтировать том (пока не будет нажата кнопка *Отмена*). Если TrueCrypt не

удастся расшифровать основной заголовок, но в то же время получится расшифровать встроенную резервную копию заголовка, том будет смонтирован с выдачей пользователю предупреждения о том, что повреждён заголовок тома (и информации, как его восстановить).

Настройки -> Параметры

Вызывает диалоговое окно настроек программы, в котором помимо прочих можно изменить следующие параметры:

Очищать кэш паролей при выходе

Если включено, пароли (а также содержимое обработанных ключевых файлов), кэшированные (сохранённые) в памяти драйвера, будут удалены при выходе из TrueCrypt.

Кэшировать пароли в памяти драйвера

Если включено, пароли и/или содержимое обработанных ключевых файлов для четырёх последних успешно смонтированных томов TrueCrypt будут кэшироваться (временно запоминаться). Это позволяет монтировать тома без необходимости то и дело вводить их пароли (и выбирать ключевые файлы). TrueCrypt никогда не сохраняет никаких паролей на диске (тем не менее, см. главу *Требования безопасности и меры предосторожности*). Кэширование паролей включается/отключается в настройках программы (*Настройки -> Параметры*) и в окне запроса пароля. В случае шифрования системного раздела/диска, кэширование пароля дозагрузочной аутентификации можно включить или выключить в настройках шифрования системы (*Настройки* > '*Шифрование системы*').

Открывать окно Проводника для успешно смонтированного тома

Если включено, то после успешного монтирования тома TrueCrypt будет автоматически открываться окно Проводника с содержимым корневой папки этого тома (например, `T:\`).

Другой значок в системном лотке, если есть смонтированные тома

Если включено, то когда смонтирован том TrueCrypt, в области уведомлений (в системном лотке) отображается другой значок TrueCrypt. Исключение составляют:

- разделы/диски внутри области действия ключа шифрования активной системы (например, системный раздел, зашифрованный TrueCrypt, или не-системный раздел, расположенный на системном диске, зашифрованном TrueCrypt, смонтированный во время работы зашифрованной операционной системы);
- тома TrueCrypt, не полностью доступные из-под учётной записи пользователя (например, том, смонтированный из-под другой учётной записи);
- тома TrueCrypt, не отображаемые в окне программы TrueCrypt, например, системные избранные тома, которые пытались размонтировать с помощью

копии TrueCrypt без прав администратора при включённом параметре '*Просматривать/размонтировать системные избранные тома могут лишь администраторы*'.

Работа TrueCrypt в фоновом режиме – Включено

См. главу *Работа TrueCrypt в фоновом режиме*.

Работа TrueCrypt в фоновом режиме – Выход, если нет смонтированных томов

Если включено, работа TrueCrypt в фоновом режиме автоматически и без выдачи сообщений прекращается, как только в системе не будет смонтированных томов TrueCrypt. Более подробную информацию см. в главе *Работа TrueCrypt в фоновом режиме*. Обратите внимание, что данный параметр нельзя отключить, если TrueCrypt выполняется в переносном (portable) режиме.

Автоматически размонтировать тома при неактивности в течение...

По прошествии *n* минут, в течение которых с томом TrueCrypt не выполнялось никаких операций по записи/считыванию данных, этот том будет автоматически размонтирован.

Автоматически размонтировать тома даже при открытых файлах/папках

Этот параметр применим только к авторазмонтированию (не к обычному размонтированию). Он форсирует размонтирование (без выдачи запроса) автоматически размонтируемого тома в случае, если тот содержит открытые в данный момент файлы или папки (т. е. файлы/папки, используемые системой или приложениями).

Монтирование томов TrueCrypt

Если вы этого ещё не делали, см. разделы *Смонтировать* и *Автомонтирование* в главе *Главное окно программы*.

Кэшировать пароли и ключевые файлы

При выборе этого параметра, в окне ввода пароля он будет действовать только для конкретной попытки монтирования. Но его также можно сделать стандартным (принимаемым по умолчанию) в настройках программы. См. подробности в разделе *Настройки -> Параметры*, подраздел *Кэшировать пароли в памяти драйвера*.

Параметры монтирования

Параметры монтирования влияют на текущий монтируемый том. Чтобы открыть диалоговое окно *Параметры монтирования*, нажмите кнопку *Параметры* в окне ввода пароля. После кэширования правильного пароля, тома при нажатии кнопки *Смонтировать* будут монтироваться автоматически. Если же вам потребуется изменить параметры монтирования тома, уже монтировавшегося с кэшированием пароля, при щелчке по кнопке *Смонтировать* или избранному тому в меню *Избранное* удерживайте нажатой клавишу <Control> (<Ctrl>), либо выберите команду *Смонтировать том с параметрами* в меню *Тома*.

Параметры монтирования, принимаемые по умолчанию, устанавливаются в основных настройках программы (*Настройки -> Параметры).*

Монтировать как том только для чтения

Если включено, смонтированный том будет недоступен для записи данных.

Монтировать том как сменный носитель

См. раздел *Том, смонтированный как сменный носитель*.

По возможности применять копию заголовка, встроенную в том

Все тома, созданные с помощью TrueCrypt версии 6.0 или более новой, содержат встроенную резервную копию заголовка (расположенную в конце тома). Если вы включите эту опцию, TrueCrypt попытается смонтировать том, используя встроенную резервную

копию заголовка. Обратите внимание, что в случае повреждения заголовка тома вам не нужно применять данную опцию. Вместо этого вы можете починить заголовок, выбрав *Сервис* > *Восстановить заголовок тома*.

Монтировать раздел с шифрованием ОС без дозагрузочной аутентификации

Включите этот параметр, если нужно смонтировать раздел, входящий в область действия шифрования системы, без дозагрузочной аутентификации. Пример: вы хотите смонтировать раздел, расположенный на зашифрованном системном диске с другой ОС, которая сейчас не запущена. Это может пригодиться, скажем, когда требуется создать резервную копию или восстановить операционную систему, зашифрованную с помощью TrueCrypt (из другой операционной системы). Обратите внимание, что эту опцию также можно включить при использовании функций *Автомонтирование* или *Автомонтирование всех томов на основе устройств*.

Защита скрытого тома

См. раздел *Защита скрытых томов от повреждений*.

Распараллеливание

Если компьютер оснащён многоядерным процессором (или несколькими процессорами), TrueCrypt при операциях шифрования и дешифрования использует все ядра (или процессоры) параллельно. Например, когда нужно расшифровать порцию данных, сначала эта порция делится им на несколько более мелких частей. Количество частей равно числу ядер (или процессоров). Затем все части расшифровываются параллельно (часть 1 расшифровывается потоком 1, часть 2 – потоком 2, и т. д.). Тот же метод применяется и при шифровании.

Таким образом, если в компьютере установлен, скажем, четырёхядерный процессор, шифрование и дешифрование будут выполняться в четыре раза быстрее, чем при использовании одноядерного процессора с эквивалентными характеристиками (соответственно, в два раза быстрее, чем с помощью двухядерного процессора, и т. д.).

Увеличение скорости шифрования/дешифрования прямо пропорционально числу ядер и/или процессоров.

Примечание: процессоры с технологией Hyper-Threading имеют несколько логических ядер на одном физическом (или несколько логических процессоров в одном физическом). Если в настройках компьютера (например, в BIOS) включена технология Hyper-Threading, TrueCrypt создаёт по одному потоку на каждое логическое ядро/процессор. Так, скажем, на шестиядерном процессоре, имеющим на одном физическом ядре по два логических, TrueCrypt использует 12 потоков.

Если компьютер имеет многоядерный процессор (или несколько процессоров), также выполняется параллельно и деривация ключа заголовка. В результате при использовании многоядерного ЦП (или многопроцессорного ПК) монтирование тома происходит в

несколько раз быстрее, чем при использовании одноядерного ЦП (или однопроцессорного ПК) с аналогичными характеристиками.

Примечание: распараллеливание было впервые реализовано в TrueCrypt 6.0.

Конвейеризация

При шифровании или дешифровании данных TrueCrypt использует так называемую конвейеризацию (асинхронную обработку, pipelining). Когда какое-либо приложение загружает часть файла из зашифрованного TrueCrypt тома/диска, TrueCrypt автоматически расшифровывает её (в ОЗУ). Благодаря конвейеризации, приложению не нужно ждать расшифровки любой части файла, оно может начать загружать другие части файла немедленно. То же самое относится к шифрованию при записи данных в зашифрованный том/диск.

Конвейеризация позволяет считывать и записывать данные на зашифрованном диске так же быстро, как если бы диск не был зашифрован (это применимо к томам TrueCrypt и на основе файла, и на основе раздела).

Примечание: конвейеризация была впервые реализована в TrueCrypt 5.0 и присутствует только в версиях TrueCrypt для Windows.

Аппаратное ускорение

Некоторые процессоры (ЦП) поддерживают аппаратное ускорение шифрования по алгоритму AES,[1] которое в этом случае выполняется, как правило, в 4-8 раз быстрее, чем чисто программное шифрование при использовании тех же процессоров.

По умолчанию TrueCrypt использует аппаратное ускорение AES на компьютерах, оснащённых процессорами, поддерживающими инструкции Intel AES-NI. В частности, TrueCrypt использует инструкции AES-NI при выполнении так называемых AES-раундов (т. е. основных частей алгоритма AES).[2] Для генерирования ключей никакие инструкции AES-NI в TrueCrypt не применяются.

Примечание: по умолчанию TrueCrypt использует аппаратное ускорение AES также при загрузке зашифрованной системы Windows и при её выходе из состояния гибернации (при условии, что процессор поддерживает инструкции Intel AES-NI).

Чтобы выяснить, способен ли TrueCrypt использовать аппаратное ускорение AES в вашем компьютере, выберите *Настройки* > *Быстродействие* и посмотрите, что написано в поле *Процессор в этом ПК поддерживает аппаратное ускорение AES-операций*.

---

[1] В этой главе слово 'шифрование' также означает и дешифрование.

[2] Это инструкции *AESENC*, *AESENCLAST*, *AESDEC* и *AESDECLAST*, они выполняют следующие AES-преобразования: *ShiftRows*, *SubBytes*, *MixColumns*, *InvShiftRows*, *InvSubBytes*, *InvMixColumns* и *AddRoundKey* (более подробные сведения об этих преобразованиях см. в [3]).

Если вы собираетесь приобрести процессор, узнать, поддерживает ли он инструкции Intel AES-NI (также именуемые "AES New Instructions" – "Новые инструкции AES"), которые TrueCrypt применяет для аппаратного ускорения AES-операций, можно в документации на процессор или у поставщика/производителя. Примите, однако, к сведению, что некоторые процессоры Intel, присутствующие в списке совместимых с AES-NI на сайте Intel, в действительности поддерживают инструкции AES-NI только с обновлением конфигурации процессора (Processor Configuration). В этом случае вам необходимо связаться с поставщиком системной платы/компьютера и обновить системную BIOS, чтобы она включала и новейшее обновление Processor Configuration.

Если нужно отключить аппаратное ускорение AES (например, потому что вы хотите, чтобы TrueCrypt использовал только реализацию AES с полностью открытым кодом), выберите *Настройки* > *Быстродействие* и выключите опцию *Ускорять (де)шифрование AES с помощью AES-инструкций процессора*. Обратите внимание, что при изменении состояния этой опции нужно перезагрузить операционную систему, чтобы изменение режима возымело действие на все компоненты TrueCrypt. Также учтите, что когда вы создаёте диск восстановления TrueCrypt (Rescue Disk), состояние этой опции записывается в диск восстановления и используется при каждой загрузке с него (влияя на фазы перед загрузкой и начальной загрузки). Чтобы создать новый диск восстановления TrueCrypt, выберите *Система* > *Создать диск восстановления*.

Примечание: аппаратное ускорение было впервые реализовано в TrueCrypt 7.0.

Горячие клавиши

Чтобы задать общесистемные горячие клавиши TrueCrypt, выберите в меню *Настройки* команду *Горячие клавиши*. Обратите внимание, что горячие клавиши работают только когда TrueCrypt запущен или работает в фоновом режиме.

Ключевые файлы

Ключевой файл это файл, чьё содержимое объединено с паролем (информацию о методе, используемом для объединения ключевого файла с паролем, см. в главе *Технические подробности*, раздел *Ключевые файлы*). Пока не будет предоставлен правильный ключевой файл, ни один том, использующий этот ключевой файл, не может быть смонтирован.

Использовать ключевые файлы необязательно. Тем не менее, их применение даёт ряд преимуществ. Ключевые файлы:

- могут повысить стойкость защиты к атакам методом полного перебора (brute force), особенно при недостаточно надёжном пароле тома;
- позволяют использовать токены безопасности и смарт-карты (см. ниже);
- позволяют нескольким пользователям монтировать один том, используя разные пароли или PIN-коды: просто снабдите каждого пользователя токеном безопасности

или смарт-картой, содержащими один и тот же ключевой файл TrueCrypt, и позвольте им выбрать свой собственный пароль или PIN для защиты их токенов безопасности или смарт-карт;

- позволяют управлять многопользовательским *совместным* доступом (все владельцы ключевых файлов должны представить свои ключевые файлы, прежде чем том можно будет смонтировать).

В качестве ключевого файла TrueCrypt можно использовать файл любого типа (например, .txt, .exe, .mp3[1], .avi), однако мы рекомендуем отдавать предпочтение сжатым файлам (таким, как .mp3, .jpg, .zip и т. д.). Обратите внимание, что TrueCrypt никогда не изменяет содержимое ключевых файлов.

Разрешается выбирать более одного ключевого файла; их последовательность значения не имеет. Кроме того, ключевой файл со случайным содержимым может сгенерировать и непосредственно TrueCrypt. Чтобы это сделать, выберите *Сервис -> Генератор ключевых файлов*.

Примечание: для шифрования системы ключевые файлы в данный момент не поддерживаются.

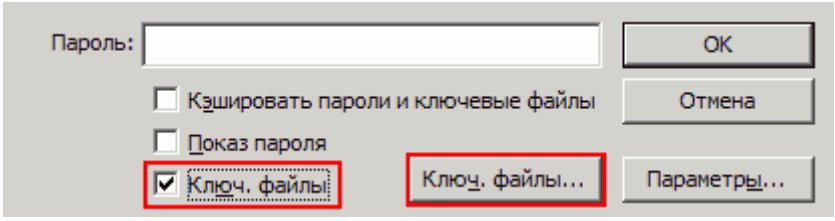
ВНИМАНИЕ: Если вы потеряете ключевой файл или в ключевом файле будет изменён хотя бы один бит в первых 1024 килобайтах, монтировать тома, использующие этот ключевой файл, станет невозможно*!*

ПРЕДУПРЕЖДЕНИЕ: Если включено кэширование паролей, в кэше паролей также будет сохраняться содержимое ключевых файлов, использованных для успешного монтирования тома. После этого том можно будет повторно монтировать даже в случае отсутствия/недоступности ключевого файла. *Чтобы этого избежать, нажмите* Очистить кэш *или отключите кэширование паролей (см. раздел* Настройки -> Параметры, *подраздел* Кэшировать пароли в памяти драйвера).

См. также информацию о выборе паролей и ключевых файлов в главе *Требования безопасности и меры предосторожности*.

Диалоговое окно ключевых файлов

Если вы хотите воспользоваться ключевыми файлами (т. е. “применить” их) при создании или монтировании томов или при изменении паролей, в вашем распоряжении опция *Ключ. файлы* и кнопка *Ключ. файлы* ниже поля ввода пароля.



[1] Если в качестве ключевого используется файл MP3 (или аналогичного формата, в котором применяются служебные поля – «теги»), необходимо убедиться, что никакая программа не изменяет внутри него теги ID3 (название композиции, имя исполнителя и т. д.). В противном случае монтировать тома с помощью этого ключевого файла будет невозможно.

Эти управляющие элементы присутствуют в разных диалоговых окнах, но всегда выполняют одинаковые функции. Включите опцию *Ключ. файлы* и нажмите кнопку *Ключ. файлы*. При этом должно появиться диалоговое окно, в котором вы сможете указать ключевые файлы (чтобы это сделать, нажмите кнопку *Файлы* или *Токен-файлы*) *или* путь поиска ключевых файлов (нажмите кнопку *Путь*).

Токены безопасности и смарт-карты

TrueCrypt может непосредственно использовать ключевые файлы, находящиеся на токенах безопасности или на смарт-картах, соответствующих стандарту PKCS #11 (2.0 или новее) [23], что позволяет пользователю сохранять файл (объект данных) на токене/карте. Чтобы использовать такие файла в качестве ключевых файлов TrueCrypt, нажмите кнопку *Токен-файлы* (в диалоговом окне ключевых файлов).

Доступ к хранящемуся в токене безопасности или смарт-карте ключевому файлу, как правило, защищён PIN-кодами, которые можно ввести либо с аппаратной цифровой клавиатуры («пинпада»), либо из интерфейса TrueCrypt. Кроме того, возможны и другие методы защиты, например, с помощью сканирования отпечатков пальцев.

Чтобы предоставить TrueCrypt доступ с токену безопасности или смарт-карте, необходимо сначала установить программную библиотеку PKCS #11 (2.0 или новее) для этого токена или смарт-карты. Такая библиотека может либо поставляться вместе с устройством, либо быть доступной для загрузки на сайте поставщика или других сторонних фирм.

Если в вашем токене безопасности или смарт-карте нет файлов (объектов данных), которые можно было бы использовать в качестве ключевых файлов TrueCrypt, вы можете воспользоваться TrueCrypt для импорта любого файла на токен безопасности или смарт-карту (если это поддерживается устройством). Чтобы это сделать, выполните следующее:

1. В диалоговом окне ключевых файлов нажмите кнопку *Токен-файлы*.
2. Если токен или смарт-карта защищены PIN-кодом, паролем или иным способом (например, считывателем отпечатков пальцев), идентифицируйте себя (например, введя PIN-код на пинпаде).
3. В появившемся диалоговом окне *Ключевые файлы токена безопасности* нажмите *Импорт кл.файла в токен* и выберите файл, который вы хотите импортировать в токен или смарт-карту.

Обратите внимание, что можно импортировать, например, 512-бит ключевые файлы со случайным содержимым, созданные с помощью TrueCrypt (см. *Сервис -> Генератор ключевых файлов* ниже).

Чтобы закрыть все открытые сеансы токена безопасности, либо выберите *Сервис* > *Закрыть все токен-сессии*, либо определите и воспользуйтесь комбинацией горячих клавиш (*Настройки* > *Горячие клавиши* > *Закрыть все токен-сессии*).

Путь поиска ключевых файлов

Добавив папку в диалоговом окне ключевых файлов (для этого нажмите кнопку *Путь*), вы тем самым укажете *путь поиска ключевых файлов*. Все файлы, обнаруженные в пути поиска ключевых файлов,[1] будут использоваться как ключевые.

ВАЖНО: Обратите внимание, что папки (и содержащиеся в них файлы), найденные в путях поиска ключевых файлов, игнорируются.

Пути поиска ключевых файлов особенно удобны, если вы, например, храните ключевые файлы на USB-накопителе («флэшке»), который всегда носите с собой. В этом случае можно назначить букву диска USB-накопителя как путь поиска ключевых файлов, принимаемый по умолчанию. Чтобы это сделать, выберите *Настройки -> Ключевые файлы по умолчанию*. Затем нажмите кнопку *Путь*, укажите букву диска, присвоенную USB-накопителю, и нажмите *OK*. Теперь при каждом монтировании тома (при условии, что в диалоговом окне ввода пароля включена опция *Ключ. файлы*) TrueCrypt будет просматривать этот путь и использовать все файлы, которые он обнаружит в USB-накопителе, как ключевые.

ВНИМАНИЕ: Когда вы добавляете в список ключевых файлов папку (в отличие от файла), запоминается только путь, но не имена файлов! Это означает, что, например, если создать в этой папке новый файл или скопировать в неё ещё один какой-либо файл, то все тома, которые используют ключевые файлы из этой папки, будет невозможно смонтировать (до тех пор, пока из папки не будет удалён этот новый файл).

Пустой пароль и ключевой файл

Если используется ключевой файл, пароль может быть пустым, т. е. ключевой файл может служить единственным элементом, необходимым для монтирования тома (чего мы делать не рекомендуем). Если при монтировании тома установлены ключевые файлы по умолчанию и включено их использование, то перед запросом пароля TrueCrypt сначала автоматически пытается выполнить монтирование с помощью пустого пароля и ключевых файлов по умолчанию (это, однако, не относится к функции *Автомонтирование*). Если нужно задать параметры монтирования (например, чтобы смонтировать тот как доступный только для чтения, включить защиту скрытого тома, и т. д.) для тома, который уже был смонтирован таким способом, то при щелчке по кнопке *Монтировать* удерживайте нажатой клавишу <Control> (<Ctrl>) (или выберите команду *Смонтировать том с параметрами* в меню *Тома*). Этим вы откроете диалоговое окно *Параметры монтирования*.

Быстрый выбор

Ключевые файлы или пути поиска ключевых файлов можно быстро выбирать следующими способами:

- щёлкните правой кнопкой мыши на кнопке *Ключ. файлы* в диалоговом окне ввода пароля и выберите один из пунктов в появившемся меню;

[1] Обнаруженные во время монтирования тома, изменения его пароля или выполнения любой другой операции, вызывающей перешифрование заголовка тома.

- перетащите значки соответствующих файлов/папок в окно ключевых файлов или в окно ввода пароля.

Тома -> Добавить/удалить ключевые файлы в/из том(а)

Эта функция позволяет выполнить повторное шифрование заголовка тома с помощью ключа шифрования заголовка, полученного из любого количества ключевых файлов (с паролем или без него) или без ключевых файлов вовсе. Так, том, для монтирования которого требуется только пароль, можно преобразовать в том, для успешного монтирования которого нужны ключевые файлы (в дополнению к паролю). Обратите внимание, что в заголовке тома содержится мастер-ключ шифрования, с помощью которого зашифрован этот том. Поэтому при использовании этой функции хранящиеся в томе данные *не* потеряются.

Эту функцию также можно использовать, чтобы изменить/установить ключевые файлы тома (т. е. чтобы удалить некоторые или все ключевые файлы и применить новые).

Замечание: эта функция внутренне равносильна функции смены пароля.

Когда TrueCrypt выполняет перешифрование заголовка тома, исходный заголовок сначала перезаписывается 256 раз случайными данными с целью не дать возможности неприятелю воспользоваться такими технологическими способами, как магнитно-силовая микроскопия или магнитно-силовая сканирующая туннельная микроскопия [17] для восстановления перезаписанного заголовка (тем не менее, см. также главу *Требования безопасности и меры предосторожности*).

Тома -> Удалить из тома все ключевые файлы

Эта функция позволяет выполнить повторное шифрование заголовка тома с помощью ключа шифрования заголовка, полученного из пароля и без участия ключевых файлов (т. е. чтобы для монтирования тома нужно было указывать только пароль, без каких-либо ключевых файлов). Обратите внимание, что в заголовке тома содержится мастер-ключ шифрования, с помощью которого зашифрован этот том. Поэтому при использовании этой функции хранящиеся в томе данные *не* потеряются.

Замечание: эта функция внутренне равносильна функции смены пароля.

Когда TrueCrypt выполняет перешифрование заголовка тома, исходный заголовок сначала перезаписывается 256 раз случайными данными с целью не дать возможности неприятелю воспользоваться такими технологическими способами, как магнитно-силовая микроскопия или магнитно-силовая сканирующая туннельная микроскопия [17] для восстановления перезаписанного заголовка (тем не менее, см. также главу *Требования безопасности и меры предосторожности*).

Сервис -> Генератор ключевых файлов

Эта функция служит для генерирования файла со случайным содержимым, который можно использовать в качестве ключевого файла (рекомендуется). В этой функции используется

реализованный в TrueCrypt генератор случайных чисел. Обратите внимание, что размер результирующего файла всегда равен 64 байтам (т. е. 512 битам), что также является максимально возможной длиной пароля TrueCrypt.

Настройки -> Ключевые файлы по умолчанию

Используйте эту функцию, чтобы установить используемые по умолчанию ключевые файлы и/или пути поиска ключевых файлов. Эта функция особенно удобна, если вы, например, храните ключевые файлы на USB-накопителе («флэшке»), который всегда носите с собой. В этом случае вы можете добавить его букву диска в используемую по умолчанию конфигурацию ключевых файлов. Чтобы это сделать, нажмите кнопку *Путь*, укажите букву диска, присвоенную USB-накопителю, и нажмите *OK*. Теперь при каждом монтировании тома (при условии, что в диалоговом окне ввода пароля включена опция *Ключ. файлы*) TrueCrypt будет просматривать этот путь и использовать все файлы, которые он там обнаружит, как ключевые.

ВНИМАНИЕ: Когда вы добавляете в список ключевых файлов папку (в отличие от файла), запоминается только путь, но не имена файлов! Это означает, что, например, если создать в этой папке новый файл или скопировать в неё ещё один какой-либо файл, то все тома, которые используют ключевые файлы из этой папки, будет невозможно смонтировать (до тех пор, пока из папки не будет удалён этот новый файл).

ВАЖНО: Обратите внимание, что когда вы устанавливаете используемые по умолчанию ключевые файлы и/или пути поиска ключевых файлов, имена файлов и пути сохраняются в файле Default Keyfiles.xml *в незашифрованном виде. Подробности см. в главе* Системные файлы TrueCrypt и программные данные*.*

Токены безопасности и смарт-карты

TrueCrypt поддерживает использование токенов безопасности (или криптографических) и смарт-карт (считывателей смарт-карт), доступ к которым выполняется по протоколу PKCS #11 (2.0 или новее) [23]. Подробности см. в разделе *Токены безопасности и смарт-карты*, глава *Ключевые файлы*.

Портативный (переносной) режим

Программа TrueCrypt может работать в так называемом портативном (portable) режиме, т. е. без необходимости быть установленной (инсталлированной) в системе, в среде которой она запущена. Тем не менее, при этом нужно помнить о паре вещей:

1) Чтобы запустить TrueCrypt в портативном режиме, необходимо иметь права администратора компьютера (причины этого см. в главе *Использование TrueCrypt без прав администратора*).

   Примечание: вне зависимости от типа используемого программного обеспечения, с точки зрения сохранности персональной информации *небезопасно* работать с конфиденциальными данными в системе, где у вас нет привилегий администратора, так как администратор может без труда получить и скопировать ваши конфиденциальные данные, в том числе пароли и ключи.

2) Прибегнув к исследованию файла реестра, можно выяснить, что в Windows запускалась программа TrueCrypt (и что монтировался том TrueCrypt), даже если использовался портативный режим.

Примечание: если для вас это реально существующая проблема, см. данный вопрос.

