3.4	1. Шифрование данных средствами прикладных программных продуктов. 2. Создание и использование защищенных криптоконтейнеров TrueCrypt.			2	Выполнение практических заданий

Тема: 3.4 Аппаратное и программное обеспечение защищенных компьютерных систем.

Учебные вопросы:

1. Шифрование данных средствами прикладных программных продуктов.
2. Создание и использование защищенных криптоконтейнеров TrueCrypt.

1. Шифрование данных средствами прикладных программных продуктов

Краткие теоретические сведения:

Использование программы «AxCrypt» шифрования файлов и папок

Одним из доступных и, вместе с тем, эффективных программных средств, позволяющих надежно шифровать папки и отдельные файлы, является бесплатная программа «AxCrypt».

Основные характеристики программы «AxCrypt»:

шифрование файлов с помощью пароля и ключевого файла, созданного программой;

использование алгоритма шифрования AES[1].

возможность создания зашифрованного *.EXE файла[2];

запуск зашифрованного файла без сохранения расшифрованной копии на диске;

возможность пакетного шифрования файлов и папок;

интеграция функциональных возможностей в контекстное меню Windows;

удаление файлов без возможности восстановления с помощью специальных программ.

Алгоритм работы с программой «AxCrypt» представляет следующую последовательность действий:

1. Создание ключевого файла (необязательный этап).

Примечание: ключевой файл – это файл любого типа (например, *.txt, *.exe, *.mp3, *.avi и др.), размер которого, как правило, значительно превышает длину основного пароля (для того, чтобы сделать атаку методом перебора ключевых файлов неосуществимой, размер ключевого файла должен быть не менее 30 байт) и чьё содержимое объединено с основным паролем. Использовать ключевые файлы необязательно, однако, их применение

[1] Advanced Encryption Standard (AES) – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США.

[2] .EXE (сокр. англ. *executable* – исполнимый) – расширение исполняемых файлов, применяемое в операционных системах семейства Windows.

обеспечивает более высоких уровень безопасности. Ключевые файлы могут существенно повысить стойкость защиты к атакам методом полного перебора (*brute force*), особенно при недостаточно надёжном пароле. Пока не будет предоставлен правильный ключевой файл, ни один зашифрованный файл, использующий этот ключевой файл, не сможет быть расшифрован.

Для того, чтобы создать ключевой файл средствами программы «AxCrypt» (программа позволяет создавать ключевые файлы только в формате *.txt), нажмите правой кнопкой мыши на системную папку «Мой компьютер» и в появившемся контекстном меню выберите команду **AxCrypt > Создать файл ключа** (рис. 1). После появления на экране соответствующего предупреждения нажмите кнопку «Ок», введите имя ключевого файла и его местоположение.

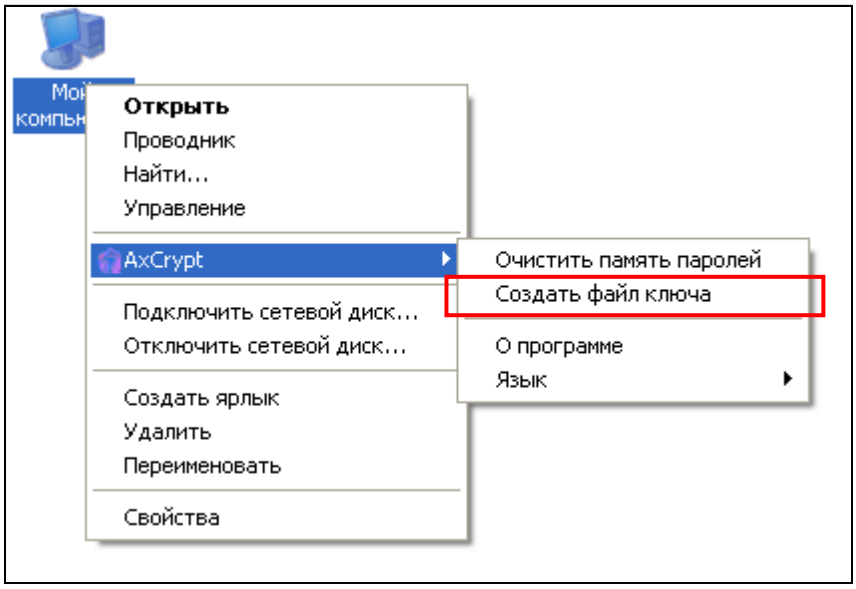

Рис. 1. Создание файла ключа

2. *Шифрование.* Для того, чтобы зашифровать объект (файл, папку) либо группу объектов, их следует выделить, нажать на выделенное правой кнопкой мыши и в появившемся контекстном меню выбрать одну их команд:

а) *шифровать*. Выделенные объекты будут зашифрованы без сохранения копий;

б) *шифровать копию*. Автоматически будут созданы копии выделенных объектов, которые и будут зашифрованы. Их оригиналы останутся нетронутыми;

в) *шифровать копию в .EXE*. Будут созданы копии выделенных объектов, которые будут зашифрованы в формате исполняемых файлов, позволяющем осуществлять их расшифровку на любом ПК без программы «AxCrypt».