*З*апускать TrueCrypt в портативном режиме можно двумя способами:

1) Можно непосредственно запустить файл *TrueCrypt.exe* после извлечения файлов из самораспаковывающегося дистрибутивного пакета TrueCrypt.

   Примечание: чтобы извлечь файлы из самораспаковывающегося дистрибутивного пакета TrueCrypt, запустите его и выберите на второй странице мастера установки TrueCrypt пункт *Extract* (вместо *Install*).
   Примечание переводчика: если в папке с самораспаковывающимся дистрибутивным пакетом у вас также находится русский языковый файл TrueCrypt, на второй странице мастера установки нужный пункт будет называться *Извлечь* (выберите его вместо *Установить*).

2) Можно воспользоваться функцией настройки *переносного диска* (*Traveler Disk)*, чтобы подготовить специальный носимый с собой диск и запускать TrueCrypt с него.

Второй вариант имеет ряд преимуществ, описанных ниже в этой главе.

Примечание: при работе в переносном (‘portable’) режиме драйвер TrueCrypt выгружается, когда он становится больше не нужен (например, когда закрыты все копии главного приложения и/или мастера создания томов и нет смонтированных томов TrueCrypt). Тем не менее, при форсированном размонтировании тома TrueCrypt, когда TrueCrypt работает в переносном режиме, или монтировании доступного для записи отформатированного как NTFS тома в среде Windows Vista или новее, драйвер TrueCrypt может *не* быть выгруженным при выходе из TrueCrypt (он будет выгружен только при завершении работы системы или её перезагрузке). Этим предотвращаются различные проблемы, обусловленные ошибкой в Windows (например, невозможность повторного запуска TrueCrypt до тех пор, пока размонтированный том используется какими-либо приложениями).

Сервис -> Настройка переносного диска

Эта функция служит для подготовки специального переносного диска для запуска с него TrueCrypt. Обратите внимание, что ‘переносной диск’ TrueCrypt это *не* том TrueCrypt, а *незашифрованный* том. ‘Переносной диск’ содержит исполняемые файлы TrueCrypt и, дополнительно, файл-сценарий ‘autorun.inf’ (см. ниже раздел *Настройка автозапуска*). При выборе *Сервис -> Настройка переносного диска* появится диалоговое окно *Настройка переносного диска*. Далее приведено описание некоторых параметров в этом диалоговом окне, нуждающихся в пояснении.

С мастером создания томов TrueCrypt

Включите эту опцию, если вы намереваетесь создавать новые тома TrueCrypt, запуская TrueCrypt с переносного диска, который вы подготавливаете. Отключение данной опции сэкономит место на переносном диске.

Настройка автозапуска (файл autorun.inf)

Данная группа параметров позволяет настроить ‘переносной диск’ на автоматический запуск TrueCrypt или монтирование указанного тома TrueCrypt при вставке ‘переносного диска’. Это делается путём создания на переносном диске особого файла-сценария с именем ‘*autorun.inf*’. Указанный файл автоматически выполняется операционной системой всякий раз при вставке ‘переносного диска’.

Обратите, однако, внимание, что данная функция работает лишь с такими сменными носителями, как диски CD/DVD (для работы с флэш-накопителями USB требуется Windows XP SP2, Windows Vista или более новая версия Windows), и только в том случае, если это разрешено в операционной системе. В зависимости от конфигурации ОС, эти функции автозапуска и автомонтирования могут работать, только если файлы переносного диска расположены на носителе, доступном только для чтения, например, CD/DVD (это не ошибка в TrueCrypt, а ограничение Windows).

Также примите к сведению, что файл ‘*autorun.inf*’ должен находиться в корневой папке (т. е., например, в *G:*\, *X:*\, *Y:*\ и т. д.) на **незашифрованном** диске, иначе данная функция работать не будет.

Языковые пакеты

Языковые пакеты содержат выполненные сторонними лицами переводы текстов интерфейса TrueCrypt. Некоторые языковые пакеты также включают переведённое Руководство пользователя TrueCrypt. Обратите внимание, что в настоящий момент языковые пакеты поддерживаются только версией TrueCrypt для Windows.

Установка

Чтобы установить языковый пакет, выполните следующее:

1. Загрузите языковый пакет с сайта TrueCrypt по адресу: http://www.truecrypt.org/localizations
2. Извлеките файлы из языкового пакета (архива) в папку, в которой у вас установлена программа TrueCrypt, т. е. в папку, где находится файл '*TrueCrypt.exe*'; например, в '*C:\Program Files\TrueCrypt*'.
3. Запустите TrueCrypt.
4. Выберите *Settings -> Language* (*Настройки -> Язык*), щёлкните мышью по пункту с желаемым языком и нажмите *OK*.

Чтобы вернуть английский язык, выберите *Настройки -> Язык (Language)*. Затем щёлкните по пункту *English* и нажмите *OK*.

Алгоритмы шифрования

Тома TrueCrypt могут быть зашифрованы с помощью следующих алгоритмов:

Алгоритм	Разработчики	Размер ключа (бит)	Размер блока (бит)	Режим операции
AES	J. Daemen, V. Rijmen	256	128	XTS
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	XTS
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpent		256; 256; 256	128	XTS
Serpent-AES		256; 256	128	XTS
Serpent-Twofish-AES		256; 256; 256	128	XTS
Twofish-Serpent		256; 256	128	XTS

Информацию о режиме XTS см. в разделе *Режимы операции*.

AES

Advanced Encryption Standard (AES) это одобренный FIPS (Федеральные стандарты обработки информации) криптографический алгоритм (также известен как Rijndael, авторы: Joan Daemen и Vincent Rijmen, создан в 1998 г.), разрешённый к применению федеральными ведомствами и учреждениями США для криптостойкой защиты секретной информации [3]. TrueCrypt использует AES с 14 раундами и 256-бит ключом (т. е. стандарт AES-256, опубликованный в 2001 г.), работающий в режиме XTS (см. раздел *Режимы операции*).

В июне 2003 г., после того как Агентство национальной безопасности США (NSA, US National Security Agency) провело исследование и анализ AES, американский комитет CNSS (Committee on National Security Systems) объявил в [1], что реализация и надёжность AES-256 (и AES-192) достаточны для защиты секретной информации вплоть до уровня Top Secret («совершенно секретно»). Это относится ко всем правительственным ведомствам и учреждениям США, рассматривающих приобретение или использование продуктов, включающих Advanced Encryption Standard (AES), для обеспечения требований информационной безопасности, связанных с защитой национальных систем безопасности и/или информации, связанной с госбезопасностью [1].

Serpent

Данный шифр создали Ross Anderson, Eli Biham и Lars Knudsen; алгоритм был опубликован в 1998 г. Он использует ключ длиной 256 бит и блок размером 128 бит, работает в режиме XTS (см. раздел *Режимы операции*). Serpent был одним из финалистов конкурса AES. В результате голосования он занял второе место, уступив алгоритму AES (Rijndael), хотя и выглядит как имеющий больший запас надёжности, нежели Rijndael [4]. Говоря точнее, Serpent выглядит как имеющий *высокий* запас надёжности, тогда как Rijndael – только *достаточный* запас [4]. Кроме того, в адрес алгоритма Rijndael раздавались критические замечания о том, что его математическая структура в будущем может подвергнуться атакам [4].

В документе [5] команда Twofish представила таблицу коэффициентов надёжности финалистов конкурса AES. Коэффициент безопасности определялся следующим образом: число раундов полного шифра делилось на наибольшее число раундов, которые были взломаны. Следовательно, взломанный шифр имеет наименьший коэффициент безопасности, равный 1. Среди финалистов конкурса AES наибольший коэффициент безопасности оказался у Serpent: 3,56 (для всех поддерживаемых размеров ключей). Коэффициент безопасности алгоритма Rijndael-256 составил 1,56.

Несмотря на эти факты, победителем в конкурсе AES был выбран всё-таки Rijndael за его сочетание надёжности, производительности, эффективности, возможностей реализации и гибкости [4]. На последней конференции AES алгоритм Rijndael получил 86 голосов, Serpent – 59, Twofish – 31, RC6 – 23, и MARS – 13 голосов [18, 19].[1]

Twofish

Шифр создали Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall и Niels Ferguson; опубликован в 1998 г. Он использует ключ длиной 256 бит и блок размером 128 бит, работает в режиме XTS (см. раздел *Режимы операции*). Twofish был одним из финалистов конкурса AES. Отличительная особенность – применение зависящих от ключа S-box'ов. Twofish можно рассматривать как совокупность 2^{128} различных криптосистем, где выбором криптосистемы управляют 128 бит, получаемые деривацией 256-бит ключа [4]. В документе [13] команда Twofish заявляет, что зависящие от ключа S-box'ы представляют собой форму запаса надёжности от неизвестных атак [4].

AES-Twofish

[1] Это голоса «за». Если вычесть голоса «против» из голосов «за», результаты следующие: Rijndael: 76 голосов, Serpent: 52 голоса, Twofish: 10 голосов, RC6: -14 голосов, MARS: -70 голосов [19].

Последовательно выполняемые (каскадом) [15, 16] два шифра, работающие в режиме XTS (см. раздел *Режимы операции*). Каждый блок размером 128 бит сначала шифруется алгоритмом Twofish (с длиной ключа 256 бит) в режиме XTS, а затем алгоритмом AES (с длиной ключа 256 бит) также в режиме XTS. Каждый из этих каскадных шифров использует свой собственный ключ. Все ключи шифрования взаимонезависимы (обратите внимание, что ключи заголовка также независимы, хотя и получены в результате деривации одного пароля – см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). Информация о каждом отдельном шифре приведена выше.

AES-Twofish-Serpent

Последовательно выполняемые (каскадом) [15, 16] три шифра, работающие в режиме XTS (см. раздел *Режимы операции*). Каждый блок размером 128 бит сначала шифруется алгоритмом Serpent (с длиной ключа 256 бит) в режиме XTS, затем алгоритмом Twofish (с длиной ключа 256 бит) в режиме XTS, и, наконец, алгоритмом AES (с длиной ключа 256 бит) в режиме XTS. Каждый из этих каскадных шифров использует свой собственный ключ. Все ключи шифрования взаимонезависимы (обратите внимание, что ключи заголовка также независимы, хотя и получены в результате деривации одного пароля – см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). Информация о каждом отдельном шифре приведена выше.

Serpent-AES

Последовательно выполняемые (каскадом) [15, 16] два шифра, работающие в режиме XTS (см. раздел *Режимы операции*). Каждый блок размером 128 бит сначала шифруется алгоритмом AES (с длиной ключа 256 бит) в режиме XTS, а затем алгоритмом Serpent (с длиной ключа 256 бит) также в режиме XTS. Каждый из этих каскадных шифров использует свой собственный ключ. Все ключи шифрования взаимонезависимы (обратите внимание, что ключи заголовка также независимы, хотя и получены в результате деривации одного пароля – см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). Информация о каждом отдельном шифре приведена выше.

Serpent-Twofish-AES

Последовательно выполняемые (каскадом) [15, 16] три шифра, работающие в режиме XTS (см. раздел *Режимы операции*). Каждый блок размером 128 бит сначала шифруется алгоритмом AES (с длиной ключа 256 бит) в режиме XTS, затем алгоритмом Twofish (с длиной ключа 256 бит) в режиме XTS, и, наконец, алгоритмом Serpent (с длиной ключа 256 бит) в режиме XTS. Каждый из этих каскадных шифров использует свой собственный ключ. Все ключи шифрования взаимонезависимы (обратите внимание, что ключи заголовка также независимы, хотя и получены в результате деривации одного пароля – см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). Информация о каждом отдельном шифре приведена выше.

Twofish-Serpent

Последовательно выполняемые (каскадом) [15, 16] два шифра, работающие в режиме XTS (см. раздел *Режимы операции*). Каждый блок размером 128 бит сначала шифруется алгоритмом Serpent (с длиной ключа 256 бит) в режиме XTS, а затем алгоритмом Twofish (с длиной ключа 256 бит) также в режиме XTS. Каждый из этих каскадных шифров использует

свой собственный ключ. Все ключи шифрования взаимонезависимы (обратите внимание, что ключи заголовка также независимы, хотя и получены в результате деривации одного пароля – см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*). Информация о каждом отдельном шифре приведена выше.

Алгоритмы хеширования

Выбор алгоритма хеширования предлагается в мастере создания томов, в диалоговом окне ввода пароля, а также в диалоговом окне генератора ключевых файлов. Выбранный пользователем алгоритм хеширования применяется реализованным в TrueCrypt генератором случайных чисел как функция псевдослучайного “смешивания”, а также механизмом деривации ключа заголовка (HMAC – алгоритмом усиления криптостойкости других криптоалгоритмов на основе хеш-функции, как определено в PKCS #5 v2.0) как псевдослучайную функцию. При создании нового тома, генератором случайных чисел создаются мастер-ключ, вторичный ключ (режим XTS) и соль. Более подробную информацию см. в разделах *Генератор случайных чисел* и *Деривация ключа заголовка, соль и подсчёт итераций*.

RIPEMD-160

Этот опубликованный в 1996 г. хеш-алгоритм создали Hans Dobbertin, Antoon Bosselaers и Bart Preneel в открытом академическом сообществе. Размер вывода RIPEMD-160 равен 160 битам. RIPEMD-160 это улучшенная версия хеш-функции RIPEMD, разработанной в рамках проекта RIPE (*RACE Integrity Primitives Evaluation*) Европейского союза в 1988-1992 годах. RIPEMD-160 был принят Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) в международном стандарте ISO/IEC 10118-3:2004 [21].

SHA-512

Хеш-алгоритм SHA-512 создан Агентством национальной безопасности США (NSA) и опубликован американским Национальным институтом стандартов и технологий (NIST) в FIPS PUB 180-2 [14] в 2002 г. (первый черновой проект был опубликован в 2001 г.). Размер вывода этого алгоритма равен 512 битам.

Whirlpool

Хеш-алгоритм Whirlpool создали Vincent Rijmen (соавтор алгоритма шифрования AES) и Paulo S. L. M. Barreto. Размер вывода этого алгоритма равен 512 битам. Первая версия Whirlpool, сейчас называемая Whirlpool-0, была опубликована в ноябре 2000 г. Вторая версия, носящая сегодня имя Whirlpool-T, была отобрана в набор криптографических примитивов (похожий на конкурс AES проект, организованный Европейским союзом) для NESSIE (*New European Schemes for Signatures, Integrity and Encryption*). TrueCrypt использует третью (последнюю) версию Whirlpool, принятую Международной организацией

по стандартизации (ISO) и Международной электротехнической комиссией (IEC) в международном стандарте ISO/IEC 10118-3:2004 [21].

Поддерживаемые операционные системы

Примечание: после того, как была выпущена эта версия TrueCrypt, могла появиться новая операционная система, проверенная на полную совместимость с TrueCrypt и добавленная в список поддерживаемых ОС. Поэтому если это самая новая стабильная версия TrueCrypt, вам следует ознакомиться с интернет-версией данной главы по адресу http://www.truecrypt.org/docs/?s=supported-operating-systems.

Эта версия TrueCrypt поддерживает следующие операционные системы:

- Windows 7 (32- и 64-разрядные версии)
- Windows Vista
- Windows Vista x64 (64-разрядная версия)
- Windows XP
- Windows XP x64 (64-разрядная версия)
- Windows Server 2008 R2 (64-разрядная версия)
- Windows Server 2008
- Windows Server 2008 x64 (64-разрядная версия)
- Windows Server 2003
- Windows Server 2003 x64 (64-разрядная версия)
- Windows 2000 SP4

- Mac OS X 10.7 Lion (32- и 64-разрядные версии)
- Mac OS X 10.6 Snow Leopard
- Mac OS X 10.5 Leopard
- Mac OS X 10.4 Tiger

- Linux (32- и 64-разрядные версии, ядро 2.6 или совместимое)

Примите к сведению, что следующие операционные системы (помимо прочих) не поддерживаются: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, встроенные/планшетные версии Windows.

См. также раздел *Операционные системы, поддерживающие системное шифрование*.

Использование в режиме командной строки

Информация в этом разделе применима к версии TrueCrypt для Windows. Сведения об использовании в режиме командной строки **версий для Linux и Mac OS X** можно получить, выполнив следующую команду: `truecrypt -h`

/help или */?*	Показать справку по использованию в командной строке.
/volume или */v*	Имя файла и путь тома TrueCrypt для монтирования (не используйте при размонтировании). Чтобы смонтировать том на основе раздела/устройства, используйте, например, `/v \Device\Harddisk1\Partition3` (узнать путь к разделу/устройству можно, запустив TrueCrypt и нажав кнопку *Устройство*). Монтировать раздел или динамический том также можно используя его имя тома (например, `/v \\?\Volume{5cceb196-48bf-46ab-ad00-70965512253a}\`). Узнать имя тома можно, например, с помощью `mountvol.exe`. Также помните, что в путях устройств учитывается регистр букв.
/letter или */l*	Буква диска, присваиваемая монтируемому тому. Если ключ `/l` опущен и указан ключ `/a`, то тому присваивается первая незанятая буква диска.
/explore или */e*	Открыть окно Проводника после монтирования тома.
/beep или */b*	Звуковой сигнал после успешного монтирования или размонтирования.
/auto или */a*	Если этот ключ указан без параметров, то выполняется автоматическое монтирование тома. Если указан параметр `devices` (пример: `/a devices`), то выполняется автомонтирование всех доступных в данный момент томов TrueCrypt на основе устройств/разделов. Если указан параметр `favorites`, то выполняется автомонтирование избранных томов. Обратите внимание, что ключ `/auto` подразумевается, если указаны ключи `/quit` и `/volume`. Если требуется подавить вывод на экран окна программы, используйте ключ `/quit`.

/dismount или */d* — Размонтировать том с указанной буквой диска (например, `/d x`). Если буква диска не указана, будут размонтированы все смонтированные в данный момент тома TrueCrypt.

/force или */f* — Принудительно размонтировать (если размонтируемый том содержит файлы, используемые системой или какой-либо программой) и принудительно смонтировать в совместно используемом (shared) режиме (т. е. без эксклюзивного доступа).

/keyfile или */k* — Указать ключевой файл или путь поиска ключевых файлов. В случае нескольких ключевых файлов, параметры выглядят, например, так: `/k c:\keyfile1.dat /k d:\KeyfileFolder /k c:\kf2`
Чтобы указать ключевой файл, находящийся в токене безопасности или смарт-карте, используйте следующий синтаксис: `token://slot/`*SLOT_NUMBER*`/file/`*FILE_NAME*

/tokenlib — Использовать указанную библиотеку PKCS #11 для токенов безопасности и смарт-карт.

/cache или */c* — `y` или без параметров: включить кэширование паролей; `n`: отключить кэширование паролей (пример: `/c n`). Обратите внимание, что при отключении кэширования пароли в кэше не удаляются (чтобы очистить кэш паролей, используйте ключ `/w`).

/history или */h* — `y` или без параметров: включить сохранение истории смонтированных томов; `n`: отключить сохранение истории томов (пример: `/h n`).

/wipecache или */w* — Удалить все пароли, кэшированные (сохранённые) в памяти драйвера.

/password или */p* — Пароль тома. Если в пароле есть пробелы, он должен быть заключён в двойные кавычки (например, `/p "My Password"`). Чтобы указать пустой пароль, используйте ключ `/p ""`. ***ВНИМАНИЕ: Такой метод ввода пароля может быть небезопасен, например, если на незашифрованном диске записывается незашифрованная история операций в командной строке.***

/quit или */q* — Автоматически выполнить запрошенные действия и выйти (без отображения главного окна TrueCrypt). Если в качестве параметра указано `preferences` (пример: `/q preferences`), то будут загружены/сохранены настройки программы, и они переопределят параметры, указанные в командной строке.
`/q background` запускает TrueCrypt в фоновом режиме (значок в области уведомлений), если только это не запрещено в настройках.

/silent или */s* — При указании вместе с ключом `/q` подавляет взаимодействие с пользователем (запросы, сообщения об ошибках, предупреждения и т. д.). Если ключ `/q` не указан, этот параметр никакого действия не оказывает.

/mountoption или */m*

`ro` или `readonly`: смонтировать том как доступный только для чтения.

`rm` или `removable`: смонтировать том как сменный носитель (см. раздел *Том, смонтированный как сменный носитель*).

`ts` или `timestamp`: не сохранять дату/время модификации контейнера.

`sm` или `system`: смонтировать без дозагрузочной аутентификации раздел, входящий в область действия шифрования системы (например, раздел, расположенный на зашифрованном системном диске с другой операционной системой, которая в данный момент не запущена). Полезно, например, для операций резервирования или починки.
Примечание: если вы указываете пароль как параметр ключа `/p`, убедитесь, что пароль набран с использованием стандартной американской раскладки клавиатуры (при использовании графического интерфейса программы это делается автоматически). Это необходимо потому, что пароль требуется вводить на этапе до загрузки операционной системы (до запуска Windows), когда раскладки клавиатуры, отличные от американской, ещё недоступны.

`bk` или `headerbak`: смонтировать том с помощью встроенной резервной копии заголовка.
Примечание: встроенная резервная копия заголовка содержится во всех томах, созданных TrueCrypt версии 6.0 или более новой (эта копия располагается в конце тома).

`recovery`: не проверять контрольные суммы, хранящиеся в заголовке тома. Этот параметр следует использовать только в случае повреждения заголовка тома и когда такой том невозможно смонтировать даже с параметром `headerbak`.

Пример: `/m ro`. Если нужно указать несколько опций монтирования, строка ключей может выглядеть, например, так: `/m rm /m ts`

TrueCrypt Format.exe (Мастер создания томов TrueCrypt):

/noisocheck или */n*

Не проверять правильность записи на носители дисков восстановления TrueCrypt (Rescue Disk). Это может пригодиться, например, в корпоративном окружении, где бывает удобнее иметь дело с централизованным хранилищем ISO-образов, нежели с носителями CD или DVD. **ВНИМАНИЕ:** *Никогда не пытайтесь применять этот ключ, чтобы облегчить повторное использование ранее созданного диска восстановления TrueCrypt.* Помните, что при каждом шифровании системного раздела/диска вы обязаны создавать новый диск восстановления TrueCrypt, даже если используете тот же самый пароль. Ранее созданный диск восстановления нельзя использовать повторно, так как он был создан для другого мастер-ключа.

Синтаксис

TrueCrypt.exe [/a [devices|favorites]] [/b] [/c [y|n]] [/d [*буква диска*]] [/e] [/f] [/h [y|n]] [/k *ключевой файл или путь поиска*] [/l *буква диска*] [/m {bk|rm|recovery|ro|sm|ts}] [/p *пароль*] [/q [background|preferences]] [/s] [/tokenlib *путь*] [/v *том*] [/w]

"TrueCrypt Format.exe" [/n]

Примечание: последовательность указания ключей значения не имеет.

Примеры

Смонтировать том *d:\myvolume* на первую свободную букву диска с запросом пароля (главное окно программы не отображается):

truecrypt /q /v d:\myvolume

Размонтировать том, смонтированный как диск с буквой *X* (главное окно программы не отображается):

truecrypt /q /dx

Смонтировать том с именем *myvolume.tc* с помощью пароля *MyPassword*, как диск с буквой *X*. После монтирования TrueCrypt откроет окно Проводника и подаст звуковой сигнал; монтирование будет автоматическим:

truecrypt /v myvolume.tc /lx /a /p MyPassword /e /b

Модель механизма защиты

***Примечание для исследователей безопасности**: если вы намереваетесь сообщить о проблеме с безопасностью или опубликовать атаку на TrueCrypt, пожалуйста, удостоверьтесь, что вы не пренебрегаете описанной ниже моделью механизма защиты TrueCrypt. В противном случае атака (или проблема с безопасностью) будет расцениваться как недействительная/поддельная.*

TrueCrypt это компьютерная программа, в чьи основные цели входят:

- защита данных путём их шифрования перед записью на диск;
- расшифровка зашифрованных данных после их считывания с диска.

В задачи TrueCrypt **не** входит:

- шифрование или защита любой области ОЗУ (оперативной памяти ПК);
- защита данных в компьютере,[1] если атакующий имеет привилегии администратора[2] в среде операционной системы, установленной в этом компьютере;
- защита данных в компьютере, содержащем какое-либо вредоносное ПО (например, вирус, «троянского коня», шпионскую программу) или любую часть ПО (включая TrueCrypt или компонент операционной системы), которая была изменена, создана или может быть подконтрольна атакующему;

[1] В этой главе (*Модель механизма защиты*) фраза “данные в компьютере” означает данные на внутренних и внешних устройствах хранения информации/носителях (включая сменные устройства и сетевые диски), подключённых к компьютеру.

[2] В этой главе (*Модель механизма защиты*) фраза “привилегии администратора” не обязательно означает действительную учётную запись с правами администратора. Она также может относиться к атакующему, не имеющему действительной учётной записи администратора, но способному (например, из-за неправильной конфигурации системы или путём эксплуатации уязвимости в ОС или в стороннем приложении) выполнить действие, в нормальных условиях доступное лишь пользователю с действительной учётной записью администратора (например, чтение или изменение произвольной части диска или ОЗУ, и т. д.).

- защита данных в компьютере, если у атакующего был к нему физический доступ до или во время работы TrueCrypt;
- защита данных в компьютере, если у атакующего есть физический доступ к нему между временем завершения работы TrueCrypt и временем, необходимым для окончательного и безвозвратного стирания/утери всей информации из модулей временной памяти, подключённых к компьютеру (включая модули памяти в периферийных устройствах);
- защита данных в компьютере, если атакующий может удалённо перехватить излучения от аппаратуры компьютера (например, от монитора или кабелей) во время работы TrueCrypt (или иным образом выполнять удалённый мониторинг аппаратной части ПК и её использования, непосредственно или косвенно, во время работы TrueCrypt в этом ПК);
- защита данных, хранящихся в томе TrueCrypt, если атакующий без привилегий администратора имеет доступ с содержимому смонтированного тома (например, если права на файл/папку/том не препятствуют такому доступу атакующего);
- сохранение/контроль целостности или аутентичности зашифрованных и расшифрованных данных;
- предотвращение анализа трафика при передаче зашифрованных данных по сети;
- предотвращение определения неприятелем, какие сектора с содержимым тома были изменены (а также когда и сколько раз), если неприятель имеет возможность следить за томом (смонтированным или не смонтированным) до и после записи в него, либо если носитель/устройство хранения информации позволяет неприятелю определять такую информацию (например, том находится на устройстве, сохраняющем метаданные, которые можно использовать для выяснения, когда данные были записаны в конкретный сектор).
- шифрование «на месте» любых имеющихся незашифрованных данных (или перешифрование/удаление данных) в устройствах/файловых системах с технологией равномерного использования ячеек памяти (wear-leveling) или иным перераспределением данных внутренними средствами;
- гарантия выбора пользователями криптостойких паролей и ключевых файлов;
- защита любого аппаратного компонента компьютера или всего компьютера;
- защита данных в компьютере, в котором не соблюдены условия, перечисленные в главе *Требования безопасности и меры предосторожности*;
- выполнение чего-либо, указанного в раздел *Ограничения* (глава *Замеченные проблемы и ограничения*).

В среде **Windows** пользователь без привилегий администратора может (при условии, что используются стандартные конфигурации TrueCrypt и операционной системы):

- монтировать любой том TrueCrypt на основе файла при условии, что это позволено правами на файл с контейнером;
- монтировать любой том TrueCrypt на основе раздела/устройства;
- завершать процесс дозагрузочной аутентификации и, следовательно, получать доступ к данным на зашифрованном системном разделе/диске (и запускать зашифрованную операционную систему);
- пропускать процесс дозагрузочной аутентификации (это можно предотвратить, отключив параметр *Настройки* > *Шифрование системы* > *Обход дозагрузочной аутентификации по Esc*; обратите внимание, что включать/отключать данный параметр может только администратор);
- размонтировать, используя TrueCrypt, любой смонтированный этим пользователем том TrueCrypt (и, в окне программы TrueCrypt, видеть его путь и свойства). Что, однако, неприменимо к ‘системным избранным томам’, которые пользователь может

размонтировать (и т. д.) вне зависимости от того, кто их смонтировал (это можно предотвратить, включив параметр *Настройки* > *Системные избранные тома* > *Просматривать/размонтировать системные избранные тома могут лишь администраторы*; обратите внимание, что включать/отключать данный параметр может только администратор);

- создавать том TrueCrypt на основе файла с файловой системой FAT или без файловой системы (при условии, что это разрешено правами соответствующей папки);
- изменять пароль, ключевые файлы и алгоритм деривации ключа заголовка, восстанавливать заголовок или создавать его резервную копию для тома TrueCrypt на основе файла (при условии, что это разрешено правами данного файла);
- обращаться к файловой системе внутри тома TrueCrypt, смонтированного другим пользователем системы (что, однако, можно запретить, назначив соответствующие права на файл/папку/том);
- использовать пароли (и обработанные ключевые файлы), сохранённые в кэше паролей (обратите внимание, что кэширование можно отключить; см. подробности в разделе *Настройки -> Параметры*, подраздел *Кэшировать пароли в памяти драйвера*);
- просматривать основные свойства (например, размер зашифрованной области, используемые алгоритмы шифрования и хеширования, и т. д.) зашифрованного системного раздела/диска, когда работает зашифрованная система;
- запускать и использовать программу TrueCrypt (включая мастер создания томов TrueCrypt) при условии, что запущен драйвер устройств TrueCrypt и это позволяют права на файлы.

В среде **Linux** пользователь без привилегий администратора может (при условии, что используются стандартные конфигурации TrueCrypt и операционной системы):

- создавать том TrueCrypt на основе файла или раздела/устройства с файловой системой FAT или без файловой системы (при условии, что это разрешено правами соответствующей папки/устройства);
- изменять пароль, ключевые файлы и алгоритм деривации ключа заголовка, восстанавливать заголовок или делать его резервную копию для тома TrueCrypt на основе файла или раздела/устройства (при условии, что это разрешено правами данного файла/устройства);
- обращаться к файловой системе внутри тома TrueCrypt, смонтированного другим пользователем системы (что, однако, можно запретить путём назначения соответствующих прав на файл/папку/том);
- запускать и использовать программу TrueCrypt (включая мастер создания томов TrueCrypt) при условии, что это позволяют права на файлы;
- в окне программы TrueCrypt видеть путь и свойства любого тома TrueCrypt, смонтированного этим пользователем.

В среде **Mac OS X** пользователь без привилегий администратора может (при условии, что используются стандартные конфигурации TrueCrypt и операционной системы):

- монтировать любой том TrueCrypt на основе файла или раздела/устройства (при условии, что это разрешено правами соответствующего файла/устройства);
- размонтировать, используя TrueCrypt, любой смонтированный этим пользователем том TrueCrypt (и, в окне программы TrueCrypt, видеть его путь и свойства);
- создавать том TrueCrypt на основе файла или раздела/устройства (при условии, что это разрешено правами соответствующей папки/устройства);
- изменять пароль, ключевые файлы и алгоритм деривации ключа заголовка, восстанавливать заголовок или делать его резервную копию для тома TrueCrypt на

основе файла или раздела/устройства (при условии, что это разрешено правами данного файла/устройства);
- обращаться к файловой системе внутри тома TrueCrypt, смонтированного другим пользователем системы (что, однако, можно запретить путём назначения соответствующих прав на файл/папку/том);
- запускать и использовать программу TrueCrypt (включая мастер создания томов TrueCrypt) при условии, что это позволяют права на файлы.

TrueCrypt не поддерживает корневой режим выполнения set-euid.

Дополнительная информация и подробности о модели механизма защиты содержатся в главе *Требования безопасности и меры предосторожности*.

Требования безопасности и меры предосторожности

ВАЖНО: Если вы хотите пользоваться TrueCrypt, то обязаны соблюдать описанные в этой главе требования безопасности и меры предосторожности.

В этой главе описаны требования безопасности при использовании TrueCrypt и дана информация о том, как неприятель может повлиять на возможности (или ограничить их) TrueCrypt по защите данных и обеспечению правдоподобного отрицания причастности. Отказ от ответственности: мы не гарантируем, что в данной главе затронуты *все* возможные проблемы, связанные с безопасностью, и описаны *все* атаки, которые может предпринять неприятель с целью повлиять на возможности (или ограничить их) TrueCrypt по защите данных и обеспечению правдоподобного отрицания причастности.

Утечки данных

Когда смонтирован том TrueCrypt, операционная система и сторонние приложения могут записывать в незашифрованные тома (обычно в незашифрованный системный том) незашифрованную информацию о данных, хранящихся в томе TrueCrypt (например, имена и пути файлов, к которым недавно было обращение, создаваемые программами индексации базы данных, и т. д.), или собственно данные в незашифрованном виде (временные файлы и т. п.), или незашифрованную информацию о находящейся в томе TrueCrypt файловой системе. Обратите внимание, что Windows автоматически ведёт запись больших объёмов таких потенциально секретных данных, как имена и пути открываемых вами файлов, запускаемые вами приложения, и т. д.

Чтобы предотвратить утечки данных, вы должны проделать следующее (возможны и альтернативные меры).

- Если вам *не* нужна возможность правдоподобного отрицания причастности:

- Зашифруйте системный раздел/диск (о том, как это сделать, см. главу *Шифрование системы*) и убедитесь, что в течение каждого сеанса работы с секретными данными смонтированы только зашифрованные файловые системы или системы, доступные только для чтения.

  или

- Если вы не можете проделать вышеуказанное, загрузите или создайте "live CD"-версию свой операционной системы (т. е. "live"-систему, целиком расположенную на CD/DVD и оттуда же загружающуюся) – это гарантирует, что любые записываемые в системный том данные записываются в RAM-диск (диск в ОЗУ). Когда вам требуется поработать с секретными данными, загрузите систему с такого live-CD/DVD и проверьте, что в течение сеанса смонтированы только зашифрованные и/или доступные только для чтения файловые системы.

- Если вам *нужна* возможность правдоподобного отрицания причастности:

  - Создайте скрытую операционную систему. При этом защита от утечек данных будет обеспечена TrueCrypt автоматически. См. подробности в разделе *Скрытая операционная система*.

    или

  - Если вы не можете проделать вышеуказанное, загрузите или создайте "live CD"-версию свой операционной системы (т. е. "live"-систему, целиком расположенную на CD/DVD и оттуда же загружающуюся) – это гарантирует, что любые записываемые в системный том данные записываются в RAM-диск (диск в ОЗУ). Когда вам требуется поработать с секретными данными, загрузите систему с такого live-CD/DVD. Если вы используете скрытые тома, следуйте требованиям безопасности, указанным в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов*. Если скрытые тома вами не используются, проверьте, что в течение сеанса смонтированы только несистемные тома TrueCrypt на основе раздела и/или файловые системы, доступные только для чтения.

Файл подкачки

*Примечание: описанная ниже проблема вас **не** касается, если системный раздел или системный диск зашифрован (см. подробности в главе* Шифрование системы*) и если все файлы подкачки расположены на одном или нескольких разделах в области действия шифрования системы, например, на разделе, в котором установлена Windows (см. подробности в четвёртом параграфе этого подраздела).*

Файлы подкачки, иногда также именуемые swap-файлами или файлами обмена, используются операционной системой Windows для хранения частей программ и файлов с данными, не умещающихся в оперативной памяти (ОЗУ) компьютера. Это означает, что секретные данные, которые, как вы полагаете, находятся только в ОЗУ, на самом деле без вашего ведома могут быть записаны Windows в *незашифрованном* виде на жёсткий диск.

Примите к сведению, что TrueCrypt *не может* препятствовать сохранению содержимого

открытых в ОЗУ секретных файлов в *незашифрованном* виде в файле подкачки (обратите внимание, что когда вы открываете хранящийся в томе TrueCrypt файл, например, в текстовом редакторе, содержимое этого файла находится в ОЗУ в *незашифрованном* виде).

Чтобы избежать описанных выше проблем, зашифруйте системный раздел/диск (о том, как это сделать, см. в главе *Шифрование системы*) и убедитесь, что все файлы подкачки расположены на одном или нескольких разделах в области действия шифрования системы (например, на разделе, в котором установлена Windows). Обратите внимание, что в Windows XP последнее условие обычно бывает выполнено по умолчанию. В отличие от Windows XP, в Windows Vista и более новых версиях Windows файлы подкачки по умолчанию создаются на *любом* подходящем томе. Поэтому прежде чем приступить к использованию TrueCrypt, вам нужно проделать следующее: щёлкните правой кнопкой мыши по значку '*Компьютер*' (или '*Мой компьютер*') на Рабочем столе или в *меню 'Пуск'*, затем выберите *Свойства* -> (в Windows Vista и новее: -> *Свойства системы* ->) вкладку *Дополнительно* -> раздел *Быстродействие* -> *Параметры* -> вкладку *Дополнительно* -> раздел *Виртуальная память* -> *Изменить*. В Windows Vista и новее отключите параметр *Автоматически выбирать объем файла подкачки*. Затем убедитесь, что в списке томов, доступных для создания файлов подкачки, присутствуют только те, которые входят в область действия шифрования системы (например, том, в котором установлена Windows). Чтобы запретить создание файла подкачки на каком-либо конкретном томе, выделите его, затем выберите пункт *Без файла подкачки* и нажмите *Задать*. По окончании нажмите *OK* и перезагрузите компьютер.

Примечание: ещё один подходящий вариант – создание скрытой операционной системы (см. подробности в разделе Скрытая операционная система*).*

Файлы дампа памяти

*Примечание: описанная ниже проблема вас **не** касается, если системный раздел или системный диск зашифрован (см. подробности в главе* Шифрование системы*) и если система настроена так, что файлы дампа памяти сохраняются на системном диске (что, как правило, принимается по умолчанию).*

Большинство операционных систем, включая Windows, можно настроить так, чтобы при возникновении ошибки (сбоя системы, "синего экрана") выполнялась запись отладочной информации и содержимого системной памяти в так называемые файлы дампов (их также иногда называют дамп-файлами сбоев). Поэтому в файлах дампа памяти могут содержаться секретные данные. TrueCrypt *не может* препятствовать сохранению в *незашифрованном* виде в файлах дампа памяти кэшированных паролей, ключей шифрования и содержимого конфиденциальных файлов, открытых в ОЗУ. Помните, что когда вы открываете хранящийся в томе TrueCrypt файл, например, в текстовом редакторе, содержимое этого файла в *незашифрованном* виде помещается в ОЗУ (и может оставаться в ОЗУ *незашифрованным*, пока не будет выключен компьютер). Также учитывайте, что когда смонтирован том TrueCrypt, его мастер-ключ хранится *незашифрованным* в ОЗУ. Поэтому хотя бы на время каждого сеанса, в течение которого вы работаете с секретными данными, и на время монтирования тома TrueCrypt необходимо отключать в компьютере создание файлов дампа памяти. Чтобы это сделать в Windows XP или более новой версии Windows, щёлкните правой кнопкой мыши по значку '*Компьютер*' (или '*Мой компьютер*') на Рабочем столе или в *меню 'Пуск'*, затем выберите *Свойства* -> (в Windows Vista и новее: -> *Свойства системы* ->) вкладку *Дополнительно* -> раздел *Загрузка и восстановление* ->

Параметры -> раздел *Запись отладочной информации ->* выберите *(отсутствует) -> OK.*

Примечание для пользователей Windows XP/2003: так как Windows XP и Windows 2003 не предоставляют никакого API для шифрования файлов дампа памяти, в случае, если системный раздел/диск зашифрован с помощью TrueCrypt, и ваша система Windows XP настроена на запись файлов дампа памяти на системный диск, драйвер TrueCrypt автоматически запрещает Windows записывать любые данные в файлы дампа памяти.

Файл гибернации

*Примечание: описанная ниже проблема вас **не** касается, если системный раздел или системный диск зашифрован[1] (см. подробности в главе* Шифрование системы*) и если файл гибернации расположен на одном из разделов, входящих в область действия шифрования системы (что, как правило, принимается по умолчанию), например, на разделе, в котором установлена Windows. Когда компьютер переходит в состояние гибернации, данные шифруются на лету перед тем, как они будут сохранены в файле гибернации.*

Когда компьютер переходит в состояние гибернации (или входит в режим энергосбережения), содержимое его оперативной памяти записывается в так называемый файл гибернации на жёстком диске. Вы можете настроить TrueCrypt (*Настройки* > *Параметры > Размонтировать все тома при: входе в энергосбережение*) на автоматическое размонтирование всех смонтированных томов TrueCrypt, удаление их хранящихся в ОЗУ мастер-ключей и очистку кэшированных в ОЗУ паролей (если они есть) перед тем, как компьютер перейдёт в состояние гибернации (или войдёт в режим энергосбережения). Нужно, однако, иметь в виду, что если не используется шифрование системы (см. главу *Шифрование системы*), TrueCrypt не может надёжно препятствовать сохранению в файле гибернации в незашифрованном виде содержимого конфиденциальных файлов, открытых в ОЗУ. Помните, что когда вы открываете хранящийся в томе TrueCrypt файл, например, в текстовом редакторе, содержимое этого файла в *незашифрованном* виде помещается в ОЗУ (и может оставаться в ОЗУ *незашифрованным*, пока не будет выключен компьютер).

Обратите внимание, что когда компьютер переходит в режим сна, на самом деле он может быть настроен на переход в так называемый гибридный спящий режим, вызывающий гибернацию. Также учтите, что операционная система может быть настроена на переход в режим гибернации или в гибридный спящий режим при выборе пункта «Завершить работу» (см. подробности в документации на свою операционную систему).

Чтобы избежать описанных выше проблем, зашифруйте системный раздел/диск (о том, как это сделать, см. в главе *Шифрование системы*) и убедитесь, что файл гибернации находится на одном из разделов, входящих в область действия шифрования системы (что,

[1] Отказ от ответственности: так как Windows XP и Windows 2003 не предоставляют API для шифрования файлов гибернации, TrueCrypt вынужден изменять недокументированные компоненты Windows XP/2003, чтобы позволить пользователям шифровать файлы гибернации. Поэтому TrueCrypt не гарантирует, что файлы гибернации в Windows XP/2003 будут всегда зашифрованы. В ответ на нашу публичную жалобу касательно отсутствия API, корпорация Microsoft начала предоставлять общедоступный API для шифрования файлов гибернации в Windows Vista и более новых версиях Windows (см. подробности в интернете на странице Version History, описание изменений в TrueCrypt версии 5.1a). Начиная с версии 7.0, TrueCrypt использует этот API и потому способен безопасно шифровать файлы гибернации в среде Windows Vista и последующих версий Windows. Поэтому если вы используете Windows XP/2003 и вам требуется безопасное шифрование файла гибернации, мы настоятельно рекомендуем вам перейти на Windows Vista или более новую версию Windows и на TrueCrypt 7.0 или новее.

как правило, принимается по умолчанию), например, на разделе, в котором установлена Windows. Когда компьютер переходит в состояние гибернации, данные шифруются на лету перед тем, как они будут сохранены в файле гибернации.

Примечание: ещё один подходящий вариант – создание скрытой операционной системы (см. подробности в разделе Скрытая операционная система*).*

Если по каким-либо причинам вы не можете использовать шифрование системы, отключите или не допускайте гибернации в своём компьютере, по крайней мере, в течение каждого сеанса, когда вы работаете с секретными данными и монтируете том TrueCrypt.

Незашифрованные данные в ОЗУ

Важно понимать, что TrueCrypt это программа для шифрования данных только на *дисках*, но не в ОЗУ (оперативной памяти).

Не забывайте о том, что большинство программ не очищают область памяти (буферы), где они хранят незашифрованные файлы (или их части) при их загрузке из тома TrueCrypt. Это означает, что после того, как вы выйдете из такой программы, в памяти (в ОЗУ) могут оставаться незашифрованные данные, с которыми она работала, до момента, пока не будет выключен компьютер (а согласно некоторым исследованиям, даже некоторое время после отключения питания[1]). Также имейте в виду, что когда вы открываете хранящийся в томе TrueCrypt файл, например, в текстовом редакторе, а затем принудительно размонтируете этот том TrueCrypt, данный файл останется незашифрованным в области памяти (ОЗУ), используемой (занятой) текстовым редактором. Это также относится и к принудительному авторазмонтированию.

По своей сути, мастер-ключи также должны храниться в ОЗУ в незашифрованном виде. При размонтировании несистемного тома TrueCrypt удаляет его мастер-ключи (находящиеся в ОЗУ). При аккуратной перезагрузке (или аккуратном завершении работы) компьютера все несистемные тома TrueCrypt автоматически размонтируются, и, соответственно, все хранящиеся в ОЗУ мастер-ключи удаляются драйвером TrueCrypt (за исключением мастер-ключей для системных разделов/дисков — см. ниже). Однако при внезапном пропадании питания, из-за которого происходит сброс компьютера (неаккуратная перезагрузка), или в случае краха системы, **работа TrueCrypt, естественно, прекращается, и потому он не может** удалить ни ключи, ни любые другие важные данные. Более того, поскольку корпорация Microsoft не предоставляет соответствующего API для обработки гибернации и завершения работы, используемые для шифрования системы мастер-ключи невозможно надёжно удалить из ОЗУ при переходе компьютера в состояние гибернации, завершении работы или перезагрузке.[2]

---

[1] Якобы в течение 1,5–35 секунд при обычных температурах (26–44 °C) и до нескольких часов, если модули памяти охлаждены (при работающем компьютере) до очень низкой температуры (например, –50 °C). Утверждается, что модули памяти новых типов демонстрируют гораздо более короткое время разрушения информации (например, 1,5–2,5 с), чем модули старых типов (на 2008 г.).

[2] Прежде чем ключ может быть удалён из ОЗУ, необходимо размонтировать соответствующий том TrueCrypt. Для несистемных томов это не составляет проблемы. Однако поскольку Microsoft на данный момент не предоставляет никакого подходящего API для обработки финальной фазы процесса завершения работы системы, в файлах подкачки, расположенных на зашифрованных системных томах, размонтируемых при завершении работы системы, всё ещё могут оставаться действительные вытесненные из ОЗУ страницы памяти (включая части системных файлов Windows). Это может вызывать ошибки 'голубого экрана'. Чтобы предотвратить появление таких ошибок, TrueCrypt не выполняет размонтирование зашифрованных системных томов и, следовательно, не может удалить их мастер-ключи при завершении работы или перезагрузке системы.

Подводя итог, заметим, что TrueCrypt **не может** обеспечить и **не** гарантирует отсутствие в ОЗУ секретных данных (таких, как пароли, мастер-ключи или расшифрованные данные). Поэтому после каждого сеанса работы с томом TrueCrypt или работы зашифрованной операционной системы вы должны завершить работу компьютера (или, если файл гибернации зашифрован, перевести ПК в состояние гибернации) и оставить его в выключенном состоянии хотя бы на несколько минут (чем дольше, тем лучше), прежде чем снова включите его. Это необходимо для того, чтобы очистить ОЗУ (см. также раздел *Файл гибернации*).

Физическая безопасность

Если у вашего неприятеля есть физический доступ к аппаратной части компьютера **и** вы используете компьютер после того, как к нему имел физический доступ неприятель, TrueCrypt может потерять способность защищать данные в этом компьютере.[1] Это может быть вызвано тем, что неприятель мог модифицировать аппаратную часть ПК или подключить какой-либо вредоносный компонент (например, аппаратный модуль слежения на клавиатурой), который будет перехватывать пароли или ключи шифрования (например, когда вы монтируете том TrueCrypt) или как-то иначе компрометировать безопасность данного компьютера. Поэтому на компьютере, к которому имел физический доступ неприятель, использовать TrueCrypt нельзя. Кроме того, вы обязаны удостовериться, что TrueCrypt (в том числе его драйвер) не работает, когда неприятель физически обращается к компьютеру. Дополнительные сведения, относящиеся к аппаратным атакам, когда неприятель имеет непосредственный физический доступ к аппаратуре, приведены в разделе *Незашифрованные данные в ОЗУ*.

Более того, даже если у неприятеля нет физического доступа к аппаратной части компьютера *непосредственно*, пробить брешь в физической защите ПК можно путём удалённого перехвата и анализа излучений от аппаратуры компьютера (включая монитор и кабели). Например, перехваченные излучения от кабеля, соединяющего клавиатуру с компьютером, могут раскрыть набираемые вами пароли. Перечисление всех видов подобных атак (иногда называемых TEMPEST-атаками) и всех известных способов противодействия им (таких, как экранирование или радиопомехи) выходит за рамки данного документа. Вы обязаны предотвращать такие атаки. И ответственность за это лежит исключительно на вас. Если вы этого не сделаете, TrueCrypt может оказаться неспособен защищать данные в вашем компьютере.

Вредоносное ПО (malware)

Термин ‘вредоносное ПО’ (‘malware’) это собирательное название всех типов вредоносных программ, таких как компьютерные вирусы, троянцы, шпионское ПО или, в общем смысле, любое ПО (включая TrueCrypt или какой-либо компонент операционной системы), которое было изменено, обработано или может контролироваться неприятелем. Некоторые виды вредоносного ПО созданы, например, для слежения за клавиатурой, включая ввод паролей (перехваченные таким образом пароли затем либо пересылаются неприятелю через Интернет, либо сохраняются на незашифрованном локальном диске, откуда их затем сможет считать неприятель, когда получит физический доступ к компьютеру). Если вы используете TrueCrypt на компьютере, инфицированном любым видом malware, TrueCrypt

[1] В этом разделе (*Физическая безопасность*) фраза “данные в компьютере” означает данные на внутренних и внешних устройствах хранения/носителях (включая сменные устройства и сетевые диски), подключённых к ПК.

может оказаться неспособен защищать данные в этом компьютере.[1] Поэтому использовать TrueCrypt в таком компьютере нельзя.

Важно понимать, что TrueCrypt – программа для шифрования данных, а *не* для защиты от вредоносного ПО. Ответственность за отсутствие в компьютере вредоносного ПО лежит исключительно на вас. Если вы этого не обеспечите, TrueCrypt может оказаться неспособен защищать данные в вашем компьютере.

Чтобы предотвратить проникновение в компьютер вредоносного ПО, следует соблюдать множество правил. Самые важные из них следующие: регулярно обновляйте операционную систему, интернет-браузер и другое важное ПО. В Windows XP и более новых версиях Windows включите предотвращение выполнения данных (DEP) для всех программ.[2] Не открывайте подозрительные вложения в email-сообщениях, особенно исполняемые файлы, даже если они выглядят так, будто присланы кем-то из ваших знакомых или друзей (их компьютеры могут быть инфицированы вредоносным ПО, без их ведома рассылающим с их ПК/учётных записей вредоносные email-сообщения). Не щёлкайте по подозрительным ссылкам в email-сообщениях или на веб-сайтах (даже если email/сайт кажется безопасным или заслуживающим доверия). Не посещайте никаких подозрительных веб-сайтов. Не загружайте и не устанавливайте никаких подозрительных программ. Используйте только хорошее, надёжное и не содержащее вредоносного кода ПО.

Многопользовательское окружение

Не забывайте, что содержимое смонтированного тома TrueCrypt видно (доступно) всем пользователям, вошедшим в систему. Чтобы этого избежать, можно воспользоваться правами NTFS на файлы/папки, если только том не был смонтирован как сменный носитель (см. раздел *Том, смонтированный как сменный носитель*) в настольной редакции Windows Vista или более новых версий Windows (секторы тома, смонтированного как сменный носитель, могут быть доступны на уровне томов пользователям без привилегий администратора, вне зависимости от того, доступен ли он им на уровне файловой системы).

Более того, в среде Windows кэш паролей доступен всем вошедшим в систему пользователям (более подробные сведения см. в разделе *Настройки -> Параметры*, подраздел *Кэшировать пароли в памяти драйвера*).

Обратите также внимание, что при переключении пользователей в Windows XP или более новой версии Windows (функция *Быстрое переключение пользователей*) размонтирование успешно смонтированного тома TrueCrypt *не* выполняется (в отличие от перезагрузки системы, при которой размонтируются все смонтированные тома TrueCrypt).

Если том TrueCrypt на основе файла должен быть смонтирован в среде Windows 2000, права на файл-контейнер игнорируются. Во всех поддерживаемых версиях Windows пользователи без привилегий администратора могут монтировать любой том TrueCrypt на основе раздела/устройства (при условии правильного указания пароля и/или ключевых файлов). Пользователь без привилегий администратора может демонтировать только те тома, которые монтировал он сам. Это, однако, не относится к системным избранным томам, если только вы не включили опцию (по умолчанию она выключена) *Настройки* >

[1] В этом разделе (*Вредоносное ПО*) фраза “данные в компьютере” означает данные на внутренних и внешних устройствах хранения/носителях (включая сменные устройства и сетевые диски), подключённых к ПК.
[2] DEP (Data Execution Prevention) – предотвращение выполнения данных. Подробная информация о DEP доступна по адресам http://support.microsoft.com/kb/875352, http://technet.microsoft.com/en-us/library/cc700810.aspx и http://windows.microsoft.com/en-US/windows-vista/What-is-Data-Execution-Prevention.

Системные избранные тома > *Просматривать/размонтировать системные избранные тома могут лишь администраторы*.