При выборе любой из указанных команд откроется окно настройки параметров шифрования, в котором следует ввести и подтвердить пароль, а также (при необходимости) указать путь к ключевому файлу (рис. 2).

Если задать параметр «*Помнить для расшифровки*», то для расшифровки зашифрованного файла пароль вводить не потребуется до тех пор, пока

пользователь не выполнит команду **ПКМ**[3] **«Мой компьютер» > AxCrypt > Очистить память паролей**.

Если задать параметр «*Как пароль по умолчанию для шифрования*», то введенный пароль будет использоваться каждый раз по умолчанию для новых объектов шифрования до тех пор, пока пользователь не выполнит команду **ПКМ «Мой компьютер» > AxCrypt > Очистить память паролей**.

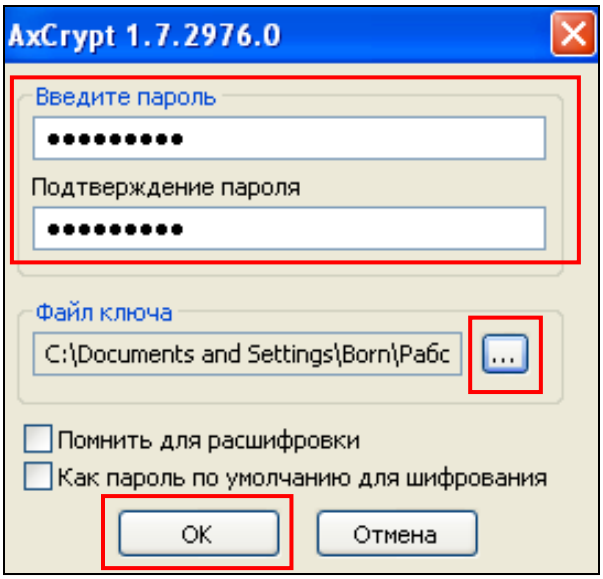

Рис. 2. Настройка параметров шифрования

После того как шифрование будет закончено расширение и иконки зашифрованных файлов сменятся (рис. 3).

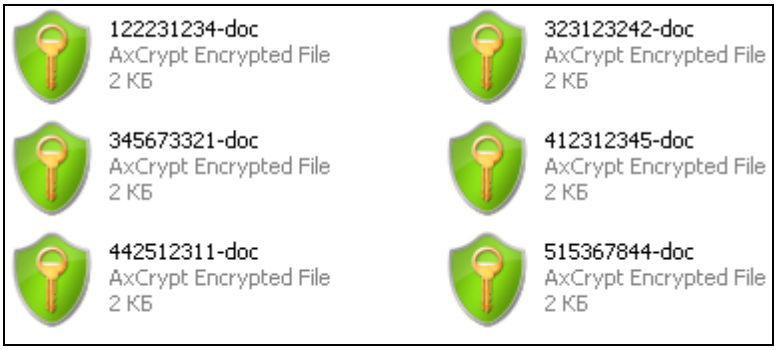

Рис. 3. Зашифрованные файлы

3. Расшифровка. В любой момент шифрование с файлов можно снять и вернуть их в исходное состояние. Для этого зашифрованные файлы выделить и выполнить команду **ПКМ > AxCrypt > Расшифровать** (рис. 4).

Если был включен параметр «*Помнить для расшифровки*», то для расшифровки выделенных файлов ввода пароля и ключевого файла не потребуется. Если был выключен, то программа потребует их ввести (рис. 5).

После этого файлы будут расшифрованы и доступны в обычном режиме.

[3] ПКМ – здесь и далее означает одиночное нажатие правой клавишей мыши на соответствующий объект.