Аутентичность и целостность данных

TrueCrypt применяет шифрование для сохранения *конфиденциальности* данных, которые подвергаются шифрованию. TrueCrypt не сохраняет и не проверяет целостность или аутентичность данных, подвергающихся шифрованию и дешифрованию. Следовательно, если вы позволите неприятелю изменить зашифрованные с помощью TrueCrypt данные, он сможет установить у любого 16-байтового блока данных случайное или предыдущее значение, которое ему удалось получить в прошлом. Обратите внимание, что неприятель не может выбрать значение, которое вы получите, когда TrueCrypt расшифровывает изменённый блок — значение будет случайным — если только противник не восстановит старую версию зашифрованного блока, которую ему удалось получить в прошлом. Ответственность за проверку целостности и аутентичности данных, зашифрованных или расшифрованных TrueCrypt, лежит только на вас (например, это можно сделать с помощью соответствующего стороннего ПО).

См. также: *Физическая безопасность*, *Модель механизма защиты*

Выбор паролей и ключевых файлов

Очень важно выбрать хороший пароль. Необходимо избегать паролей, состоящих только из одного слова, которое можно найти в каком-либо словаре (или комбинации из таких слов). Пароль не должен содержать никаких имён, дней рождения, телефонных или учётных номеров и любых других элементов, которые можно легко угадать. Хороший пароль это случайная комбинация из букв в верхнем и нижнем регистрах, цифр и специальных символов, таких как @ ^ = $ * + и т.д. Настоятельно рекомендуется выбирать пароль, состоящий не менее чем из 20 символов (чем длиннее, тем лучше), так как короткие пароли несложно взломать методом перебора (brute-force).

Чтобы сделать атаки перебором невозможными, размер ключевого файла должен быть не менее 30 байт. Если для тома используется несколько ключевых файлов, хотя бы один из них должен иметь размер 30 байт или больше. Обратите внимание, что 30-байтовое ограничение предполагает большой объём энтропии в ключевом файле. Если первые 1024 килобайта файла содержат лишь небольшой объём энтропии, такой файл нельзя использовать в качестве ключевого (вне зависимости от размера файла). Если вы не понимаете, что такое энтропия, рекомендуем доверить TrueCrypt создание файла со случайным содержимым и использовать этот файл как ключевой (выберите *Сервис -> Генератор ключевых файлов*).

При создании тома, шифровании системного раздела/диска или изменении паролей/ключевых файлов нельзя позволять никому другому выбирать или изменять пароли/ключевые файлы до тех пор, пока не будет создан том или изменены пароль/ключевые файлы. Например, вы не должны использовать никакие генераторы паролей (будь то приложения в Интернете или локальные программы), если не уверены в их высоком качестве и в том, что они не подконтрольны неприятелю, а в качестве ключевых файлов нельзя использовать файлы, загруженные из Интернета, или которые доступны другим пользователям данного компьютера (неважно, администраторы они или нет).

Изменение паролей и ключевых файлов

Примите к сведению, что заголовок тома (зашифрованный с помощью ключа заголовка, полученного из пароля/ключевого файла) содержит мастер-ключ (не путайте с паролем), посредством которого зашифрован том. Если неприятель сумеет скопировать том перед тем, как вы измените его пароль и/или ключевые файлы, он сможет воспользоваться своей копией или фрагментом (старым заголовком) тома TrueCrypt для монтирования вашего тома с помощью рассекреченного пароля и/или рассекреченных ключевых файлов, применявшихся для монтирования тома до того, как вы изменили пароль и/или ключевые файлы.

Если вы не можете сказать наверняка, знает ли неприятель ваш пароль (или обладает ли он вашими ключевыми файлами) и не делал ли он копии вашего тома, когда вам потребовалось изменить пароль и/или ключевые файлы тома, настоятельно рекомендуем создать новый том TrueCrypt и перенести в него файлы из старого тома (в новом томе будет другой мастер-ключ).

Также учтите, что если неприятель знает ваш пароль (или обладает вашими ключевыми файлами) и у него есть доступ к вашему тому, он может извлечь и сохранить у себя мастер-ключ тома. Сделав это, он получит возможность расшифровать ваш том даже после того, как вы смените пароль и/или ключевые файлы этого тома (потому что при изменении пароля и/или ключевых файлов мастер-ключ остаётся неизменным). В этом случае создайте новый том TrueCrypt и перенесите в него все файлы из старого тома.

В следующих разделах этой главы содержится дополнительная информация, касающаяся возможных проблем безопасности, связанных с изменением паролей и/или ключевых файлов:

- *Требования безопасности и меры предосторожности*
- *Журналируемые файловые системы*
- *Дефрагментация*
- *Перераспределённые сектора*

Trim-операции

В ряде запоминающих устройств (например, в некоторых твердотельных (SSD) накопителях, включая флэш-накопители USB) для маркировки секторов как свободных, например, при удалении файла, применяется так называемая операция ‘trim’. Вследствие этого такие секторы могут содержать незашифрованные нули или другие неопределённые данные (незашифрованные), даже если они расположены внутри части диска, зашифрованной с помощью TrueCrypt. TrueCrypt не блокирует trim-операцию на разделах, входящих в область действия шифрования системы (см. главу *Шифрование системы*) (если только не запущена скрытая операционная система – см. раздел *Скрытая операционная система*), а в среде Linux – на всех томах, использующих родные криптографические службы ядра Linux. В таких ситуациях неприятель сможет выяснить, какие секторы содержат пустое место (и сможет в дальнейшем воспользоваться этой информацией для анализа и атак), и это может негативно сказаться на возможности правдоподобного отрицания причастности (см. главу *Правдоподобное отрицание причастности*). Если вы хотите избежать подобных проблем, не применяйте шифрование системы на дисках, использующих trim-операцию, а в среде Linux либо настройте TrueCrypt так, чтобы не использовались родные криптографические службы ядра Linux, либо убедитесь, что тома TrueCrypt не расположены на дисках, использующих trim-операцию.

Выяснить, используется ли в устройстве trim-операция, можно в документации на это устройство или у его поставщика/производителя.

Равномерное распределение нагрузки на блоки (Wear-Leveling)

Ряд запоминающих устройств (например, некоторые твердотельные (SSD) накопители, включая флэш-накопители USB) и некоторые файловые системы используют так называемые механизмы wear-leveling, служащие для продления срока жизни запоминающего устройства или носителя. Суть работы этих механизмов в том, что даже если какое-либо приложение многократно записывает данные в один и тот же логический сектор, в действительности данные распределяются равномерно по всему носителю (т. е. логические сектора переназначаются на разные физические сектора). Отсюда следует, что неприятелю могут оказаться доступны несколько "версий" одного сектора. А это может повлечь за собой различные проблемы с безопасностью. Например, когда вы изменяете у тома пароль и/или ключевые файлы, то – в нормальных условиях – заголовок тома перезаписывается новым, заново зашифрованным заголовком. Если же том находится на устройстве, в котором применяется механизм wear-leveling, TrueCrypt не может гарантировать, что старый заголовок окажется действительно перезаписан. Если неприятель обнаружит в устройстве старый заголовок тома (который должен был быть перезаписан), он сможет воспользоваться им для монтирования тома, указав старый, рассекреченный пароль (и/или рассекреченные ключевые файлы, служившие для монтирования этого тома до того, как был перешифрован заголовок тома). Из соображений безопасности мы не рекомендуем создавать/хранить тома TrueCrypt на устройствах (или в файловых системах), в которых применяется механизм wear-leveling (и не применять TrueCrypt для шифрования любых разделов в таких устройствах или файловых системах).

Если вы решили не следовать этой рекомендации и намереваетесь использовать шифрование «на месте» на устройстве, использующем механизмы wear-leveling, то перед тем как полностью зашифровать раздел/устройство, убедитесь, что в нём не содержится никаких секретных данных (на таком устройстве TrueCrypt не может надёжно выполнить безопасное шифрование имеющихся данных «на месте»; тем не менее, после того, как раздел/диск будет полностью зашифрован, любые записываемые на него новые данные будут надёжно шифроваться «на лету»). При этом нужно соблюдать следующие меры предосторожности. Прежде чем запускать TrueCrypt для настройки дозагрузочной аутентификации, отключите файлы подкачки и перезагрузите операционную систему (после того, как системный раздел/диск будет полностью зашифрован, файлы подкачки можно будет снова включить). На период между моментом запуска TrueCrypt для настройки дозагрузочной аутентификации и моментом, когда системный раздел/диск будет полностью зашифрован, необходимо отключить гибернацию. Учтите, однако, что даже при соблюдении этих мер предосторожности *нельзя* гарантировать отсутствие утечек данных и то, что содержащаяся в устройстве секретная информация будет надёжно зашифрована. Более подробные сведения см. в разделах *Утечки данных*, *Файл подкачки* и *Файл гибернации*.

Если вам требуется возможность правдоподобного отрицания причастности, вы не должны использовать TrueCrypt ни для шифрования любой части устройства (или файловой системы), ни для создания на нём зашифрованных контейнеров, если в этом устройстве применяется механизм wear-leveling.

Выяснить, используется ли в устройстве механизм wear-leveling, можно в документации на это устройство или у его поставщика/производителя.

Перераспределённые сектора

Некоторые устройства хранения информации (например, жёсткие диски) перераспределяют/переназначают плохие сектора внутренними методами. Как только устройство обнаруживает сектор, в который невозможно записать данные, оно помечает такой сектор как плохой и переназначает его на другой сектор, расположенный в скрытой зарезервированной области диска. Все последующие операции чтения/записи с этим плохим сектором перенаправляются на сектор в зарезервированной области. Это означает, что любые содержащиеся в плохом секторе данные остаются на диске и их нельзя стереть (перезаписать другими данными), что может повлечь за собой различные проблемы с безопасностью. Например, в плохом секторе могут оставаться незашифрованные данные, которые должны были быть зашифрованы «на месте». Аналогично, в плохом секторе могут сохраниться данные, которые должны быть удалены (например, в процессе создания скрытой операционной системы). Если сектор перераспределён, это может неблагоприятно сказаться на правдоподобности отрицания причастности (см. раздел *Правдоподобное отрицание причастности*). Дополнительные примеры возможных проблем с безопасностью приведены в разделе *Требования безопасности и меры предосторожности*. Примите, однако, к сведению, что данный список – неполный (это просто примеры). Также учтите, что TrueCrypt *не может* предотвратить никаких проблем с безопасностью, связанных с перераспределёнными секторами или вызванных ими. Выяснить количество перераспределённых секторов на жёстком диске можно, например, с помощью сторонних программ для чтения так называемой информации S.M.A.R.T.

Дефрагментация

Когда вы (или операционная система) выполняете дефрагментацию файловой системы, в которой находится контейнер TrueCrypt на основе файла, копия этого контейнера (или его фрагмент) может остаться в свободной области хост-тома (в дефрагментированной файловой системе). Это может повлечь за собой ряд проблем с безопасностью. Например, если вы затем измените у тома пароль и/или ключевые файлы, а неприятель обнаружит старую копию или фрагмент (старый заголовок) тома TrueCrypt, он может с его помощью смонтировать том, используя старый рассекреченный пароль (и/или старые рассекреченные ключевые файлы, действительные для монтирования этого тома до того, как был перешифрован заголовок тома). Чтобы избежать этой и других связанных с безопасностью проблем (таких, как описано в разделе *Клонирование томов*):

- используйте тома TrueCrypt на основе раздела/устройства, а не на основе файла;
- после дефрагментации надёжно очищайте (затирайте) свободное место на хост-томе (в дефрагментированной файловой системе);
- не дефрагментируйте файловые системы, в которых вы храните тома TrueCrypt.

Журналируемые файловые системы

Если том TrueCrypt на основе файла находится в журналируемой файловой системе (такой, как NTFS), в свободной области хост-тома может оставаться копия контейнера TrueCrypt (или его фрагмента). Это может повлечь за собой ряд проблем с безопасностью. Например, если вы измените у тома пароль и/или ключевые файлы, а неприятель обнаружит старую

копию или фрагмент (старый заголовок) тома TrueCrypt, он может с его помощью смонтировать том, используя старый рассекреченный пароль (и/или старые рассекреченные ключевые файлы, действительные для монтирования этого тома до того, как был перешифрован заголовок тома). Кроме того, некоторые журналируемые файловые системы записывают в своих внутренних ресурсах время обращения к файлам и другую потенциально важную для сохранения конфиденциальности информацию. Если вам требуется возможность правдоподобно отрицать причастность (см. раздел *Правдоподобное отрицание причастности*), хранить контейнеры TrueCrypt на основе файлов в журналируемых файловых системах нельзя. Чтобы избежать возможных проблем безопасности, связанных с журналируемыми файловыми системами:

- используйте тома TrueCrypt на основе раздела/устройства, а не на основе файла;
- храните контейнер в нежурналируемой файловой системе (например, в FAT32).

Клонирование томов

Никогда не создавайте новый том TrueCrypt путём клонирования какого-либо уже существующего тома TrueCrypt. Чтобы создать новый том, всегда используйте мастер создания томов TrueCrypt. Если вы клонируете том, а затем начнёте использовать их оба – и этот том, и его клон – таким образом, что данные в каждом из них будут разными, этим вы можете способствовать облегчению криптоанализа (поскольку при разном содержимом оба тома будут использовать один и тот же набор ключей). Это особенно критично в случае, если в томе находится скрытый том. Также учтите, что в подобных случаях правдоподобное отрицание причастности невозможно (см. раздел *Правдоподобное отрицание причастности*). См. также главу *О безопасном резервировании данных*.

Дополнительные требования безопасности и меры предосторожности

Помимо всего того, что было описано в этой главе (*Требования безопасности и меры предосторожности*), вы обязаны помнить и соблюдать требования безопасности, меры предосторожности и ограничения, изложенные в следующих главах и разделах:

- ***О безопасном резервировании данных***
- ***Ограничения***
- ***Модель механизма защиты***
- ***Требования безопасности и меры предосторожности касательно скрытых томов***
- ***Правдоподобное отрицание причастности***

См. также: *Цифровые подписи*

О безопасном резервировании данных

В результате аппаратных или программных ошибок/сбоев, файлы в томе TrueCrypt могут оказаться повреждёнными. Поэтому мы настоятельно рекомендуем регулярно делать резервные копии всех важных файлов (разумеется, это относится к любым важным данным, а не только к зашифрованным в томах TrueCrypt).

Несистемные тома

Чтобы безопасно создать резервную копию несистемного тома TrueCrypt, рекомендуем следующую последовательность действий.

1. Создайте новый том TrueCrypt с помощью мастера создания томов TrueCrypt (не включайте ни опцию *Быстрое форматирование*, ни *Динамический*). Это будет ваш *резервный* том, поэтому он по размеру должен совпадать с *основным* томом (или превосходить его).

   Если *основной* том это скрытый том TrueCrypt (см. раздел *Скрытый том*), *резервный* том также должен быть скрытым томом TrueCrypt. Прежде чем создать скрытый *резервный* том, вы должны создать для него новый хост- (внешний) том при выключенной опции *Быстрое форматирование*. Кроме того, особенно если *резервный* том – на основе файла, скрытый *резервный* том должен занимать лишь очень маленькую часть контейнера, а внешний том должен быть почти целиком заполнен файлами (в противном случае это может неблагоприятно сказаться на правдоподобности отрицания наличия скрытого тома).

2. Смонтируйте вновь созданный *резервный* том.

3. Смонтируйте *основной* том.

4. Скопируйте все файлы из смонтированного *основного* тома непосредственно в смонтированный *резервный* том.

ВАЖНО: Если вы храните резервный том в месте, к которому может иметь частый доступ неприятель (например, на устройстве в банковском сейфе для хранения ценностей), вам следует повторять все описанные выше этапы (в том числе этап 1) всякий раз, когда вы будете изготавливать резервную копию тома (см. ниже).

Если вы будете выполнять все указанные выше этапы, то этим помешаете неприятелю выяснить:

- какие секторы томов изменяются (так как вы всегда выполняете этап 1), что особенно важно, например, если устройство с резервным томом находится в банковском сейфе для хранения ценностей (или любом другом месте, к которому у неприятеля может быть частый доступ) и в томе содержится скрытый том (см. подробности в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов* в главе *Правдоподобное отрицание причастности*);

- что один из томов является резервной копией другого.

Системные разделы

Примечание: помимо резервного копирования файлов, мы также рекомендуем вам делать резервные копии своего диска восстановления TrueCrypt (выберите *Система* > *Создать диск восстановления*). Более подробную информацию см. в разделе *Диск восстановления TrueCrypt (Rescue Disk)*.

Чтобы надёжно и безопасно сделать резервную копию зашифрованного системного раздела, рекомендуем следующую последовательность действий.

1. Если в вашем компьютере установлено несколько операционных систем, загрузите ту из них, которая не требует дозагрузочной аутентификации.

   Если в компьютере нет нескольких операционных систем, можно загрузиться с CD/DVD, содержащего WinPE или BartPE (‘live’-версию Windows, целиком хранящуюся на CD/DVD и оттуда же загружающуюся; подробности ищите в главе *Вопросы и ответы*, ключевое слово – ‘BartPE’).

   Если оба указанных выше варианта невозможны, подключите свой системный диск как вторичный накопитель к другому компьютеру и затем загрузите операционную систему, установленную в том компьютере.

   Примечание: из соображений безопасности, если операционная система, резервную копию которой вы хотите сделать, находится в скрытом томе TrueCrypt (см. раздел *Скрытая операционная система*), то операционная система, которую вы загружаете на этом этапе, должна быть либо ещё одной скрытой ОС, либо системой "live-CD" (см. выше). Более подробную информацию см. в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов* в главе *Правдоподобное отрицание причастности*.

2. Создайте новый несистемный том TrueCrypt с помощью мастера создания томов TrueCrypt (не включая опции *Быстрое форматирование* и *Динамический*). Это будет ваш *резервный* том, поэтому он по размеру должен совпадать с системным разделом (или превосходить его), резервную копию которого вы намереваетесь сделать.

   Если операционная система, резервную копию которой вы хотите создать, установлена в скрытом томе TrueCrypt (см. раздел *Скрытая операционная система*), *резервный* том также должен быть скрытым томом TrueCrypt. Прежде чем создать скрытый *резервный* том, вы должны создать для него новый хост- (внешний) том при выключенной опции *Быстрое форматирование*. Кроме того, особенно если *резервный* том – на основе файла, скрытый *резервный* том должен занимать лишь очень маленькую часть контейнера, а внешний том должен быть почти целиком заполнен файлами (в противном случае это может неблагоприятно сказаться на правдоподобности отрицания наличия скрытого тома).

3. Смонтируйте новый созданный *резервный* том.

4. Смонтируйте системный раздел, резервную копию которого вы хотите сделать, выполнив следующее:

   a. нажмите кнопку *Устройство* и выберите системный раздел, для которого нужно сделать резервную копию (в случае скрытой ОС, выберите раздел, содержащий скрытый том, в котором установлена скрытая ОС);

   b. нажмите *OK*;

   c. выберите *Система* > *Смонтировать без дозагрузочной аутентификации*;

   d. введите свой пароль дозагрузочной аутентификации и нажмите *OK*.

5. Смонтируйте *резервный* том, а затем с помощью какой-либо сторонней программы или средствами Windows создайте образ файловой системы, находящейся в системном разделе (который на предыдущем этапе был смонтирован как обычный том TrueCrypt) и сохраните этот образ непосредственно в смонтированном *резервном* томе.

ВАЖНО: Если вы храните резервный том в месте, к которому может иметь частый доступ неприятель (например, на устройстве в банковском сейфе для хранения ценностей), вам следует повторять все описанные выше этапы (в том числе этап 2) всякий раз, когда вы будете изготавливать резервную копию тома (см. ниже).

Если вы будете выполнять все указанные выше этапы, то этим помешаете неприятелю выяснить:

- какие секторы томов изменяются (так как вы всегда выполняете этап 2), что особенно важно, например, если устройство с резервным томом находится в банковском сейфе для хранения ценностей (или любом другом месте, к которому у неприятеля может быть частый доступ) и в томе содержится скрытый том (см.

подробности в подразделе *Требования безопасности и меры предосторожности касательно скрытых томов* в главе *Правдоподобное отрицание причастности*);.

- что один из томов является резервной копией другого.

Общие замечания

Если вы храните резервную копию тома в месте, где неприятель может сделать копию тома, имеет смысл шифровать том каскадом (последовательностью) алгоритмов (например, AES-Twofish-Serpent). В противном случае, если том зашифрован только одним алгоритмом, и этот алгоритм в дальнейшем удастся взломать (например, вследствие прогресса в криптоанализе), неприятель сумеет расшифровать имеющиеся у него копии тома. Вероятность взлома сразу трёх разных алгоритмов шифрования значительно ниже, чем одного из них.

Разное

Использование TrueCrypt без прав администратора

В среде Windows пользователь, не имеющий прав администратора, *может* использовать TrueCrypt, но только после того, как администратор компьютера установит TrueCrypt в систему. Причина этого в том, что для обеспечения незаметного для пользователя шифрования/дешифрования «на лету» требуется наличие в системе драйвера TrueCrypt, а пользователи без полномочий администратора не имеют прав на установку/запуск драйверов устройств в Windows.

После того как администратор системы установит TrueCrypt, пользователи, не обладающие правами администратора, смогут запускать TrueCrypt, монтировать/демонтировать тома TrueCrypt любого типа, загружать и сохранять в них данные, а также создавать в системе тома TrueCrypt на основе файла. В то же время, пользователям без привилегий администратора будут недоступны шифрование/форматирование разделов, создание томов NTFS, установка/удаление TrueCrypt, изменение паролей/ключевых файлов для разделов/устройств TrueCrypt, резервное копирование и восстановление из резервных копий заголовков разделов/устройств TrueCrypt, а также запуск TrueCrypt в ‘переносном’ (‘portable’) режиме.

ВНИМАНИЕ: Вне зависимости от типа используемого программного обеспечения, с точки зрения сохранности персональной информации в большинстве случаев *небезопасно* работать с конфиденциальными данными в системе, где у вас нет привилегий администратора, так как администратор может без труда получить и скопировать ваши конфиденциальные данные, в том числе пароли и ключи.

Совместное использование по сети

Если требуется обеспечить доступ к одному и тому же тому TrueCrypt сразу из нескольких операционных систем, возможны два варианта.

1. Том TrueCrypt смонтирован только на одном компьютере (скажем, на сервере), и через сеть общедоступно лишь содержимое смонтированного тома TrueCrypt (т. е. файловая система внутри тома TrueCrypt). Пользователи других компьютеров или систем не будут монтировать том (он уже смонтирован на сервере).

   Преимущества: все пользователи могут записывать данные в том TrueCrypt. Совместно используемый том может быть как на основе файла, так и на основе раздела/устройства.

   Недостаток: пересылаемые по сети данные не будут зашифрованными. Тем не менее, их всё-таки можно шифровать с помощью SSL, TLS, VPN и других технологий.

   Замечания: примите к сведению, что при перезагрузке системы совместно используемый сетевой ресурс будет автоматически восстановлен только в случае, если это системный избранный том или зашифрованный системный раздел/диск (о том, как сделать том системным избранным томом, см. в главе *Системные избранные тома*).

2. Размонтированный файл-контейнер TrueCrypt хранится на одном компьютере (скажем, на сервере). Этот зашифрованный файл доступен для совместного использования по сети. Пользователи других компьютеров или систем будут локально монтировать этот совместно используемый файл. Таким образом, том будет монтироваться одновременно в нескольких операционных системах.

Преимущество: пересылаемые по сети данные будут зашифрованными (тем не менее, их всё же рекомендуется шифровать с помощью SSL, TLS, VPN или других подходящих технологий, чтобы ещё сильнее осложнить анализ трафика и сохранить целостность данных).

Недостатки: совместно используемый том может быть только на основе файла (но не на основе раздела/устройства). В каждой из систем том должен монтироваться в режиме только для чтения (о том, как смонтировать том в режиме только для чтения, см. раздел *Параметры монтирования*). Обратите внимание, что это требование относится и к незашифрованным томам. Одна и причин, например, в том, что данные, считанные из обычной файловой системы в среде одной ОС, в это же время могут быть изменены другой ОС, и потому могут оказаться противоречивыми (что может привести к повреждению данных).

Работа TrueCrypt в фоновом режиме

Когда главное окно TrueCrypt закрыто, но TrueCrypt продолжает работать в фоновом режиме, на него возложены следующие задачи/функции.

1. Обслуживание горячих клавиш
2. Автоматическое размонтирование (например, при завершении сеанса, непреднамеренным извлечением хост-устройства, истечении времени ожидания, и т. д.)
3. Автоматическое монтирование избранных томов
4. Оповещения (например, о предотвращении повреждения скрытого тома)
5. Значок в области уведомлений в панели задач

ВНИМАНИЕ: Если TrueCrypt не запущен ни в фоновом режиме, ни явно, все указанные выше задачи/функции отключены.

TrueCrypt в фоновом режиме это на самом деле всё та же программа *TrueCrypt.exe*, продолжающая работать в фоне после того, как было закрыто её главное окно. Определить, работает TrueCrypt или нет, можно по виду области уведомления в панели задач. Если там присутствует значок TrueCrypt, значит, TrueCrypt работает в фоновом режиме. При щелчке по этому значку левой кнопкой мыши откроется главное окно TrueCrypt. При щелчке правой кнопкой мыши появится всплывающее меню с относящимися к TrueCrypt функциями.

Прекратить фоновую работу TrueCrypt можно в любой момент, щёлкнув правой кнопкой мыши по значку TrueCrypt в области уведомления и выбрав пункт *Выход*. Если вам нужно отключить работу TrueCrypt в фоновом режиме полностью и перманентно, выберите *Настройки -> Параметры* и снимите отметку с опции *Включено* в группе параметров *Работа TrueCrypt в фоновом режиме*.

Том, смонтированный как сменный носитель

Этот раздел применим к томам TrueCrypt, смонтированным, когда включена одна из следующих опций (в соответствии с их применением):

- *Настройки* > *Параметры* > *Монтировать тома как сменные носители*
- *Параметры монтирования* > *Монтировать том как сменный носитель*
- *Избранное* > *Упорядочить избранные тома* > *Монтировать выбранный том как сменный носитель*
- *Избранное* > *Упорядочить системные избранные тома* > *Монтировать выбранный том как сменный носитель*

Тома TrueCrypt, смонтированные как сменные носители, имеют следующие преимущества и недостатки:

- На таких томах TrueCrypt в Windows не создаются автоматически папки '*Recycled*' и/или '*System Volume Information*' (эти папки в Windows служат для функций Корзины и восстановления системы).
- Windows может использовать методы кэширования и отложенную запись, которые обычно применяются для сменных носителей (например, флэш-накопителей USB). Это может слегка понизить производительность, но повысить вероятность, что будет возможно быстро размонтировать том без необходимости принудительного размонтирования.

- Операционная система может иметь тенденцию сводить к минимуму число дескрипторов, открываемых ею для такого тома. Следовательно, тома, смонтированные как сменные носители, могут требовать меньшего числа принудительных размонтирований, чем другие тома.

- У томов, смонтированных как сменные носители, в среде Windows Vista и более ранних версий Windows в списке '*Компьютер*' (или '*Мой компьютер*') не отображается объём свободного места (это ограничение Windows, а не ошибка в TrueCrypt).

- В среде редакций Windows Vista и более новых версий Windows для настольных ПК, секторы тома, смонтированного как сменный носитель, могут быть доступны всем пользователям (включая пользователей без прав администратора; см. раздел *Многопользовательское окружение*).

Системные файлы TrueCrypt и программные данные

Примечание: `%windir%` это главная папка, в которой установлена Windows (например, `C:\WINDOWS`)

Драйвер TrueCrypt

`%windir%\SYSTEM32\DRIVERS\truecrypt.sys`

Примечание: этот файл отсутствует, если TrueCrypt работает в переносном (portable) режиме.

Установки TrueCrypt, данные приложения и другие системные файлы

ВНИМАНИЕ: TrueCrypt *не* шифрует никаких из указанных в этом разделе файлов (если только не выполняется шифрование системного раздела/диска).

Следующие файлы сохраняются в папке `%APPDATA%\TrueCrypt\`. В переносном (portable) режиме эти файлы сохраняются в папке, откуда был запущен файл *TrueCrypt.exe* (т. е. в папке, где расположен *TrueCrypt.exe*):

`Configuration.xml` (основной конфигурационный файл).

`System Encryption.xml` (временный конфигурационный файл, использующийся в начальном процессе шифрования/дешифрования системного раздела/диска «на месте»).

`Default Keyfiles.xml`

Примечание: этот файл может отсутствовать, если не использовалась соответствующая функция TrueCrypt.

`Favorite Volumes.xml`
Примечание: этот файл может отсутствовать, если не использовалась соответствующая функция TrueCrypt.

`History.xml` (список последних двадцати файлов/устройств, которые пытались смонтировать как тома TrueCrypt или использовать как хосты для томов TrueCrypt; эту функцию можно отключить – подробности см. в разделе *Не сохранять историю*)
Примечание: этот файл может отсутствовать, если не использовалась соответствующая функция TrueCrypt.

`In-Place Encryption`
`In-Place Encryption Wipe Algo`
(временные конфигурационные файлы, используемые при начальном процессе шифрования/дешифрования несистемного тома «на лету»).

`Post-Install Task - Tutorial`
`Post-Install Task - Release Notes`
(временные конфигурационные файлы, используемые при установке или обновлении TrueCrypt).

Следующие файлы сохраняются в папке `%ALLUSERSPROFILE%\TrueCrypt\`:

`Original System Loader` (резервная копия исходного содержимого первой дорожки диска, сделанная до того, как в неё был записан загрузчик TrueCrypt).
Примечание: этот файл может отсутствовать, если системный раздел/диск не зашифрован.

Следующие файлы сохраняются в папке `%windir%\system32` (в 32-разрядных системах) или в `%windir%\SysWOW64` (в 64-разрядных системах):

`TrueCrypt System Favorite Volumes.xml`
Примечание: этот файл может отсутствовать, если не использовалась соответствующая функция TrueCrypt.

`TrueCrypt.exe`
Примечание: копия этого файла находится в данной папке только тогда, когда включено монтирование системных избранных томов.

Как удалить шифрование

Пожалуйста, учтите, что TrueCrypt способен выполнять дешифрование «на месте» только **системных разделов и системных дисков** (выберите *Система* > *Перманентно расшифровать системный раздел/диск*). Если нужно удалить шифрование (например, когда вы больше в нём не нуждаетесь) из **несистемного тома**, выполните следующие шаги.

1. Смонтируйте том TrueCrypt.

2. Перенесите все файлы из тома TrueCrypt в любое место вне тома TrueCrypt (обратите внимание, что файлы будут «на лету» расшифрованы).

3. Размонтируйте том TrueCrypt.

4. **Если том TrueCrypt – на основе файла**, удалите этот файл (контейнер), как вы удаляете любой другой файл.

Если том – на основе раздела (также относится к флэш-накопителям USB), то в дополнение к шагам 1-3 проделайте следующее:

a. Щёлкните правой кнопкой мыши по значку '*Компьютер*' (или '*Мой компьютер*') на Рабочем столе или в меню '*Пуск*' и выберите *Управление*. Появится окно *Управление компьютером*.
b. В окне *Управление компьютером*, из списка слева, выберите *Управление дисками* (в подветви *Запоминающие устройства*).
c. Щёлкните правой кнопкой мыши на разделе, который вы хотите расшифровать, и выберите *Изменить букву диска или путь к диску*.

d. Появится окно *Изменение буквы диска или путей*. Если никакой буквы диска в этом окне не отображается, нажмите *Добавить*. В противном случае нажмите *Отмена*.
Если вы нажали *Добавить*, то в появившемся окне *Добавление буквы диска или пути* выберите букву диска, которую вы хотите присвоить тому, и нажмите *OK*.
e. В окне *Управление компьютером* снова щёлкните правой кнопкой мыши по разделу, который вы хотите расшифровать, и выберите *Форматировать*. Появится окно *Форматирование*.
f. В окне *Форматирование* нажмите *OK*. После того как раздел будет отформатирован, его больше не потребуется монтировать с помощью TrueCrypt, чтобы можно было сохранять или загружать файлы в этом разделе.

Если том – на основе устройства (т. е. на устройстве нет разделов и оно полностью зашифровано), то в дополнение к шагам 1-3 проделайте следующее:

a. Щёлкните правой кнопкой мыши по значку '*Компьютер*' (или '*Мой компьютер*') на Рабочем столе или в меню '*Пуск*' и выберите *Управление*. Появится окно *Управление компьютером*.
b. В окне *Управление компьютером*, из списка слева, выберите *Управление дисками* (в подветви *Запоминающие устройства*).
c. Появится окно *Инициализация диска*. Используйте его, чтобы проинициализировать диск.
d. В окне *Управление компьютером* щёлкните правой кнопкой мыши по области, где показано место на зашифрованном устройстве, и выберите *Создать раздел* или *Создать простой том*.
e. ВНИМАНИЕ: Прежде чем продолжить, убедитесь, что выбрали именно то устройство, которое хотели, так как все файлы на нём будут уничтожены. В появившемся окне *Мастер создания разделов* или *Мастер создания простых томов* следуйте инструкциям, чтобы создать на устройстве новый раздел. После того как раздел будет создан, устройство больше не потребуется монтировать с помощью TrueCrypt, чтобы можно было сохранять или загружать файлы в этом устройстве.

Удаление TrueCrypt

Чтобы удалить (деинсталлировать) TrueCrypt из Windows XP, выберите меню *Пуск* > *Настройка* > *Панель управления* > *Установка и удаление программ* > *TrueCrypt* > *Изменить/Удалить*.

Чтобы удалить (деинсталлировать) TrueCrypt из Windows Vista и более новых версий Windows, выберите меню *Пуск* > *Компьютер* > *Удаление или изменение программ* > *TrueCrypt* > *Удалить*.

Никакие тома TrueCrypt при деинсталляции программы не удаляются. Вы сможете снова монтировать свои тома TrueCrypt, повторно установив TrueCrypt или запустив в переносном (portable) режиме.

Цифровые подписи

Зачем нужно проверять цифровые подписи

Может так случиться, что установочный пакет TrueCrypt, который вы загружаете с нашего сервера, был создан или модифицирован взломщиком. Например, взломщик мог воспользоваться какой-либо уязвимостью в используемом нами серверном ПО и изменить хранящиеся на сервере установочные пакеты, либо он мог изменить любые файлы при их пересылке к вам.

По этой причине следует всегда проверять целостность и аутентичность любого установочного пакета TrueCrypt, который вы загружаете или получаете из какого-либо иного источника. Другими словами, следует всегда проверять, что файл создан именно нами и не был модифицирован злоумышленником. Единственный способ это сделать – проверить у файла так называемые цифровые подписи.

Типы используемых нами цифровых подписей

В настоящий момент мы используем цифровые подписи двух типов:

- Подписи **PGP** (доступны для всех пакетов с бинарными файлами и с исходным кодом для всех операционных систем).

- Подписи **X.509** (доступны для пакетов с бинарными файлами для Windows).

Преимущества подписей X.509

По сравнению с подписями PGP, подписи X.509 имеют следующие преимущества:

- значительно проще проверить, что ключ, которым подписан файл, действительно наш (а не взломщика);
- чтобы поверить подлинность подписи X.509, не требуется загружать и устанавливать никакого дополнительного ПО (см. ниже);
- не нужно загружать и импортировать наш открытый ключ (он встроен в подписанный файл);
- не нужно загружать отдельный файл с подписью (она встроена в подписанный файл).

Преимущества подписей PGP

По сравнению с подписями X.509, подписи PGP имеют следующие преимущества:

- они не зависят от источника сертификации (который может, например, фильтроваться/контролироваться неприятелем или быть ненадёжным по другим причинам).

Как проверять подписи X.509

Обратите внимание, что в настоящий момент подписи X.509 доступны только для самораспаковывающихся установочных пакетов TrueCrypt для Windows. Подпись X.509, встроенная в каждый из таких файлов вместе с цифровым сертификатом TrueCrypt Foundation, выпущена общественной организацией сертификации. Чтобы проверить целостность и подлинность самораспаковывающегося установочного пакета для Windows, проделайте следующее.

1. Загрузите самораспаковывающийся установочный пакет TrueCrypt.

2. В Проводнике Windows щёлкните правой кнопкой мыши по загруженному файлу (‘*TrueCrypt Setup.exe*’) и выберите в контекстном меню пункт *Свойства*.

3. В диалоговом окне *Свойства* перейдите на вкладку *Цифровые подписи*.

4. На вкладке *Цифровые подписи* в поле *Список подписей* дважды щёлкните по строке с надписью "*TrueCrypt Foundation*".

5. Появится диалоговое окно *Состав цифровой подписи*. Если вверху этого окна вы увидите следующую фразу, значит, целостность и подлинность пакета успешно прошли проверку и подтверждены:

   "*Эта цифровая подпись действительна.*"

Если такой фразы нет, это с большой вероятностью означает, что файл повреждён.
Примечание: в ряде устаревших версий Windows отсутствуют некоторые необходимые сертификаты, из-за чего проверка подписей не работает.

Как проверять подписи PGP

Чтобы проверить подпись PGP, проделайте следующее:

1. Установите любую программу шифрования с открытым ключом, поддерживающую подписи PGP. Ссылки на такое ПО приведены тут: http://www.truecrypt.org/links.
2. Создайте личный (секретный) ключ (о том, как это сделать, см. в документации на ПО шифрования с открытым ключом).
3. Загрузите наш открытый ключ PGP с нашего сервера или из надёжного репозитария открытых ключей и импортируйте загруженный ключ в свой keyring (о том, как это сделать, см. в документации на ПО шифрования с открытым ключом).
4. Подпишите импортированный ключ своим личным ключом, чтобы пометить его как надёжный (о том, как это сделать, см. в документации на ПО шифрования с открытым ключом).
   Примечание: если вы пропустите этот шаг и попытаетесь проверить любую нашу PGP-подпись, то получите сообщение об ошибке, гласящее, что цифровая подпись неверна.
5. Загрузите цифровую подпись, нажав кнопку *PGP Signature* рядом с файлом, который вы хотите проверить (на страницах загрузки).
6. Проверьте загруженную подпись (о том, как это сделать, см. в документации на ПО шифрования с открытым ключом).

Устранение неполадок

Рекомендуем также ознакомиться с содержащей новейшие сведения интернет-версией этой главы по адресу:
http://www.truecrypt.org/docs/?s=troubleshooting

В этом разделе приведены возможные решения типичных проблем, с которыми можно столкнуться при использовании TrueCrypt.

Примечание: если вашей проблемы здесь нет, она может быть в одном из следующих разделов:

- *Несовместимости*
- *Замеченные проблемы и ограничения*
- *Вопросы и ответы*

Удостоверьтесь, что вы используете новейшую стабильную версию TrueCrypt. Если

проблема вызвана ошибкой в какой-либо старой версии TrueCrypt, возможно, она уже исправлена. Чтобы узнать, какая у вас сейчас версия программы, выберите ***Справка*** > ***О программе***.

Проблема:

Операции записи/чтения с томом выполняются очень медленно, хотя согласно тесту, скорость используемого мною шифра выше, чем скорость жёсткого диска.

Вероятная причина:

Возможно, проблема вызвана вмешательством какой-либо сторонней программы.

Возможное решение:

Во-первых, проверьте, не имеет ли ваш файл-контейнер TrueCrypt расширения, зарезервированного за исполняемыми файлами (например, .exe, .sys или .dll). Если это так, Windows и антивирусное ПО могут вмешиваться в операции с таким контейнером и неблагоприятно влиять на скорость работы с томом.

Во-вторых, отключите или удалите приложение, которое может вмешиваться в операции с контейнером (обычно это антивирусное ПО, программы для автоматической дефрагментации дисков и т. д.). Если причина – в антивирусном ПО, часто помогает отключение в его настройках защиты в реальном времени. Если так устранить проблему не удалось, попробуйте временно отключить антивирусное ПО. Если и это не помогло, попробуйте полностью удалить это ПО и перезагрузить компьютер.

Проблема:

*Невозможно смонтировать том TrueCrypt; программа TrueCrypt сообщает: "*Неверный пароль, либо это не том TrueCrypt*".*

Вероятная причина:

Может быть повреждён заголовок тома в результате действия сторонней программы или некорректной работы аппаратного компонента компьютера.

Возможные решения:

- Если том был создан с помощью TrueCrypt версии **6.0 или более новой**, можно попытаться восстановить заголовок тома из его резервной копии, встроенной в том. Для этого:

    1) запустите TrueCrypt 6.0 или новее;

    2) нажмите кнопку *Устройство* или *Файл*, чтобы выбрать том;

    3) выберите *Сервис* > *Восстановить заголовок тома*.

- Если том был создан с помощью TrueCrypt версии **5.1a или более ранней**, можно попытаться смонтировать этот том, воспользовавшись параметром командной строки `/m recovery`. Для этого:

    1) установите TrueCrypt 6.1 или новее;

    2) на клавиатуре нажмите и удерживайте клавишу <Windows>, а затем нажмите клавишу <R> – появится диалоговое Windows-окно *Запуск программы*;

    3) введите следующую команду (указав вместо последнего аргумента, *\Device\Harddisk1\Partition0*, путь к вашему тому, а если TrueCrypt установлен не в `%ProgramFiles%`, замените `%ProgramFiles%` на путь к TrueCrypt):

    ```
    "%ProgramFiles%\TrueCrypt\TrueCrypt.exe" /q /m recovery /v
    \Device\Harddisk1\Partition0
    ```

    4) нажмите <Enter>, чтобы смонтировать том.

Проблема:

*После успешного монтирования тома Windows сообщает: "*This device does not contain a valid file system*"* (*"*Это устройство не содержит корректной файловой системы*"*) *или выдаёт похожую ошибку.*

Вероятная причина:

Может быть повреждена файловая система в томе TrueCrypt (или том не отформатирован).

Возможное решение:

Для починки файловой системы в томе TrueCrypt можно воспользоваться соответствующими средствами, входящими в состав вашей операционной системы. В Windows это утилита '*chkdsk*'. TrueCrypt предоставляет простой способ её использования для томов TrueCrypt. Сначала создайте резервную копию тома TrueCrypt (так как утилита '*chkdsk*' может вызвать ещё большие повреждения файловой системы), а затем смонтируйте его. Щёлкните правой кнопкой мыши по смонтированному тому в главном окне TrueCrypt (в списке дисков) и выберите в контекстном меню пункт *Исправить файловую систему*.

Проблема:

При попытке создать скрытый том, его максимально возможный размер оказывается непредвиденно маленьким (во внешнем томе гораздо больше свободного места).

Вероятные причины:

1. Внешний том отформатирован как NTFS.
2. Фрагментация.

3. Слишком маленький размер кластера + слишком много файлов/папок в корневой папке внешнего тома.

ИЛИ

Слишком маленький размер кластеров + слишком много файлов/папок в корневой папке внешнего тома.

Возможные решения:

Решения для случая 1:

> В отличие от файловой системы FAT, файловая система NTFS всегда сохраняет внутренние данные точно в середине тома. Поэтому скрытый том может находиться только во второй половине внешнего тома. Если это ограничение для вас неприемлемо, проделайте одно из следующего:

- переформатируйте внешний том в FAT и затем создайте внутри него скрытый том;
- если внешний том слишком большой, чтобы его можно было отформатировать в FAT, разделите этот том на несколько томов объёмом по 2 терабайта (или по 16 терабайт, если устройство использует 4-Кбайт сектора) и отформатируйте каждый из этих томов в FAT.

Решение для случая 2:

> Создайте новый внешний том (дефрагментация – не способ решения проблемы, так как она неблагоприятно влияет на возможность правдоподобного отрицания причастности – см. раздел *Дефрагментация*).

Решение для случая 3:

Примечание: указанное ниже решение применимо только к скрытым томам, созданным внутри томов с файловой системой FAT.

Дефрагментируйте внешний том (смонтируйте его, щёлкните правой кнопкой мыши по его букве диска в окне '*Компьютер*' или '*Мой компьютер*', выберите пункт *Свойства*, перейдите на вкладку *Сервис* и нажмите *Выполнить дефрагментацию*). После того как том будет дефрагментирован, закройте окно *Дефрагментация диска* и попытайтесь снова создать скрытый том.

Если это не помогло, удалите *все* файлы и папки во внешнем томе нажатием клавиш <Shift>+<Delete>, но не форматированием (не забудьте заранее отключить для этого диска Корзину и восстановление системы), и попробуйте снова создать скрытый том в этом *полностью пустом* внешнем томе (только с целью проверки). Если максимально возможный размер скрытого тома не изменился даже сейчас, причина проблемы, вероятнее всего, кроется в расширенной корневой папке. Если вы использовали размер кластеров, отличный от предлагаемого по умолчанию (последний этап в работе мастера), переформатируйте внешний том, на этот раз оставив размер кластера по умолчанию.

Если это не помогло, ещё раз переформатируйте внешний том и скопируйте в его корневую папку меньше файлов/папок, чем в прошлый раз. Если проблема не решается, повторяйте форматирование и уменьшайте количество файлов/папок в корневой папке. Если это неприемлемо или не помогает, переформатируйте внешний том, выбрав больший размер кластеров. Если это не помогло, повторяйте переформатирование, увеличивая размер кластеров, пока проблема не будет решена. В качестве альтернативы попробуйте создать скрытый том внутри тома с файловой системой NTFS.

Проблема:

Возникает одна из следующих проблем:

- *невозможно смонтировать том TrueCrypt*
- *невозможно создавать тома TrueCrypt с файловой системой NTFS*

Кроме того, возможна следующая ошибка: "The process cannot access the file because it is being used by another process" ("Процесс не может получить доступ к файлу, занятому другим процессом").

Вероятная причина:

Возможно, проблема вызвана вмешательством какой-либо сторонней программы. Обратите внимание, что это не ошибка в TrueCrypt. Операционная система сообщает TrueCrypt, что устройство заблокировано для исключительного доступа каким-либо приложением (поэтому у TrueCrypt нет возможности к нему обратиться).

Возможное решение:

Как правило, помогает отключение или удаление мешающего приложения (обычно это антивирусное ПО, программы управления дисками и т. д.).

Проблема:

На экране загрузчика TrueCrypt я пытаюсь ввести пароль и/или нажимать другие клавиши, но загрузчик никак на это не реагирует.

Вероятная причина:

У вас клавиатура USB (не PS/2), а в настройках BIOS отключена поддержка USB-клавиатур в фазе до загрузки ОС.

Возможное решение:

Нужно включить поддержку USB-клавиатур в настройках BIOS. Чтобы это сделать, выполните следующее.

Перезагрузите компьютер, нажмите клавишу <F2> или <Delete> (сразу же, как появится начальный экран BIOS) и дождитесь появления экрана с настройками BIOS. Если этот экран не появился, снова перезагрузите компьютер (нажмите кнопку сброса) и сразу же начните часто нажимать клавишу <F2> или <Delete>. Когда появится экран с настройками BIOS,

включите поддержку USB-клавиатур в дозагрузочном окружении. Обычно это выполняется выбором *Advanced* > *USB Configuration* > *Legacy USB Support* (или *USB Legacy*) > *Enabled*. (Обратите внимание, что слово ‘legacy’, т. е. ‘устаревший’, на самом деле вводит в заблуждение, так как дозагрузочные компоненты современных версий MS Windows требуют, чтобы этот параметр был включён, дабы позволить взаимодействие с пользователем.) Затем сохраните настройки BIOS (обычно это делается нажатием клавиши F10) и перезагрузите компьютер. Более подробную информацию см. в документации на BIOS/системную плату или свяжитесь со службой технической поддержки поставщика вашего компьютера.

Проблема:

После шифрования системного раздела/диска компьютер после перезагрузки не может загрузиться (также невозможно войти в экран настроек BIOS).

Вероятная причина:

Ошибка в BIOS вашего компьютера.

Возможные решения:

- Проделайте следующее:

1. Отключите зашифрованный диск.
2. Подключите незашифрованный диск с установленной операционной системой (или установите её на диск).
3. Обновите BIOS.
4. Если проблема не решилась, сообщите об этой ошибке производителю или поставщику компьютера.

ИЛИ

- Если поставщик BIOS/системной платы/компьютера не предоставил обновлений, решающих проблему, а вы используете Windows 7 или более новую версию Windows, и на диске есть дополнительный загрузочный раздел (размером менее 1 ГБ), можно попробовать переустановить Windows без этого дополнительного загрузочного раздела (чтобы обойти ошибку в BIOS). О том, как это сделать, см. тут: http://www.truecrypt.org/knowledge-base/extra-win-boot-partition

---

Проблема:

Возникает одна из следующих проблем:

- *после ввода пароля дозагрузочной аутентификации в течение предварительного теста шифрования системы компьютер зависает (при появлении сообщения* ‘Booting...’*).*

- *если зашифрован системный раздел/диск (частично или полностью), и система перезагружена первый раз с момента запуска шифрования системного*

раздела/диска, компьютер зависает после ввода пароля дозагрузочной аутентификации (при появлении сообщения 'Booting...'*).*
- *после клонирования скрытой операционной системы и ввода для неё пароля компьютер зависает (при появлении сообщения* 'Booting...'*).*

Вероятная причина:

Ошибка в BIOS вашего компьютера.

Возможные решения:

- Обновите BIOS (о том, как это сделать, см. в документации на BIOS/системную плату или свяжитесь со службой технической поддержки поставщика вашего компьютера).
- Используйте системную плату другой модели/фирмы.
- Если поставщик BIOS/системной платы/компьютера не предоставил обновлений, решающих проблему, а вы используете Windows 7 или более новую версию Windows, и на диске есть дополнительный загрузочный раздел (размером менее 1 ГБ), можно попробовать переустановить Windows без этого дополнительного загрузочного раздела (чтобы обойти ошибку в BIOS). О том, как это сделать, см. тут: http://www.truecrypt.org/knowledge-base/extra-win-boot-partition

---

Проблема:

При монтировании или размонтировании тома TrueCrypt происходит сбой системы (появляется 'синий экран' ошибки или компьютер внезапно перезагружается).

ИЛИ

После установки TrueCrypt начались частые сбои в работе операционной системы.

Вероятные причины:

- Ошибка в стороннем приложении (например, в антивирусном ПО, утилите для подстройки системы и т. д.)
- Ошибка в TrueCrypt
- Ошибка в Windows или неисправность в оборудовании компьютера

Возможные решения:

- Попробуйте отключить все антивирусные программы, утилиты для тонкой подстройки системы ("твикеры") и другие аналогичные приложения. Если это не поможет, попробуйте удалить их и перезагрузить Windows.

  Если проблема не исчезает, запустите TrueCrypt и выберите *Справка* > *Проанализировать сбой системы*. TrueCrypt проанализирует файлы дампа сбоев, которые автоматически создаются Windows при аварийных отказах (если они есть). Если TrueCrypt определяет, что сбой вероятнее всего вызван ошибкой в стороннем драйвере, будут показаны имя и поставщик этого драйвера (обратите внимание, что

проблема может быть устранена обновлением или удалением драйвера). Какой бы результат ни был получен, вы сможете отправить основную информацию о сбое системы, чтобы помочь нам определить, не вызван ли он ошибкой в TrueCrypt.

Проблема:

При попытке шифрования системного раздела/диска, во время предварительного теста, загрузчик TrueCrypt всегда сообщает, что неверно введён пароль дозагрузочной аутентификации (хотя я точно знаю, что пароль правильный).

Вероятные причины:

- Отличное от нужного состояние режима (клавиши) *Num Lock* и/или *Caps Lock*
- Повреждение данных

Возможное решение:

1. Когда вы устанавливаете пароль дозагрузочной аутентификации, запомните состояние режимов, включаемых/отключаемых клавишами <Num Lock> и <Caps Lock> (в зависимости от производителя, эти клавиши могут иметь разную маркировку, например, <Num LK>). Примечание: до установки пароля вы можете изменить состояние любой из этих клавиш так, как хотите, нужно лишь запомнить их состояния.

2. При вводе пароля на экране загрузчика TrueCrypt убедитесь, что состояние каждой из этих клавиш такое же, каким оно было тогда, когда вы устанавливали пароль.

Примечание: другие возможные решения данной проблемы см. в других частях этой главы.

Проблема:

Если системный раздел/диск зашифрован, операционная система каждые 5-60 минут 'замораживается' примерно на 10-60 секунд (что может также сопровождаться 100%-ной загрузкой ЦП).

Вероятная причина:

Проблема с ЦП и/или системной платой.

Возможные решения:

- Попробуйте обновить BIOS.

- Попробуйте отключить все функции, относящиеся к энергосбережению (включая любые особые функции приостановки ЦП), в настройках BIOS и в разделе

‘Электропитание’ в Панели управления Windows.

- Замените процессор другим (иного типа и/или производителя).
- Замените системную плату другой (иного типа и/или производителя).

Проблема:

В Windows 7/Vista (и, возможно, в более новых версиях) невозможно использовать утилиту Microsoft Windows Backup (‘Программа архивации’) для резервного копирования данных на несистемный том TrueCrypt.

Причина:

Ошибка в утилите Windows Backup.

Возможное решение:

1. Смонтируйте том TrueCrypt, на который вы хотите зарезервировать данные.
2. Щёлкните правой кнопкой мыши по папке в этом томе (или по букве диска, на котором он расположен, в списке ‘*Компьютер*’) и выберите в подменю пункт *Общий доступ и безопасность* (в Windows Vista – *Общий доступ*).
3. Выполните инструкции, чтобы открыть общий доступ к папке со своей учётной записи.
4. В Windows Backup выберите эту папку с общим доступом (расположение/путь в сети) как место назначения.
5. Запустите процесс резервирования.

Примечание: указанное выше решение **не**применимо для редакций *Starter (Начальная)* и *Home (Домашняя)* Windows 7 (и, возможно, более новых версий).

Проблема:

В Windows Vista и более новых версиях Windows из окна ‘Компьютер’ невозможно изменить метку файловой системы у тома TrueCrypt.

Причина:

Из-за проблемы в Windows, метка записывается только в файл реестра, а не в файловую систему.

Возможное решение:

- Щёлкните правой кнопкой мыши по смонтированному тому в окне ‘*Компьютер*’, выберите *Свойства* и введите новую метку для этого тома.

Проблема:

Не удаётся зашифровать раздел/устройство, так как мастер создания томов TrueCrypt сообщает, что раздел/устройство сейчас используется.

Возможное решение:

Закройте, отключите или удалите все программы, которые могут как-либо использовать раздел/устройство (например, антивирусное ПО). Если это не помогает, щёлкните правой кнопкой мыши по значку '*Компьютер*' (или '*Мой компьютер*') на Рабочем столе и выберите *Управление -> Запоминающие устройства -> Управление дисками.* Затем щёлкните правой кнопкой мыши по разделу, который вы хотите зашифровать, и выберите *Изменить букву диска или путь к диску.* Далее нажмите *Удалить* и *OK.* Перезагрузите операционную систему.

Проблема:

При создании скрытого тома мастер сообщает, что невозможно заблокировать внешний том.

Вероятная причина:

Внешний том содержит файлы, используемые одним или несколькими приложениями.

Возможное решение:

Закройте все программы, которые используют файлы во внешнем томе. Если это не помогает, попробуйте отключить или удалить установленное у вас антивирусное ПО и затем перезагрузить систему.

Проблема:

При обращении к контейнеру на основе файла, доступного через сеть, выдаётся ошибка "insufficient memory" (недостаточно памяти) или "not enough server storage is available" (недостаточно места на сервере).

Вероятная причина:

Установлено слишком маленькое значение *IRPStackSize* в реестре Windows.

Возможное решение:

Найдите в реестре Windows ключ *IRPStackSize* и установите у него большее значение. Затем перезагрузите систему. Если в реестре нет такого ключа, создайте его в ветви *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters* и установите у него значение 16 или выше, после чего перезагрузите систему. Более подробную информацию см. на страницах http://support.microsoft.com/kb/285089/ и http://support.microsoft.com/kb/177078/

Несовместимости

Рекомендуем вам также ознакомиться с версией этой главы в Интернете, которая может содержать более новые сведения. Она доступна по адресу: http://www.truecrypt.org/docs/?s=incompatibilities

Активация Adobe Photoshop® и других продуктов с помощью FLEXnet Publisher® / SafeCast

*Примечание: описанная ниже проблема вас **не** касается, если используются TrueCrypt 5.1 или новее и алгоритм шифрования без каскадирования (т. е. AES, Serpent или Twofish).[1] Эта проблема вас **не** касается и в том случае, если вы пользуетесь дозагрузочной аутентификацией (см. главу Шифрование системы).*

ПО активации Acresso FLEXnet Publisher, в прошлом – Macrovision SafeCast (применяемое для активации сторонних программ, например, *Adobe Photoshop*), записывает данные в первую дорожку диска. Если это происходит, когда системный раздел/диск зашифрован с помощью TrueCrypt, часть загрузчика TrueCrypt оказывается повреждённой, и загрузить Windows не удастся. В этом случае воспользуйтесь своим диском восстановления TrueCrypt, чтобы вновь получить доступ к системе. Сделать это можно двумя способами.

1. Если вы хотите, чтобы у стороннего ПО сохранилась активация, вам придётся *каждый раз* загружать систему с помощью CD/DVD-диска восстановления TrueCrypt. Для этого просто вставьте свой диск восстановления в CD/DVD-накопитель и введите пароль на появившемся экране диска.

2. Если вы не желаете каждый раз загружать систему с CD/DVD-диска восстановления TrueCrypt, то можете восстановить загрузчик TrueCrypt на системном диске. Чтобы это сделать, на экране диска восстановления выберите *Repair Options* > *Restore TrueCrypt Boot Loader*. Учтите, однако, что стороннее ПО будет при этом деактивировано.

Информация о том, как пользоваться диском восстановления TrueCrypt, приведена в главе *Диск восстановления TrueCrypt (Rescue Disk)*.

Возможное постоянное решение: обновите TrueCrypt до версии 5.1 или более новой, дешифруйте системный раздел/диск, а затем повторно его зашифруйте, используя

[1] Причина в том, что при не-каскадном шифре загрузчик TrueCrypt имеет меньший размер, чем при каскадном, поэтому на первой дорожке диска хватает места для резервной копии загрузчика TrueCrypt. Поэтому в случае повреждения загрузчика TrueCrypt, вместо него автоматически используется его резервная копия.

алгоритм без каскадирования (т. е. AES, Serpent или Twofish).*

Примите к сведению, что это не ошибка в TrueCrypt (данная проблема вызвана некорректным механизмом активации в стороннем ПО).

Замеченные проблемы и ограничения

Настоятельно рекомендуем также ознакомиться с интернет-версией этой главы, содержащей новейшие сведения, по адресу:
http://www.truecrypt.org/docs/?s=issues-and-limitations

Замеченные проблемы

- (На момент создания этого документа подтверждённых проблем не было.)

Ограничения

- [*Примечание: данное ограничение не относится к пользователям Windows Vista и Windows более новых версий*.] В Windows XP/2003 TrueCrypt не поддерживает шифрование всего системного диска, если тот содержит расширенные (логические) разделы. Весь системный диск можно зашифровать при условии, что он содержит только первичные разделы. На любом системном диске, который частично или полностью зашифрован, создавать расширенные (логические) разделы нельзя (можно только первичные). *Примечание*: если требуется зашифровать весь диск, содержащий расширенные разделы, можно зашифровать системный раздел и в дополнение создать тома TrueCrypt на основе раздела внутри любых несистемных разделов на этом диске. Либо, как альтернативный вариант, обновить систему до Windows Vista или более новой версии Windows.

- В настоящее время TrueCrypt не поддерживает шифрование системного диска, который был преобразован в динамический.

- Пароли томов TrueCrypt могут содержать только пригодные для печати ASCII-символы. Другие символы в паролях не поддерживаются, так как они могут вызывать различные проблемы (например, невозможность смонтировать том).

- Для обхода проблемы в Windows XP, загрузчик TrueCrypt всегда автоматически настраивается под версию ОС, в которой он установлен. Если версия системы изменилась (например, загрузчик TrueCrypt был установлен, когда работала Windows Vista, а позднее использовался для загрузки Windows XP), вы можете столкнуться с рядом известных и неизвестных проблем (например, на некоторых ноутбуках возможен сбой при выводе экрана входа в Windows XP). Обратите внимание, что это относится к

мультизагрузочным конфигурациям, дискам восстановления TrueCrypt и обманным/скрытым операционным системам (поэтому если скрытая система, к примеру, Windows XP, то и обманной системой тоже должна быть Windows XP).

- Возможность монтирования раздела, входящего в область действия шифрования системы с дозагрузочной аутентификацией (например, раздел, расположенный на зашифрованном системном диске с другой операционной системой, которая в данный момент не запущена), выполняемое, например, выбором *Система* > *Смонтировать без дозагрузочной аутентификации*, ограничена первичными разделами (расширенные/логические разделы монтировать таким способом невозможно).

- Из-за проблемы в Windows 2000, в этой операционной системе TrueCrypt не поддерживает Windows Mount Manager (Диспетчер монтирования Windows). Поэтому некоторые входящие в состав Windows 2000 инструменты, например, программа дефрагментации дисков, с томами TrueCrypt не работают. Более того, в Windows 2000 невозможно использовать службы Диспетчера монтирования, например, присваивать тому TrueCrypt точку монтирования (т. е. присоединять том TrueCrypt к какой-либо папке).

- TrueCrypt не поддерживает дозагрузочную аутентификацию для операционных систем, установленных внутри файлов VHD, за исключением загрузки с помощью соответствующего ПО для виртуальных машин, например, Microsoft Virtual PC.

- Служба Windows ‘Теневое копирование тома’ в настоящий момент поддерживается только для разделов, входящих в область шифрования системы (например, системный раздел, зашифрованный с помощью TrueCrypt, или несистемный раздел, расположенный на зашифрованном с помощью TrueCrypt системном диске, смонтированном при работе зашифрованной операционной системы). Примечание: для других типов томов служба ‘Теневое копирование тома’ не поддерживается, так как недоступна документация на необходимый API.

- Параметры загрузки Windows невозможно изменять из скрытой операционной системы, если система загружается не из раздела, в котором она установлена. Причина в том, что когда работает скрытая система, из соображений безопасности загрузочный раздел монтируется как доступный только для чтения. Чтобы можно было изменить параметры загрузки, запустите обманную ОС.

- У зашифрованных разделов невозможно изменять размер. Исключение составляют разделы на полностью зашифрованном системном диске, размер которых можно изменять, когда запущена зашифрованная ОС.

- Если системный раздел/диск зашифрован, систему нельзя обновлять (например, с Windows XP до Windows Vista) или восстанавливать из дозагрузочного окружения (с помощью установочного CD/DVD Windows или дозагрузочного компонента Windows). В таких случаях требуется сначала дешифровать системный раздел/диск. Примечание: в запущенную операционную систему можно *устанавливать обновления* (обновления безопасности, пакеты обновления и т. п.) без каких-либо проблем, даже если системный раздел/диск зашифрован.

- Шифрование системы поддерживается только на дисках, подключённых локально по интерфейсу ATA/SCSI (термин ATA также означает SATA и eSATA).

- При использовании шифрования системы (это также относится к скрытым операционным системам), TrueCrypt не поддерживает изменения в мультизагрузочной конфигурации (например, изменение числа операционных систем и их расположения). В частности, конфигурация должна оставаться неизменной и той же, какой она была, когда мастер создания томов TrueCrypt начинал подготовку к шифрованию системного раздела/диска (или созданию скрытой операционной системы).

Примечание: единственное исключение – мультизагрузочная конфигурация, при которой зашифрованная с помощью TrueCrypt операционная система всегда располагается на диске #0, и это единственная операционная система на данном диске (либо на этом диске есть ещё одна обманная зашифрованная TrueCrypt система и ещё одна скрытая зашифрованная TrueCrypt система и нет никаких других операционных систем), а диск подключён или отключён до включения компьютера (например, с помощью выключателя питания на внешнем модуле для диска eSATA). При этом на других дисках в компьютере могут быть установлены любые дополнительные (зашифрованные или не зашифрованные) операционные системы (при отключении диска #0 диск #1 становится диском #0, и т.д.)

- При низком уровне заряда аккумуляторной батареи ноутбука Windows может пренебрегать отправкой соответствующих сообщений запущенным приложениям, когда компьютер входит в режим экономии энергии. Поэтому в таких ситуациях функция автоматического размонтирования томов TrueCrypt может не сработать.

- Надежное и безопасное сохранение любых меток даты/времени у любого файла (скажем, у контейнера или ключевого файла) не гарантируется (причинами могут быть, например, журналы файловой системы, метки времени файловых атрибутов или невозможность выполнения этого операционной системой по различным документированным или недокументированным причинам). Примечание: если выполняется запись в скрытый том на основе файла, метка времени у контейнера может измениться. Правдоподобное объяснение может быть таким: это произошло при изменении пароля (внешнего) тома. Также учтите, что TrueCrypt никогда не сохраняет метки времени у системных избранных томов (вне зависимости от установок).

- Особое ПО (например, низкоуровневый дисковый редактор), выполняющее запись на дисковый накопитель в обход драйверов в драйверном стеке класса ‘DiskDrive’ (GUID этого класса – 4D36E967-E325-11CE-BFC1-08002BE10318), может записывать незашифрованные данные в несистемный диск, управляющий смонтированным томом (‘Partition0’) и в зашифрованные разделы/диски, входящие в область действия шифрования активной системы (записываемые таким способом данные TrueCrypt не шифрует). Аналогично, программы, выполняющие запись данных на дисковый накопитель в обход драйверов в драйверном стеке класса ‘Storage Volume’ (GUID этого класса – 71A27CDD-812A-11D0-BEC7-08002BE2092F) могут записывать незашифрованные данные в тома TrueCrypt на основе раздела (даже если те смонтированы).

- Из соображений безопасности, когда запущена скрытая операционная система, TrueCrypt гарантирует, что все локальные незашифрованные файловые системы и нескрытые тома TrueCrypt доступны только для чтения. Это, однако, не относится к файловым системам на CD/DVD-подобных носителях и на нетипичных или нестандартных устройствах/носителях (например, любые устройства/носители, чей класс отличается от класса Windows-устройств ‘Storage Volume’, или которые не

соответствуют требованиям данного класса (GUID этого класса – 71A27CDD-812A-11D0-BEC7-08002BE2092F)).

- Тома TrueCrypt на основе устройств, расположенные на дискетах (флоппи-дисках), не поддерживаются. Примечание: на дискетах по-прежнему можно создавать тома TrueCrypt на основе файлов.

- Дополнительные ограничения перечислены в разделе *Модель механизма защиты*.

Вопросы и ответы

Примечание: новейшая версия списка часто задаваемых вопросов (FAQ) по работе с TrueCrypt доступна по адресу http://www.truecrypt.org/faq.

Я не могу вспомнить свой пароль! Существует ли какой-нибудь способ ('потайная дверь'), чтобы можно было извлечь файлы из моего тома TrueCrypt?

TrueCrypt не позволяет восстановить никаких зашифрованных данных без знания правильного пароля или ключа. Мы не можем восстановить ваши данные, так как не знаем и не можем узнать выбранный вами пароль или сгенерированный вами ключ. Единственный способ восстановить ваши файлы – попытаться "взломать" пароль или ключ, но на это могут уйти тысячи или миллионы лет (в зависимости от длины и качества пароля или ключевых файлов, быстродействия программной/аппаратной части компьютера, алгоритмов и других факторов). Если вам сложно в это поверить, примите к сведению, что даже ФБР не удалось расшифровать том TrueCrypt после года безуспешных попыток.

Существует ли руководство по быстрому началу работы или какое-то пособие для новичков?

Да. Первая глава, Руководство для новичков, содержит снимки экранов и пошаговые инструкции создания, монтирования и использования тома TrueCrypt.

Можно ли зашифровать раздел/диск, на котором установлена Windows?

Да (см. раздел Шифрование системы).

Можно ли воспроизводить видеофайлы (.avi, .mpg и т. д.) прямо с тома TrueCrypt, в котором они записаны?

Да, зашифрованные с помощью TrueCrypt тома ведут себя как обычные диски. Вы указываете правильный пароль (и/или ключевой файл) и монтируете (открываете) том TrueCrypt. Когда вы дважды щёлкаете по значку видеофайла, операционная система запускает ассоциированное с этим типом файлов приложение – обычно это медиапроигрыватель. Затем медиапроигрыватель начинает загружать маленькую начальную часть видеофайла из зашифрованного тома TrueCrypt в ОЗУ (оперативную

память компьютера), чтобы его воспроизвести. Во время загрузки этой части TrueCrypt автоматически её расшифровывает (в ОЗУ), после чего расшифрованная часть видео (находящаяся в ОЗУ) воспроизводится медиапроигрывателем. Пока эта часть воспроизводится, медиапроигрыватель начинает загружать другую небольшую часть видеофайла из зашифрованного тома TrueCrypt в ОЗУ, и процесс повторяется.

То же самое происходит, например, при записи видео: прежде чем часть видеофайла будет записана в том TrueCrypt, она шифруется TrueCrypt в ОЗУ, и только затем записывается на диск. Такой процесс называется шифрованием/дешифрованием «на лету», и он работает для файлов всех типов (не только видео).

Будет ли TrueCrypt всегда бесплатным и с открытым кодом?

Да, будет. Мы никогда не станем выпускать коммерческие версии TrueCrypt, поскольку уверены, что ПО для обеспечения безопасности должно быть с открытым исходным кодом и бесплатным.

Могу ли я оказать финансовое содействие проекту TrueCrypt?

Да. Пожалуйста, посетите для этого страницу http://www.truecrypt.org/donations/

Почему у TrueCrypt открытый исходный код? Каковы преимущества этого?

Поскольку исходный код TrueCrypt доступен всем желающим, у независимых экспертов есть возможность проверить, что он не содержит никаких брешей в безопасности или потайных 'лазеек'. Если бы исходный код был недоступен, экспертам пришлось бы прибегать к реинжинирингу исполняемых файлов. Однако проанализировать и осмыслить такой полученный в результате реинжиниринга код настолько сложно, что это практически невозможно *(особенно если код столь большой, как у TrueCrypt).*

Примечание: аналогичная проблема имеет место и в случае с аппаратурой для шифрования. Выполнить её реинжиниринг и проверить отсутствие брешей в безопасности и потайных 'лазеек' крайне сложно.

Исходный код TrueCrypt открыт, но есть ли кто-нибудь, кто на самом деле его проверял?

Да. Фактически, исходный код постоянно проверяют множество независимых исследователей и пользователей. Мы знаем это благодаря многим ошибкам и нескольким проблемам безопасности, обнаруженным независимыми исследователями (в том числе некоторыми хорошо известными) в результате просмотра исходного кода.

Так как TrueCrypt это ПО с открытым исходным кодом, независимые исследователи могут проверить, что исходный код не содержит никаких дефектов безопасности и 'потайных дверей'. Могут ли они также проверить, что официально распространяемые исполняемые файлы собраны из публично доступного исходного кода и не содержат никакого дополнительного кода?

Да, могут. Помимо исследования исходного кода, независимые эксперты могут скомпилировать исходный код и сравнить результирующие исполняемые файлы с официальными. При этом возможны некоторые расхождения (например, метки времени или встроенные цифровые подписи), но эти различия можно проанализировать и убедиться, что они несут никакого вредоносного кода.

Можно ли использовать TrueCrypt на флэш-накопителе USB?

У вас есть два варианта:

1) *Зашифровать весь флэш-накопитель USB. Однако при этом с него не удастся запускать TrueCrypt.*
   Примечание: Windows не поддерживает несколько разделов на флэш-накопителях USB.

2) *Создать на флэш-накопителе USB файл-контейнер TrueCrypt (о том, как это сделать, см. главу Руководство для новичков). Если оставить на флэш-накопителе достаточно места (выбрав соответствующий размер контейнера TrueCrypt), то можно будет также хранить в нём программу TrueCrypt (*вместе *с контейнером – не* в *контейнере) и оттуда же её запускать (см. главу Портативный (переносной) режим).*

Шифрует ли TrueCrypt также имена файлов и папок?

Да. Вся файловая система внутри тома TrueCrypt зашифрована (включая имена файлов, имена папок и содержимое каждого файла). Это относится к обоим типам томов TrueCrypt – т. е. к файловым контейнерам (виртуальным дискам TrueCrypt) и к зашифрованным с помощью TrueCrypt разделам/устройствам.

Использует ли TrueCrypt распараллеливание?

Да. Увеличение скорости шифрования/дешифрования прямо пропорционально числу ядер/процессоров в компьютере. См. подробности в главе Распараллеливание.

Можно ли считывать данные из зашифрованного тома/диска и записывать их туда так же быстро, как при использовании диска без шифрования?

Да, поскольку TrueCrypt использует конвейеризацию и распараллеливание. См. подробности в главах Конвейеризация и Распараллеливание.
Поддерживает ли TrueCrypt аппаратное ускорение шифрования?

Да. См. подробности в главе Аппаратное ускорение.

Можно ли загружать Windows, установленную в скрытом томе TrueCrypt?

Да, можно (начиная с TrueCrypt 6.0). См. подробности в разделе Скрытая операционная система.

Смогу ли я смонтировать свой том TrueCrypt на любом компьютере?

*Да. Тома TrueCrypt не зависят от операционной системы. Том TrueCrypt можно смонтировать на любом компьютере, в котором можно запустить TrueCrypt (см. также вопрос "*Можно использовать TrueCrypt в Windows, если у меня нет прав администратора?*").*

Можно ли извлечь или выключить устройство с «горячим» подключением (например, флэш-накопитель USB или жёсткий диск с интерфейсом USB), когда на нём находится смонтированный том TrueCrypt?

*Прежде чем отсоединить или выключить такое устройство, сначала всегда следует в TrueCrypt размонтировать том, а затем выполнить операцию "*Извлечь*", если это доступно (по щелчку правой кнопкой мыши на устройстве в списке "*Компьютер*" или "*Мой компьютер*"), либо воспользоваться функцией "*Безопасное извлечение устройства*" (встроенной в Windows и доступной в области уведомлений на панели задач). В противном случае возможна потеря данных.*

Что такое «скрытая операционная система»?

См. раздел Скрытая операционная система.

Что такое «правдоподобное отрицание причастности»?

См. главу Правдоподобное отрицание причастности.

Смогу ли я монтировать свой раздел/контейнер TrueCrypt после того, как переустановлю или обновлю операционную систему?

Да, тома TrueCrypt не зависят от операционной системы. При этом, однако, нужно убедиться, что программа установки вашей операционной системы не выполняет форматирование раздела, где находится том TrueCrypt.

Примечание: если системный раздел/диск зашифрован, и вы хотите переустановить или обновить Windows, сначала его нужно расшифровать (выберите Система > Перманентно расшифровать системный раздел/диск*). В то же время, запущенную операционную систему обновлять (устанавливать обновления безопасности, пакеты обновления и т. п.) можно без всяких проблем, даже если системный раздел/диск зашифрован.*

Могу ли я обновить TrueCrypt со старой версии до новейшей без каких-либо проблем?

Как правило, да. Тем не менее, перед обновлением ознакомьтесь с примечаниями к версиям для всех версий TrueCrypt, выпущенных после вашей. В случае, если имеются известные проблемы или несовместимости, касающиеся обновления вашей версии до более новой, они будут там указаны.

Могу ли я обновить версию TrueCrypt, если зашифрован системный раздел/диск, или мне нужно сначала его дешифровать?

Как правило, вы можете обновлять программу до самой новой версии без дешифрования системного раздела/диска (просто запустите программу установки TrueCrypt, и она автоматически обновит TrueCrypt в вашей системе). Тем не менее, перед обновлением ознакомьтесь с примечаниями к версиям для всех версий TrueCrypt, выпущенных после вашей. В случае, если имеются известные проблемы или несовместимости, касающиеся обновления вашей версии до более новой, они будут там указаны. Обратите внимание, что данный ответ адресован и пользователям скрытых операционных систем. Также примите к сведению, что если системный раздел/диск зашифрован, то устанавливать более ***старую*** *версию TrueCrypt нельзя.*

Я использую дозагрузочную аутентификацию. Можно ли сделать так, чтобы при включении компьютера никто не мог увидеть, что я пользуюсь TrueCrypt?

Да (начиная с TrueCrypt версии 6.1). Чтобы это сделать, загрузите зашифрованную систему, запустите TrueCrypt, выберите Настройки > Шифрование системы*, включите опцию '*Пустой экран аутентификации*' и нажмите* OK*. После этого загрузчик TrueCrypt при включении компьютера не будет выводить на экран никакого текста (даже если введён неправильный пароль). При вводе пароля будет казаться, что компьютер "завис". При этом, однако, важно помнить, что если неприятелю доступно для анализа содержимое жёсткого диска, то он сможет обнаружить и наличие загрузчика TrueCrypt.*

Я использую дозагрузочную аутентификацию. Можно ли настроить загрузчик TrueCrypt так, чтобы он выводил на экран только обманное сообщение об ошибке?

Да (начиная с TrueCrypt версии 6.1). Чтобы это сделать, загрузите зашифрованную систему, запустите TrueCrypt, выберите Настройки > Шифрование системы*, включите опцию '*Пустой экран аутентификации*' и введите в соответствующем поле обманное сообщение об ошибке (например, можно ввести сообщение "*Missing operating system*", которое обычно выводит загрузчик Windows, если ему не удаётся обнаружить загрузочный раздел Windows). При этом, однако, важно помнить, что если неприятелю доступно для анализа содержимое жёсткого диска, то он сможет обнаружить и наличие загрузчика TrueCrypt.*

Можно ли настроить TrueCrypt так, чтобы при каждом старте Windows выполнялось автоматическое монтирование несистемного тома TrueCrypt, пароль для которого совпадает с паролем для системного раздела/диска (т. е. с паролем дозагрузочной аутентификации)?

Да. Для этого сделайте следующее:

1. *Смонтируйте том (на ту букву диска, на которую вы хотите, чтобы он монтировался каждый раз).*
2. *Щёлкните правой кнопкой мыши на томе в списке дисков в главном окне TrueCrypt и выберите '*Добавить в системные избранные*'.*
3. *В появившемся окне упорядочивания системных избранных томов включите опцию '*Монтировать системные избранные тома при старте Windows*' и нажмите* OK*.*

*Более подробную информацию см. в главе '*Системные избранные тома*'.*

Можно ли автоматически монтировать том при каждом моём входе в Windows?

Да. Для этого сделайте следующее:

1. *Смонтируйте том (на ту букву диска, на которую вы хотите, чтобы он монтировался каждый раз).*
2. *Щёлкните правой кнопкой мыши на томе в списке дисков в главном окне TrueCrypt и выберите '*Добавить в избранные*'.*
3. *В появившемся окне* 'Избранные тома' *включите опцию '*Монтировать выбранный том при входе в систему*' и нажмите* OK*.*

После этого при каждом входе в Windows вам будет предлагаться указать пароль тома (и/или ключевые файлы), и в случае правильного ввода том будет смонтирован.

Как альтернативный вариант, если тома – на основе раздела/устройства, и если вам не нужно монтировать их всякий раз только на какие-то конкретные буквы дисков, вы можете проделать следующее:

1. *Выберите* Настройки > Параметры*. Появится окно 'Параметры*'.
2. *В группе '*Действия при входе в Windows*' включите опцию '*Монтировать все тома на устройствах' *и нажмите* OK*.*

*Примечание: TrueCrypt не будет спрашивать пароль, если вы включили кэширование пароля дозагрузочной аутентификации (*Настройки > Шифрование системы*), а у томов такой же пароль, что и у системного раздела/диска.*

Можно ли автоматически монтировать том при подключении к компьютеру хост-устройства, на котором находится этот том?

Да. Например, если вы храните контейнер TrueCrypt на флэш-накопителе USB («флэшке») и хотите, чтобы он автоматически монтировался при вставке «флэшки» в порт USB, сделайте следующее:

1. *Смонтируйте том (на ту букву диска, на которую вы хотите, чтобы он монтировался каждый раз).*
2. *Щёлкните правой кнопкой мыши на томе в списке дисков в главном окне TrueCrypt и выберите '*Добавить в избранные*'.*
3. *В появившемся окне* 'Избранные тома' *включите опцию '*Монтировать выбранный том при подключении устройства, на котором он расположен*' и нажмите* OK*.*

После этого при каждой вставке «флэшки» в USB-разъём вам будет предлагаться указать пароль тома (и/или ключевые файлы) (если только он уже не был помещён в кэш), и в случае правильного ввода том будет смонтирован.

*Примечание: TrueCrypt не будет спрашивать пароль, если вы включили кэширование пароля дозагрузочной аутентификации (*Настройки > Шифрование системы*), а пароль у тома такой же, как и у системного раздела/диска.*

Можно ли поместить в кэш (запомнить) мой пароль дозагрузочной аутентификации, чтобы его можно было использовать для монтирования несистемных томов в течение данного сеанса работы?

Да. Выберите Настройки > Шифрование системы *и включите параметр '*Кэшировать пароль дозагрузочной аутентификации в памяти драйвера*'.*

Я живу в стране, где в отношении её граждан нарушаются основные права человека. Существует ли возможность использовать TrueCrypt, не оставляя никаких 'следов' в незашифрованной Windows?

Да. Для этого нужно запускать TrueCrypt в переносном (portable) режиме в среде BartPE или аналогичном окружении. BartPE (расшифровывается как "Bart's Preinstalled Environment") в действительности представляет собой операционную систему Windows, подготовленную таким образом, чтобы она целиком находилась на CD/DVD и оттуда же загружалась (реестр, временные файлы и т. п. хранятся в ОЗУ – жёсткий диск при этом не используется вовсе и даже может отсутствовать). Чтобы преобразовать установочный компакт-диск Windows XP в BartPE CD, можно воспользоваться бесплатным конструктором Bart's PE Builder. Обратите внимание, что для BartPE даже не требуется никакого особого модуля (плагина) TrueCrypt. Сделайте следующее:

1. *Создайте BartPE CD и загрузитесь с него. (Внимание: все следующие шаги должны выполняться из среды BartPE.)*

2. *Загрузите самораспаковывающийся пакет TrueCrypt в RAM-диск (который BartPE создаёт автоматически).*

   ***Примечание**: если неприятель имеет возможность перехватывать данные, которые вы отправляете или получаете через Интернет, и вам нужно, чтобы он не знал, что вы загружали TrueCrypt, выполняйте загрузку через **I2P**, **Tor** или другие аналогичные анонимайзеры работы в сети.*

3. *Проверьте цифровые подписи у загруженного файла (подробности см. в разделе Цифровые подписи).*

4. *Запустите загруженный файл и выберите на второй странице мастера установки TrueCrypt опцию* Extract *(вместо* Install*). Извлеките содержимое на RAM-диск.*
   Примечание переводчика: если в папке с самораспаковывающимся дистрибутивным пакетом у вас также находится русский языковый файл TrueCrypt, на второй странице мастера установки нужный пункт будет называться Извлечь *(выберите его вместо*

Установить*)*

5. *Запустите файл* TrueCrypt.exe *с RAM-диска.*

Примечание: в качестве альтернативного варианта вы можете создать скрытую операционную систему (см. раздел Скрытая операционная система). См. также главу Правдоподобное отрицание причастности.

Можно ли шифровать системный раздел/диск, если у меня нет клавиатуры со стандартной раскладкой США?

Да, TrueCrypt поддерживает все раскладки клавиатуры.

Можно ли сохранять данные в разделе с обманной системой, не рискуя повредить раздел со скрытой системой?

Да. Вы можете записывать данные в раздел с обманной системой в любое время безо всякого риска повредить скрытый том (потому что обманная система не *установлена в том же разделе, что и скрытая система). Подробности см. в разделе Скрытая операционная система.*

Можно ли использовать TrueCrypt в Windows, если у меня нет прав администратора?

См. главу 'Использование TrueCrypt без прав администратора'.

Сохраняет ли TrueCrypt мой пароль на диске?

Нет.

Как TrueCrypt проверяет правильность введённого пароля?

См. главу Технические подробности, раздел Схема шифрования.

Можно ли зашифровать раздел/диск без потери находящихся там данных?

Да, но должны быть соблюдены следующие условия:

- *Если вы хотите зашифровать весь системный диск (который может содержать несколько разделов) или системный раздел (другими словами, если вам нужно зашифровать диск или раздел, где установлена Windows), вы можете это сделать при условии, что используете TrueCrypt 5.0 или новее и Windows XP или более новую версию Windows (например, Windows 7) (выберите '*Система*' > '*Зашифровать системный раздел/диск*' и следуйте инструкциям мастера).*

- *Если вы хотите зашифровать несистемный раздел «на месте», то можете это сделать при условии, что он содержит файловую систему NTFS и что вы*

используете TrueCrypt 6.1 или новее и Windows Vista или более новую версию Windows (например, Windows 7) (нажмите ‘Создать том’ > ‘Зашифровать несистемный раздел/диск’ > ‘Обычный том’ > ‘Устройство’ > ‘Зашифровать раздел на месте’ *и следуйте инструкциям мастера).*

Можно ли запустить TrueCrypt без его установки в систему (инсталляции)?

Да, см. главу Портативный (переносной) режим.

Некоторые программы шифрования для предотвращения атак применяют криптопроцессор TPM. Будет ли его также использовать и TrueCrypt?

Нет. Такие программы используют TPM для защиты против атак, при которых ***необходимо****, чтобы неприятель имел права администратора или физический доступ к компьютеру, и неприятелю нужно, чтобы после его доступа вы воспользовались компьютером.* ***Однако если удовлетворено любое из этих условий, защитить компьютер в действительности невозможно*** *(см. ниже), поэтому нужно прекратить им пользоваться (а не полагаться на TPM).*

Если неприятель обладает правами администратора, он может, например, выполнить сброс TPM, захватить содержимое ОЗУ (с хранящимися там мастер-ключами) или файлов в смонтированных томах TrueCrypt (расшифрованных «на лету»), которое затем может быть переправлено неприятелю через Интернет или сохранено на незашифрованном локальном диске (с которого неприятель считает эту информацию, когда получит физический доступ к компьютеру).

Если у неприятеля есть физический доступ к аппаратной части компьютера (и вы пользовались ПК после того, как с ним имел дело неприятель), он может, например, внедрить в него вредоносный компонент (скажем, аппаратный модуль слежения за нажатием клавиш на клавиатуре), который будет захватывать пароли, содержимое ОЗУ (с хранящимися там мастер-ключами) или файлов в смонтированных томах TrueCrypt (расшифрованных «на лету»), после чего пересылать все эти данные неприятелю по Интернету или сохранять на незашифрованном локальном диске (с которого неприятель сможет считать их, когда снова получит физический доступ к компьютеру).

Единственная вещь, которую TPM почти способен гарантировать, – создание ложного чувства безопасности (одно только имя – “Trusted Platform Module” (модуль доверенной платформы) – вводит в заблуждение и создаёт ложное чувство безопасности). Для настоящей защиты TPM в действительности излишен (а внедрение избыточных функций, как правило, ведёт к созданию так называемого bloatware – функционально избыточного и ресурсоёмкого ПО). Функции, подобные этой, иногда называют ‘театральной безопасностью’ [6].

Подробности см. в разделах Физическая безопасность *и* Вредоносное ПО (malware).

Почему Windows Vista (и более новые версии Windows) спрашивают у меня разрешения при каждом запуске TrueCrypt в ‘переносном’ (‘portable’) режиме?

Когда вы запускаете TrueCrypt в переносном режиме, TrueCrypt должен загрузить и запустить свой драйвер. Драйвер нужен TrueCrypt для обеспечения незаметного пользователю шифрования/дешифрования «на лету», а пользователи без прав администратора запускать драйверы устройств в Windows не могут. Поэтому Windows Vista и более новые версии Windows запрашивают у вас разрешение на запуск TrueCrypt с привилегиями администратора.

Обратите внимание, что если вы установите (инсталлируете) TrueCrypt в систему (в отличие от запуска TrueCrypt в переносном режиме), запрос разрешения при каждом запуске выдаваться не будет.

Нужно ли размонтировать тома TrueCrypt перед завершением работы или перезагрузкой Windows?

Нет. При завершении работы или перезагрузке системы TrueCrypt размонтирует все свои смонтированные тома автоматически.

Какой тип тома TrueCrypt лучше – раздел или файл-контейнер?

Файловые контейнеры это обычные файлы, поэтому с ними можно обращаться точно так же, как с любыми обычными файлами (например, как и другие файлы, их можно перемещать, переименовывать и удалять). Разделы/диски могут быть лучше в плане производительности. Примите к сведению, что если контейнер сильно фрагментирован, операции чтения и записи с ним могут выполняться значительно дольше. Чтобы решить эту проблему, дефрагментируйте файловую систему, в которой хранится этот контейнер (при размонтированном томе TrueCrypt).

Как лучше выполнять резервирование (backup) тома TrueCrypt?

См. главу О безопасном резервировании данных.

Что произойдёт, если я отформатирую раздел TrueCrypt?

*См. ответ на вопрос "*Можно ли изменить файловую систему в зашифрованном томе?*" в этом списке часто задаваемых вопросов.*

Можно ли изменить файловую систему в зашифрованном томе?

*Да, будучи смонтированными, тома TrueCrypt могут быть отформатированы в FAT12, FAT16, FAT32, NTFS или в любую другую файловую систему. Тома TrueCrypt ведут себя как обычные дисковые устройства, поэтому вы можете щёлкнуть правой кнопкой мыши по значку устройства (например, в окне '*Компьютер*' или '*Мой компьютер*') и выбрать пункт 'Форматировать'. Текущее содержимое тома будет при этом потеряно, но сам том останется полностью зашифрованным. Если вы отформатируете зашифрованный с помощью TrueCrypt раздел, когда том на основе этого раздела не смонтирован, то этот том будет уничтожен, а раздел перестанет быть зашифрованным (он станет*

пустым).

Можно ли смонтировать контейнер TrueCrypt, находящийся на CD или DVD?

Да. Однако если вам требуется монтировать том TrueCrypt на не допускающем записи носителе (таком, как CD или DVD) в среде Windows 2000, файловой системой внутри тома TrueCrypt должна быть FAT (Windows 2000 не может монтировать файловую систему NTFS на носителях, доступных только для чтения).

Можно ли изменить пароль для скрытого тома?

Да, диалог смены пароля работает как для обычных, так и для скрытых томов. Просто введите в диалоговом окне 'Изменение пароля' пароль для скрытого тома в поле 'Текущий пароль'.

Замечание: сначала TrueCrypt пытается расшифровать заголовок обычного тома, и если это не удаётся, то пытается расшифровать область внутри тома, где может находиться заголовок скрытого тома (если внутри есть скрытый том). Если попытка успешна, пароль изменяется у скрытого тома. (При обеих попытках используется пароль, введённый в поле '*Текущий пароль*'.)

Если я использую HMAC-RIPEMD-160, равняется ли размер ключа шифрования заголовка всего 160 битам?

Нет, TrueCrypt никогда не использует вывод хеш-функции (и алгоритма HMAC) непосредственно как ключ шифрования. См. подробности в разделе 'Деривация ключа заголовка, соль и подсчёт итераций'.

Как записать на DVD контейнер TrueCrypt размером больше 2 Гбайт?

Используемое вами ПО для записи DVD должно позволять выбирать формат DVD. Если это так, выберите формат UDF (в формате ISO файлы размером больше 2 Гбайт не поддерживаются).

Можно ли использовать утилиты* chkdsk, Disk Defragmenter *и им подобные для данных, находящихся на смонтированном томе TrueCrypt?

Да, тома TrueCrypt ведут себя как настоящие физические дисковые устройства, поэтому с содержимым смонтированного тома TrueCrypt можно использовать любые программы для проверки/починки/дефрагментации файловых систем.

Поддерживает ли TrueCrypt 64-разрядные версии Windows?

Да.

Могу ли я смонтировать мой том TrueCrypt в Windows, Mac OS X и Linux?

Да, тома TrueCrypt обладают полной межплатформной совместимостью.

Можно ли установить приложение в том TrueCrypt и запускать его оттуда?

Да.

Что произойдёт, если повредится часть тома TrueCrypt?

Один повреждённый бит в зашифрованных данных обычно вызывает повреждение всего блока шифротекста, в котором он расположен. Используемые TrueCrypt блоки шифротекста имеют размер 16 байт (т. е. 128 бит). В TrueCrypt применяется режим операции, гарантирующий, что в случае повреждения данных внутри блока, остальные блоки это не затронет (более подробную информацию см. в разделе Режимы операции*). Также см. вопрос '*Что делать, если в томе TrueCrypt повреждена зашифрованная файловая система?*'*

Что делать, если в томе TrueCrypt повреждена зашифрованная файловая система?

*Файловая система внутри тома TrueCrypt может оказаться повреждённой так же, как и любая другая обычная незашифрованная файловая система. Если это произошло, для её починки можно воспользоваться соответствующими средствами, входящими в состав вашей операционной системы. В Windows это утилита 'chkdsk'. TrueCrypt предоставляет простой способ её использования для томов TrueCrypt: щёлкните правой кнопкой мыши по смонтированному тому в главном окне TrueCrypt (в списке дисков) и выберите в контекстном меню пункт '*Исправить файловую систему*'.*

Мы используем TrueCrypt в корпоративном окружении/на предприятии. Есть ли способ для администратора сбросить пароль от тома или дозагрузочной аутентификации в случае, если пользователь его забыл (или потерял ключевой файл)?

Да. Примите к сведению, что в TrueCrypt не встроено никаких "потайных лазеек". Тем не менее, есть *способ "сбросить" пароли/ключевые файлы для тома и для дозагрузочной аутентификации. После того, как вы создадите том, сохраните резервную копию его заголовка в файле (выберите* Сервис -> Создать резервную копию заголовка тома*) до того, как позволите пользователю без прав администратора начать работать с этим томом. Обратите внимание: в заголовке тома (зашифрованного с помощью ключа заголовка, полученного из пароля/ключевого файла) содержится мастер-ключ, которым зашифрован том. Затем попросите пользователя выбрать пароль и установите его для него/неё (*Тома -> Изменить пароль тома*) или сгенерируйте для пользователя ключевой файл. После этого вы можете разрешить пользователю начать работать с томом и изменять пароль/ключевые файлы без вашего участия/разрешения. Теперь если пользователь забудет свой пароль или потеряет ключевой файл, вы сможете "сбросить" пароль/ключевые файлы тома в ваши исходные администраторские пароль/ключевые файлы, восстановив заголовок тома из файла с резервной копией (*Сервис -> Восстановить заголовок тома*).*

Аналогичным образом можно сбросить пароль к дозагрузочной аутентификации. Чтобы создать резервную копию данных мастер-ключа (которая будет сохранена на диске восстановления TrueCrypt и зашифрована вашим паролем администратора), выберите 'Система' > 'Создать диск восстановления'. Чтобы установить пользовательский пароль дозагрузочной аутентификации, выберите 'Система' > 'Изменить пароль'. Чтобы восстановить ваш пароль администратора, загрузитесь с диска восстановления TrueCrypt, выберите 'Repair Options' > 'Restore key data' и введите свой пароль администратора. Примечание: записывать каждый ISO-образ диска восстановления TrueCrypt на CD/DVD не требуется. Можно завести централизованное хранилище ISO-образов для всех рабочих станций (вместо хранилища дисков CD/DVD). Подробности см. в разделе Использование в режиме командной строки (ключ /noisocheck*).*

Можно ли нашей коммерческой компании использовать TrueCrypt бесплатно?

При условии, что выполняются все условия лицензии TrueCrypt, вы можете устанавливать и использовать TrueCrypt бесплатно на любом количестве ваших компьютеров.

Мы используем том с совместным доступом по сети. Существует ли способ автоматически восстанавливать этот совместно используемый сетевой ресурс при перезагрузке системы?

См. главу Совместное использование по сети.

Можно ли обращаться к одному и тому же тому TrueCrypt одновременно из нескольких операционных систем (например, к тому с совместным доступом по сети)?

См. главу Совместное использование по сети.

Может ли пользователь получить доступ к своему тому TrueCrypt через сеть?

См. главу Совместное использование по сети.

После шифрования несистемного раздела его исходная буква диска по-прежнему видна в окне 'Мой компьютер'. Если дважды щёлкнуть мышью по этой букве диска, Windows выдаёт запрос на форматирование этого диска. Можно ли как-нибудь скрыть или высвободить эту букву диска?

Да, чтобы высвободить букву диска, проделайте следующее:

1. *Щёлкните правой кнопкой мыши по значку 'Компьютер' (или 'Мой компьютер') на Рабочем столе или в меню 'Пуск' и выберите пункт* Управление*. Появится окно 'Управление компьютером'.*
2. *В списке слева выберите 'Управление дисками' (в подветви* Запоминающие устройства*).*
3. *Щёлкните правой кнопкой мыши по зашифрованному разделу/устройству и выберите 'Изменить букву диска или путь к диску'.*

4. *Нажмите* Удалить.
5. *Если Windows попросит подтвердить действие, нажмите* Да.

Когда я подключаю к компьютеру зашифрованный флэш-накопитель USB, Windows предлагает его отформатировать. Можно ли как-нибудь предотвратить появление этого запроса?

Да, но потребуется удалить присвоенную этому устройству букву диска. О том, как это сделать, см. вопрос ‘После шифрования несистемного раздела его исходная буква диска по-прежнему видна в окне ‘Мой компьютер’.’

Как удалить или отменить шифрование, если оно мне больше не нужно? Как перманентно расшифровать том?

См. раздел Как удалить шифрование.

Что изменится, если включить параметр ‘Монтировать тома как сменные носители’?

См. раздел Том, смонтированный как сменный носитель.

Нужно ли «затирать» (“wipe”) свободное место и/или файлы в томе TrueCrypt?

Примечание: “затереть” ("wipe") = надёжно удалить; перезаписать важные данные другими с целью сделать невозможным их восстановление.

Если вы полагаете, что неприятель сможет расшифровать том (например, вынудив вас сообщить пароль), тогда ответ – да. В противном случае в этом нет необходимости, так как том полностью зашифрован.

Как TrueCrypt определяет алгоритм, с помощью которого зашифрован том TrueCrypt?

См. раздел Схема шифрования (глава Технические подробности).

Технические подробности

Система обозначений

C	Блок шифротекста
$D_K()$	Алгоритм дешифрования, используемый ключом K шифрования/дешифрования
$E_K()$	Алгоритм шифрования, используемый ключом K шифрования/дешифрования
$H()$	Функция хеширования
i	Блочный индекс для n-бит блоков; n зависит от контекста
K	Криптографический ключ
P	Блок незашифрованного текста
^	Побитовая операция “исключающее ИЛИ” (XOR)
$\oplus$	Сложение по модулю 2^n, где n – битовый размер самого левого операнда и результирующего значения (например, если левый операнд – 1-бит значение, а правый операнд – 2-бит значение, то: $1 \oplus 0 = 1$; $1 \oplus 1 = 0$; $1 \oplus 2 = 1$; $1 \oplus 3 = 0$; $0 \oplus 0 = 0$; $0 \oplus 1 = 1$; $0 \oplus 2 = 0$; $0 \oplus 3 = 1$)
$\otimes$	Модульное умножение двух полиномов в бинарном поле GF(2) по модулю $x^{128}+x^7+x^2+x+1$ (GF означает Galois Field – поле Галуа)
||	Конкатенация

Схема шифрования

При монтировании тома TrueCrypt (предполагаем, что нет кэшированных паролей/ключевых файлов) или при дозагрузочной аутентификации выполняются следующие операции:

1. Считываются (помещаются) в ОЗУ первые 512 байт тома (т. е. заголовок обычного тома), из которых первые 64 байта это соль (см. *Спецификация формата томов TrueCrypt*). Для шифрования системы (см. главу *Шифрование системы*) в ОЗУ считываются последние 512 байт первой дорожки логического диска (загрузчик TrueCrypt располагается в первой дорожке системного диска и/или диска восстановления TrueCrypt).

2. Считываются (помещаются) в ОЗУ байты 65536–66047 тома (см. раздел *Спецификация формата томов TrueCrypt*). Для шифрования системы считываются байты 65536–66047 раздела, расположенного сразу за активным разделом[1] (см. раздел *Скрытая операционная система*). Если внутри этого тома имеется скрытый том (или внутри раздела, следующего за загрузочным разделом), то в этой точке мы считали его заголовок; в противном случае мы просто считали случайные данные (есть скрытый том внутри или его нет, определяется только попыткой расшифровать эти данные; подробности см. в разделе *Скрытый том*).

3. Сейчас TrueCrypt пытается расшифровать заголовок обычного тома, считанный в (1). Все данные, использованные и сгенерированные в ходе процесса дешифрования, хранятся в ОЗУ (TrueCrypt никогда не сохраняет их на диске). Указанные ниже параметры неизвестны[2] и определяются методом проб и ошибок (т. е. проверкой всех возможных комбинаций следующего):

    a. PRF (псевдослучайная функция), применяемая при деривации ключа заголовка (как определено в PKCS #5 v2.0; см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*), которая может быть одной из следующих: HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.
    Введённый пользователем пароль (который может сопровождаться одним или несколькими ключевыми файлами – см. раздел *Ключевые файлы*) и соль, считанная в (1), переданные функции деривации ключа заголовка, создающей последовательность значений (см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*), из которых формируются ключ шифрования заголовка и вторичный ключ заголовка (режим XTS). (Эти ключи используются для

[1] Если размер активного раздела меньше 256 Мбайт, то данные считываются из *второго* раздела позади активного (Windows 7 и более новые версии по умолчанию загружаются не из раздела, в котором они установлены).

[2] Эти параметры держатся в секрете *не* для того, чтобы осложнить жизнь неприятелю, а в основном для того, чтобы сделать тома TrueCrypt неидентифицируемыми (неотличимыми от набора случайных данных), чего было бы сложно добиться, если бы эти параметры хранились незашифрованными внутри заголовка тома. Примите также к сведению, что если для шифрования системы используется некаскадный алгоритм, то этот алгоритм *известен* (его можно определить, проанализировав содержимое незашифрованного загрузчика TrueCrypt, хранящегося в первой дорожке логического диска или на диске восстановления TrueCrypt).

дешифрования заголовка тома.)

b. Алгоритм шифрования: AES-256, Serpent, Twofish, AES-Serpent, AES-Twofish-Serpent и т. д.

c. Режим операции: XTS, LRW (*опротестованный/устаревший*), CBC (*опротестованный/устаревший*)

d. Ключевые файлы

4. Дешифрование считается успешно выполненным, если первые четыре байта расшифрованных данных содержат ASCII-строку “TRUE” и если контрольная сумма CRC-32 последних 256 байт расшифрованных данных (заголовок тома) совпадает со значением, находящимся в байте #8 расшифрованных данных (неприятелю это значение неизвестно, поскольку оно зашифровано – см. раздел *Спецификация формата томов TrueCrypt*). Если эти условия не выполнены, процесс продолжается с (3) снова, но на этот раз вместо данных, считанных в (1), используются данные, считанные в (2) (т. е. возможный заголовок скрытого тома). Если условия оказываются опять невыполненными, монтирование прекращается (неверный пароль, повреждённый том, не том TrueCrypt).

5. Теперь мы знаем (или предполагаем с очень высокой вероятностью), что у нас правильный пароль, правильный алгоритм шифрования, режим, размер ключа и правильный алгоритм деривации ключа заголовка. Если мы успешно расшифровали данные, считанные в (2), мы также знаем, что монтируется скрытый том, и знаем его размер, полученный из данных, считанных в (2) и расшифрованных в (3).

6. Подпрограмма шифрования переинициализируется с первичным мастер-ключом[1] и вторичным мастер-ключом (режим XTS – см. раздел *Режимы операции*), которые получены из расшифрованного заголовка тома (см. раздел *Спецификация формата томов TrueCrypt*). Эти ключи могут быть использованы для дешифрования любого сектора тома, за исключением области заголовка тома (или, в случае шифрования системы, области ключевых данных), зашифрованного с помощью ключей заголовка. Том смонтирован.

См. также раздел *Режимы операции* и подраздел *Деривация ключа заголовка, соль и подсчёт итераций*, а также главу *Модель механизма защиты*.

[1] Мастер-ключи генерируются во время создания тома и впоследствии уже не могут быть изменены. Смена пароля выполняется перешифрованием заголовка тома с использованием нового ключа заголовка (полученного из нового пароля).

Режимы операции

Режим операции, используемый TrueCrypt для шифрования разделов, дисков и виртуальных томов – XTS.

Режим XTS это, фактически, режим XEX [12], который разработал Phillip Rogaway в 2003 г., с незначительной модификацией (режим XEX использует один ключ для двух разных целей, тогда как режим XTS использует два независимых ключа).

В 2010 г. режим XTS был одобрен NIST (Национальным институтом стандартов и технологий США) для защиты конфиденциальных данных на устройствах хранения информации [24]. В 2007 г. он был также одобрен IEEE (Институтом инженеров по электротехнике и электронике США) для криптографической защиты данных в блочно-ориентированных устройствах хранения информации (IEEE 1619).

Описание режима XTS:

$C_i = E_{K1}(P_i \wedge (E_{K2}(n) \otimes \alpha^i)) \wedge (E_{K2}(n) \otimes \alpha^i)$

где:
$\otimes$ означает умножение двух полиномов в бинарном поле GF(2) по модулю $x^{128}+x^7+x^2+x+1$
$K1$ это ключ шифрования (256-бит для каждого поддерживаемого шифра; т. е. AES, Serpent и Twofish)
$K2$ это вторичный ключ (256-бит для каждого поддерживаемого шифра; т. е. AES, Serpent и Twofish)
i это индекс шифроблока внутри единицы данных; для первого шифроблока внутри единицы данных $i = 0$
n это индекс единицы данных внутри области действия $K1$; для первой единицы данных $n = 0$
α это примитивный элемент поля Галуа (2^{128}), соответствующий полиному x (т. е. 2)

Размер каждой единицы данных всегда равен 512 байтам (вне зависимости от размера сектора).

Дальнейшие сведения, касающиеся режима XTS, см., например, в [12] и [24].

Деривация ключа заголовка, соль и подсчёт итераций

Ключ заголовка используется для шифрования и дешифрования зашифрованной области заголовка тома TrueCrypt (в случае шифрования системы – области ключевых данных), которая содержит мастер-ключ и другую информацию (см. разделы *Схема шифрования* и *Спецификация формата томов TrueCrypt*). В томах, созданных с помощью TrueCrypt 5.0 или новее (и в случае шифрования системы), эта область зашифрована в режиме XTS (см. раздел *Режимы операции*). Для генерирования ключа заголовка и вторичного ключа заголовка (режим XTS) TrueCrypt использует метод PBKDF2, определённый в PKCS #5 v2.0; см. *Ссылки* [7].

В программе применяется 512-бит соль, что означает 2^{512} ключей для каждого пароля. Этим значительно уменьшается уязвимость по отношению к атакам с ‘offline’-словарём/’радужной таблицей’ (использование соли крайне осложняет предвычисление всех ключей для словаря паролей) [7]. Соль состоит из случайных значений, созданных генератором случайных чисел TrueCrypt в процессе создания тома. Функция деривации ключа заголовка основана на HMAC-SHA-512, HMAC-RIPEMD-160 или HMAC-Whirlpool (см. [8, 9, 20, 22]) – какая из них будет применяться, выбирается пользователем. Длина полученного в результате деривации ключа не зависит от размера вывода лежащей в основе хеш-функции. Например, длина ключа заголовка для шифра AES-256 всегда равна 256 битам, даже если используется HMAC-RIPEMD-160 (в режиме XTS применяется дополнительный 256-бит вторичный ключ заголовка; следовательно, для AES-256 всего применяются два 256-бит ключа). Более подробную информацию см. в [7]. Для деривации ключа заголовка выполняется 1000 итераций (или 2000, если в качестве лежащей в основе хеш-функции используется HMAC-RIPEMD-160), что увеличивает время, необходимое для выполнения полного поиска паролей (т. е. атаки методом перебора) [7].

Используемые шифрами при каскадном шифровании ключи заголовка взаимонезависимы, хотя и получены деривацией одного и того же пароля (к которому могут быть применены ключевые файлы). Например, для последовательности (каскада) AES-Twofish-Serpent, функции деривации ключа заголовка дано указание получить из введённого пароля 768-бит ключ шифрования (и, для режима XTS, вдобавок 768-бит *вторичный* ключ заголовка из введённого пароля). Сгенерированный 768-бит ключ заголовка затем разделяется на три 256-бит ключа (для режима XTS *вторичный* ключ заголовка также разделяется на три 256-бит ключа, поэтому в действительности каскад в целом использует шесть 256-бит ключей), из которых первый ключ используется шифром Serpent, второй – шифром Twofish, а третий – AES (кроме того, для режима XTS первый вторичный ключ используется шифром Serpent, второй вторичный ключ – шифром Twofish, и третий вторичный ключ – шифром AES). Отсюда следует, что даже если у неприятеля окажется один из ключей, он не сможет им

воспользоваться для деривации остальных, поскольку не существует реально осуществимого способа определить пароль по полученному из него в результате деривации ключу (за исключением атаки полным перебором при слабом пароле).

Генератор случайных чисел

Для генерирования мастер-ключа шифрования, вторичного ключа (режим XTS), соли и ключевых файлов в TrueCrypt используется генератор случайных чисел (RNG). Он создаёт в ОЗУ (оперативной памяти компьютера) пул из случайных значений. Этот пул размером 320 байт заполняется данными, получаемыми из следующих источников:

- перемещения мыши
- нажатия клавиш
- *Mac OS X и Linux*: значения, генерируемые встроенным RNG (*/dev/random* и */dev/urandom*)
- *только MS Windows*: MS Windows CryptoAPI (регулярно собираются с интервалом 500 мс)
- *только MS Windows*: статистика сетевого интерфейса (NETAPI32)
- *только MS Windows*: различные дескрипторы Win32, переменные времени и счётчики (регулярно собираются с интервалом 500 мс)

Прежде чем значение, полученное из любого вышеуказанного источника, будет записано в пул, оно разделяется на отдельные байты (например, 32-бит число делится на четыре байта). Затем эти байты индивидуально записываются в пул операцией сложения по модулю 2^8 (не заменяя старые значения в пуле) в позиции указателя пула. После записи байта позиция указателя пула перемещается на один байт вперёд. Когда указатель достигает конца пула, его позиция устанавливается в начало пула. После записи в пул каждого шестнадцатого байта, ко всему пулу автоматически применяется функция перемешивания (см. ниже).

Функция перемешивания пула

Назначение этой функции – выполнение диффузии [2]. Диффузия максимально распространяет (рассеивает) влияние индивидуальных “необработанных” (“raw”) входных бит по пулу, что также скрывает статистические зависимости. После записи в пул каждого шестнадцатого байта, эта функция применяется ко всему пулу.

Описание функции перемешивания пула:

1. Пусть R это пул случайных значений
2. Пусть H это выбранная пользователем функция хеширования (SHA-512, RIPEMD-160 или Whirlpool)
3. l = байтовый размер вывода функции хеширования H (т. е. если H это RIPEMD-160, то $l = 20$; если H это SHA-512, то $l = 64$)

4. z = байтовый размер пула случайных значений R (320 байт)
5. $q = z / l - 1$ (например, если H это Whirlpool, то $q = 4$)
6. R это поделённые на l-байт блоки $B_0...B_q$.
   Для $0 \le i \le q$ (т. е. для каждого блока B) выполняются следующие шаги:
   a. $M = H(B_0 \| B_1 \| ... \| B_q)$ [т. е. пул случайных значений хешируется с помощью хеш-функции H, что даёт хеш M]
   b. $B_i = B_i \wedge M$
7. $R = B_0 \| B_1 \| ... \| B_q$

Например, если $q = 1$, пул случайных значений будет перемешан следующим образом:

1. $(B_0 \| B_1) = R$
2. $B_0 = B_0 \wedge H(B_0 \| B_1)$
3. $B_1 = B_1 \wedge H(B_0 \| B_1)$
4. $R = B_0 \| B_1$

Создаваемые значения

Содержимое пула RNG никогда прямо не экспортируется (даже когда TrueCrypt даёт RNG инструкцию сгенерировать и экспортировать значение). Таким образом, даже если неприятель завладеет созданным RNG значением, это ему никак не поможет в определении или предсказании (с помощью полученного значения) любых других значений, созданных RNG в течение сеанса (определить содержимое пула, основываясь на сгенерированном RNG значении, невозможно).

RNG это гарантирует, выполняя следующие этапы всякий раз, когда TrueCrypt даёт инструкцию сгенерировать и экспортировать значение:

Данные, получаемые из перечисленных выше источников, добавляются в пул, как описано ниже.

- Запрошенное число байт копируется из пула в выходной буфер (копирование начинается с позиции указателя пула; по достижению конца пула копирование продолжается с начала пула, если запрошенное число байт больше размера пула, значение не генерируется и возвращается ошибка).

- Состояние каждого бита в пуле инвертируется (т.е. 0 становится 1, а 1 становится 0).

- Данные, полученные из какого-либо перечисленного выше источника, добавляются в пул, как описано выше.

- Содержимое пула трансформируется с помощью функции перемешивания пула . Примечание: эта функция использует криптографически стойкую одностороннюю хеш-функцию, выбираемую пользователем (подробности см. выше в разделе *Функция*

перемешивания пула).

- Трансформированное содержимое пула подвергается воздействию операции XOR в выходном буфере следующим образом:
    - Указатель записи в выходном буфере устанавливается в 0 (первый байт буфера).
    - Из пула считывается байт в позиции указателя пула и подвергается операции XOR в байт в выходном буфере в позиции указателя записи выходного буфера.
    - Позиция указателя пула смещается вперёд на один байт. По достижении конца пула позиция указателя устанавливается в 0 (первый байт пула).
    - Позиция указателя записи выходного буфера перемещается вперёд на один байт.
    - Этапы 2–4 повторяются для каждого остающегося байта в выходном буфере (чья длина равна запрошенному числу байт).
- Содержимое выходного буфера, являющееся окончательным значением, сгенерированным RNG, экспортируется.

Первоисточники

При разработке и реализации генератора случайных чисел за основу были взяты следующие работы:

- *Software Generation of Practically Strong Random Numbers*, автор: Peter Gutmann [10]
- *Cryptographic Random Numbers*, автор: Carl Ellison [11]

Ключевые файлы

Ключевой файл TrueCrypt это файл, содержимое которого объединяется с паролем. В качестве ключевого файла TrueCrypt можно использовать файл любого типа. Ключевой файл можно также получить с помощью встроенного генератора ключевых файлов TrueCrypt (RNG): он позволяет создать файл со случайным содержимым (более подробные сведения см. в разделе *Генератор случайных чисел*).

Максимальный размер ключевого файла неограничен; однако обрабатываются только его первые 1 048 576 байт (1 Мбайт) (все остальные байты игнорируются во избежание проблем с производительностью при обработке чрезвычайно больших файлов). Разрешается указывать как один, так и несколько ключевых файлов (их количество не ограничено).

Ключевые файлы допускается хранить в токенах безопасности и в смарт-картах, удовлетворяющих стандарту PKCS-11 [23] и защищённых несколькими PIN-кодами (которые можно вводить с помощью аппаратного пинпада либо из графического интерфейса TrueCrypt).

Ключевые файлы обрабатываются и применяются к паролю следующим образом:

1. Пусть *P* это указанный пользователем пароль к тому TrueCrypt (может быть пустым)
2. Пусть *KP* это пул ключевых файлов
3. Пусть *kpl* это размер пула ключевых файлов *KP*, в байтах (64, т. е. 512 бит); *kpl* должен быть кратен размеру вывода хеш-функции *H*
4. Пусть *pl* это длина пароля *P*, в байтах (в текущей версии: $0 \le pl \le 64$)
5. Если $kpl > pl$, добавляем $(kpl - pl)$ нулевых байт к паролю *P* (таким образом, $pl = kpl$)
6. Заполняем пул ключевых файлов *KP* нулевыми байтами в количестве *kpl*
7. Для каждого ключевого файла выполняем следующие шаги:
    a. Устанавливаем позицию указателя пула ключевых файлов в начало пула
    b. Инициализируем хеш-функцию *H*
    c. Загружаем один за другим все байты ключевого файла и для каждого загруженного байта выполняем следующие шаги:
        i. Хешируем загруженный байт с помощью хеш-функции *H* без инициализации хеша, чтобы получить промежуточный хеш (состояние)

M. Не финализируем хеш (состояние сохраняется для следующего раунда).

ii. Делим состояние *M* на индивидуальные байты.
Например, если размер вывода хеша – 4 байта, $(T_0 \parallel T_1 \parallel T_2 \parallel T_3) = M$

iii. Записываем эти байты (полученные на этапе 7.c.ii) индивидуально в пул ключевых файлов операцией сложения по модулю 2^8 (не заменяя старые значения в пуле) в позиции указателя пула. После записи байта позиция указателя пула перемещается на один байт вперёд. Когда указатель достигает конца пула, его позиция устанавливается в начало пула.

8. Применяем содержимое пула ключевых файлов к паролю *P*, используя следующий метод:
   a. Делим пароль *P* на индивидуальные байты $B_0...B_{pl-1}$.
   Обратите внимание, что если пароль короче, чем пул ключевых файлов, то пароль дополняется нулевыми байтами до длины пула в шаге 5 (отсюда следует, что с этого момента длина пароля всегда больше или равна длине пула ключевых файлов).
   b. Делим пул ключевых файлов *KP* на индивидуальные байты $G_0...G_{kpl-1}$
   c. Для $0 \le i < kpl$ выполняем: $B_i = B_i \oplus G_i$
   d. $P = B_0 \parallel B_1 \parallel ... \parallel B_{pl-2} \parallel B_{pl-1}$
9. Теперь передаём пароль *P* (после того, как к нему было применено содержимое пула ключевых файлов) функции деривации ключа заголовка PBKDF2 (PKCS #5 v2), которая обрабатывает его (наряду с солью и другими данными) с помощью выбранного пользователем криптостойкого хеш-алгоритма (например, SHA-512). Более подробные сведения см. в разделе *Деривация ключа заголовка, соль и подсчёт итераций*.

Роль хеш-функции *H* – только в выполнении диффузии [2]. В качестве хеш-функции *H* используется CRC-32. Обратите внимание, что вывод CRC-32 затем обрабатывается с помощью криптостойкого хеш-алгоритма: в паролю применяется содержимое пула ключевых файлов (в дополнение к хешированию с помощью CRC-32), который затем передаётся функции деривации ключа заголовка PBKDF2 (PKCS #5 v2), обрабатывающей его (наряду с солью и другими данными) с помощью выбранного пользователем криптостойкого хеш-алгоритма (например, SHA-512). Результирующие значения используются для формирования ключа заголовка и вторичного ключа заголовка (режим XTS).

Спецификация формата томов TrueCrypt

Смещение (байты)	Размер (байты)	Статус шифрования[1]	Описание
0	64	Не зашифровано[3]	Соль
64	4	Зашифровано	ASCII-строка “TRUE”
68	2	Зашифровано	Версия формата заголовка тома (5)
70	2	Зашифровано	Минимальная версия программы, необходимая для открытия тома
72	4	Зашифровано	CRC-32 (расшифрованных) байтов 256–511
76	16	Зашифровано	Зарезервировано (должно содержать нули)
92	8	Зашифровано	Размер скрытого тома (для не-скрытых томов — 0)
100	8	Зашифровано	Размер тома
108	8	Зашифровано	Байтовое смещение начала области действия мастер-ключа
116	8	Зашифровано	Размер зашифрованного участка в области действия мастер-ключа
124	4	Зашифровано	Биты флагов (бит 0 установлен: шифрование системы; бит 1 установлен: несистемный “на месте” зашифрованный том; биты 2-31 зарезервированы)
128	4	Зашифровано	Размер сектора (в байтах)
132	120	Зашифровано	Зарезервировано (должно содержать нули)
252	4	Зашифровано	CRC-32 (расшифрованных) байтов 64–251
256	*Пер.*	Зашифровано	Объединённые первичный и вторичный мастер-ключи[4]
512	65024	Зашифровано	Зарезервировано (при шифровании системы этот элемент опущен157)
65536	65536	Зашифровано /	Область заголовка скрытого тома (если внутри тома

[1] Зашифрованные области заголовка тома зашифрованы в режиме XTS с помощью первичного и вторичного ключей заголовка. Подробности см. в разделах *Схема шифрования* и *Деривация ключа заголовка, соль и подсчёт итераций*.

		Не зашифровано157	нет скрытого тома, эта область содержит случайные данные[3]). При шифровании системы этот элемент опущен.[4] См. байты 0–65535.
131072	*Пер.*	Зашифровано	Область данных (границы действия мастер-ключа). При шифровании системы смещение может быть другим (зависит от смещения системного раздела).
S–131072[1]	65536	Зашифровано / Не зашифровано157	Резервная копия заголовка (зашифрованная другим ключом заголовка, полученным с помощью другой соли). При шифровании системы этот элемент опущен.157 См. байты 0–65535.
S–65536	65536	Зашифровано / Не зашифровано157	Резервная копия заголовка скрытого тома (зашифрованная другим ключом заголовка, полученным с помощью соли). Если внутри тома нет скрытого тома, эта область содержит случайные данные.157 При шифровании системы этот элемент опущен.157 См. байты 0–65535.

Примите к сведению, что данная спецификация относится к томам, созданным с помощью TrueCrypt версии 7.0 или более новой. Формат томов на основе файла идентичен формату томов на основе раздела/устройства (однако "заголовок тома" или ключевые данные у системного раздела/диска хранятся в последних 512 байтах первой дорожки логического диска). Тома TrueCrypt не содержат никаких "сигнатур" или идентификационных строк. Будучи размонтированными, они выглядят как состоящие исключительно из случайных данных.

При создании каждого тома TrueCrypt, свободное место в томе заполняется случайными данными.[0] Случайные данные генерируются следующим образом: непосредственно перед началом форматирования тома TrueCrypt с помощью генератора случайных чисел (см. раздел *Генератор случайных чисел*) создаются временный ключ шифрования и временный вторичный ключ (режим XTS). Этими временными ключами инициализируется выбранный пользователем алгоритм шифрования. Затем с помощью алгоритма шифрования зашифровываются блоки незашифрованного текста, состоящие из нулей. Алгоритм шифрования работает в режиме XTS (см. раздел *Режимы операции*). Получаемые блоки шифротекста используются для заполнения (перезаписи) свободного места в томе. Временные ключи хранятся в ОЗУ, а по окончании форматирования стираются.

Поля, расположенные с байта #0 (соль) и #256 (мастер-ключи) содержат случайные данные, созданные генератором случайных чисел (см. раздел *Генератор случайных чисел*) во время создания тома. Если в томе TrueCrypt содержится скрытый том (внутри его пустого места),

[1] *S* это размер хоста тома (в байтах).

[3] Обратите внимание, что шифровать соль не требуется, так как её не нужно сохранять в тайне [7] (соль это последовательность случайных значений).

[4] Тут хранятся несколько объединённых мастер-ключей, когда том зашифрован последовательностью (каскадом) шифров (вторичные ключи используются для режима XTS).

[3] См. ниже в этом разделе сведения о методе, используемом для заполнения свободного места в томе случайными данными при его создании.

[4] Здесь в значение "шифрование системы" не входит скрытый том, содержащий скрытую операционную систему.

[0] При условии, что выключены опции *Быстрое форматирование* и *Динамический*, и что том не содержит файловую систему, зашифрованную «на месте» (обратите внимание, что TrueCrypt не позволяет создавать скрытый том внутри такого тома).

заголовок скрытого тома расположен с байта #65536 хост-тома (заголовок хост/внешнего тома расположен с байта #0 хост-тома – см. раздел *Скрытый том*). Если внутри тома TrueCrypt нет скрытого тома, байты 65536–131071 тома (т. е. область, где может находиться заголовок скрытого тома) содержат случайные данные (см. выше сведения о методе, применяемом для заполнения свободного пространства в томе случайными данными при его создании). Строение заголовка у скрытого тома такое же, как у обычного тома (байты 0–65535).

Максимально возможный размер тома TrueCrypt – 2^{63} байт (8 589 934 592 Гбайт). Однако из соображений безопасности (в связи с 128-бит размером блока, используемым алгоритмами шифрования), максимально разрешённый размер тома составляет 1 Пбайт (1 048 576 Гбайт).

Встроенные резервные копии заголовков

Каждый том TrueCrypt, созданный с помощью TrueCrypt версии 6.0 или новее, содержит встроенную резервную копию заголовка, расположенную в конце тома (см. выше). Резервная копия заголовка это *не* копия заголовка тома, так как она зашифрована другим ключом заголовка, полученным с использованием другой соли (см. раздел *Деривация ключа заголовка, соль и подсчёт итераций*).

При смене пароля и/или ключевых файлов или при восстановлении заголовка из встроенной (или внешней) резервной копии выполняется перешифрование заголовка тома и резервной копии заголовка (встроенной в том) с помощью других ключей заголовка (полученных с использованием вновь сгенерированной соли – соль для заголовка тома отличается от соли для резервной копии заголовка). Каждая соль создаётся генератором случайных чисел TrueCrypt (см. раздел *Генератор случайных чисел*).

Более подробные сведения о резервных копиях заголовков см. в подразделе *Сервис -> Восстановить заголовок тома* в главе *Главное окно программы*.

Соответствие стандартам и спецификациям

TrueCrypt соответствует следующим стандартам, спецификациям и рекомендациям:

- ISO/IEC 10118-3:2004 [21]
- FIPS 197 [3]
- FIPS 198 [22]
- FIPS 180-2 [14]
- NIST SP 800-3E [24]

- PKCS #5 v2.0 [7]
- PKCS #11 v2.20 [23]

Правильность реализации алгоритмов шифрования можно проверить с помощью теста векторов (выберите *Сервис > Тест алгоритмов генерирования векторов*) или путём исследования исходного кода TrueCrypt.

Исходный код

TrueCrypt это бесплатное программное обеспечение с открытым исходным кодом. Полный исходный код TrueCrypt (написанный на C, C++ и ассемблере) свободно доступен для ознакомления и исследования на сайте

http://www.truecrypt.org/

Планы на будущее

Список функций, запланированных для реализации в будущих версиях, доступен в Интернете на странице
http://www.truecrypt.org/future

Связь с разработчиками

Информация о том, как с нами связаться, доступна в Интернете на странице
http://www.truecrypt.org/contact

Правовая информация

Лицензия

Текст лицензионного соглашения, в соответствии с которым распространяется TrueCrypt, содержится в файле *License.txt*, входящем в состав дистрибутивных пакетов с самой программой TrueCrypt и с её исходным кодом, а также доступен по адресу:

http://www.truecrypt.org/legal/license

Авторские права

На данное ПО в целом:
Copyright © 2012 TrueCrypt Developers Association. Все права защищены.

На части данного ПО:
Copyright © 2003-2012 TrueCrypt Developers Association. Все права защищены.
Copyright © 1998-2000 Paul Le Roux. Все права защищены.
Copyright © 1998-2008 Brian Gladman, Worcester, UK. Все права защищены.
Copyright © 2002-2004 Mark Adler. Все права защищены.

Дополнительную информацию см. в правовых примечаниях к частям исходного кода.

Торговые марки

Все упомянутые в этом документе торговые марки являются исключительной собственностью их соответствующих владельцев.

История версий

7.1a

7 февраля 2012 г.

Улучшения и исправления ошибок:

- Незначительные улучшения и исправления ошибок (*Windows, Mac OS X и Linux*)

Список изменений в более ранних версиях см. тут: http://www.truecrypt.org/docs/?s=version-history

Благодарности

Мы выражаем благодарность следующим людям:

Paul Le Roux за предоставление его исходного кода E4M; TrueCrypt 1.0 ведёт своё происхождение от E4M, а некоторые части исходного кода E4M и поныне входят в исходный код текущей версии TrueCrypt.

Brian Gladman, автору превосходных подпрограмм AES, Twofish и SHA-512.

Peter Gutmann за его документ о случайных числах и за создание библиотеки cryptlib, послужившей источником части исходного кода генератора случайных чисел.

Wei Dai, автору подпрограмм Serpent и RIPEMD-160.

Mark Adler и другим авторам подпрограммы Inflate.

Разработчикам алгоритмов шифрования, хеширования и режима операции:
Horst Feistel, Don Coppersmith, Walt Tuchmann, Lars Knudsen, Ross Anderson, Eli Biham, Bruce Schneier, David Wagner, John Kelsey, Niels Ferguson, Doug Whiting, Chris Hall, Joan Daemen, Vincent Rijmen, Carlisle Adams, Stafford Tavares, *Phillip Rogaway, Hans Dobbertin, Antoon Bosselaers*, *Bart Preneel*, *Paulo S. L. M. Barreto.*

Всем остальным, благодаря кому стал возможен этот проект, всем, кто нас морально поддерживал, а также всем тем, кто присылал нам сообщения об ошибках и предложения по улучшению программы.

Большое вам спасибо.

Ссылки

[1] U.S. Committee on National Security Systems (CNSS), *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, CNSS Policy No. 15, Fact Sheet No. 1, June 2003, документ доступен тут: http://csrc.nist.gov/groups/STM/cmvp/documents/CNSS15FS.pdf.

[2] C. E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, v. 28, n. 4, 1949

[3] NIST, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001, документ доступен тут: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[4] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, NIST, *Report on the Development of the Advanced Encryption Standard (AES)*, October 2, 2000, Journal of Research of the National Institute of Standards and Technology, Vol. 106, No. 3, May-June 2001, документ доступен тут: http://nvl.nist.gov/pub/nistpubs/jres/106/3/j63nec.pdf.

[5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, *The Twofish Team's Final Comments on AES Selection,* May 15, 2000, документ доступен тут: http://csrc.nist.gov/archive/aes/round2/comments/20000515-bschneier.pdf.

[6] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Springer, 2003

[7] RSA Laboratories, *PKCS #5 v2.0: Password-Based Cryptography Standard*, RSA Data

Security, Inc. Public-Key Cryptography Standards (PKCS), March 25, 1999, документ доступен тут: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2-0.pdf
а также, с разрешения RSA Laboratories, тут: http://www.truecrypt.org/docs/pkcs5v2-0.pdf.

[8] H. Krawczyk, M. Bellare, R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, RFC 2104, February 1997, документ доступен тут: http://www.ietf.org/rfc/rfc2104.txt.

[9] M. Nystrom, RSA Security, *Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512*, RFC 4231, December 2005, документ доступен тут: http://www.ietf.org/rfc/rfc4231.txt.

[10] Peter Gutmann, *Software Generation of Practically Strong Random Numbers*, представлено в 1998 г. на симпозиуме Usenix Security Symposium, документ доступен тут: http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix98.pdf.

[11] Carl Ellison, *Cryptographic Random Numbers*, изначально как приложение к стандарту P1363, документ доступен тут: http://world.std.com/~cme/P1363/ranno.html.

[12] P. Rogaway, *Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC*, Asiacrypt 2004. LNCS vol. 3329. Springer, 2004. Также документ доступен тут:: http://www.cs.ucdavis.edu/~rogaway/papers/offsets.pdf.

[13] J. Kelsey, *Twofish Technical Report #7: Key Separation in Twofish*, AES Round 2 public comment, April 7, 2000

[14] NIST, *Secure Hash Standard*, FIPS 180-2, August 1, 2002, документ доступен тут: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf.

[15] U. Maurer, J. Massey, *Cascade Ciphers: The Importance of Being First*, Journal of Cryptology, v. 6, n. 1, 1993

[16] Bruce Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996

[17] Peter Gutmann, *Secure Deletion of Data from Magnetic and Solid-State Memory*, впервые опубликовано в Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996, документ доступен тут: http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

[18] Веб-страница шифра Serpent: http://www.cl.cam.ac.uk/~rja14/serpent.html.

[19] M. E. Smid, *AES Issues*, AES Round 2 Comments, May 22, 2000, документ доступен тут: http://csrc.nist.gov/archive/aes/round2/comments/20000523-msmid-2.pdf.

[20] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996

[21] International Organization for Standardization (ISO), *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*, ISO/IEC 10118-3:2004, February 24, 2004

[22] NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198, March 6, 2002, документ доступен тут: http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf.

[23] RSA Laboratories, *PKCS #11 v2.20: Cryptographic Token Interface Standard*, RSA Security, Inc. Public-Key Cryptography Standards (PKCS), June 28, 2004, документ доступен тут: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf.

[24] Morris Dworkin, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, NIST Special Publication 800-3E, January 2010, документ доступен тут: http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf.

Translated by Dmitry Yerokhin