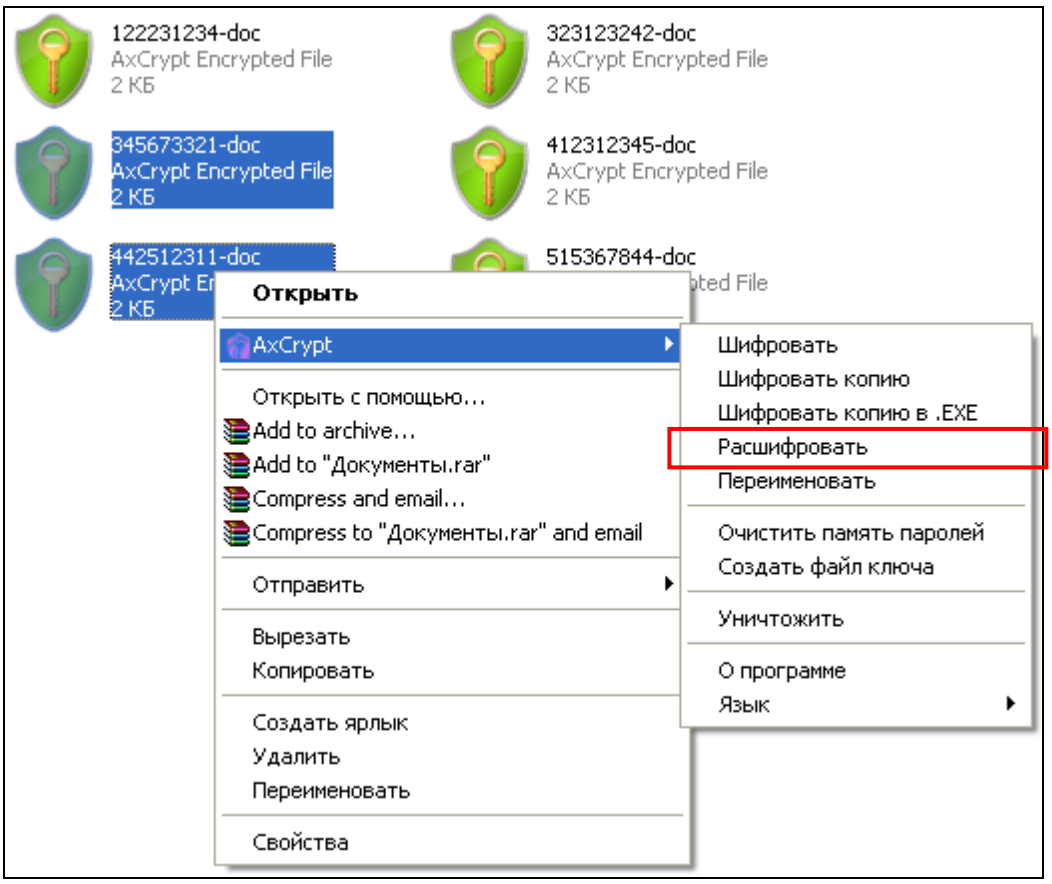

Рис. 4. Расшифровка выделенных файлов

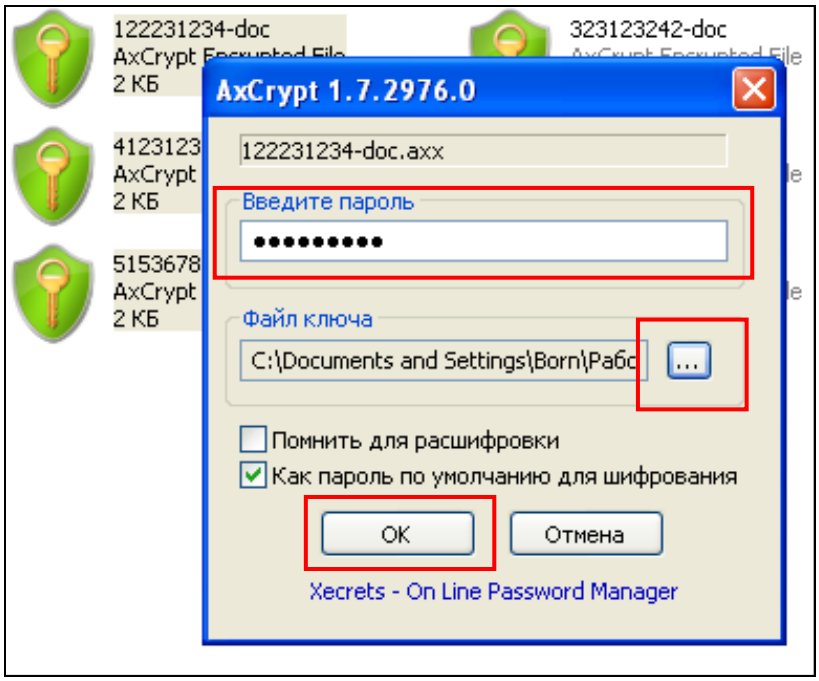

Рис. 5. Ввод пароля и ключевого файла (опционально) при расшифровке файлов

4. Безвозвратное удаление файлов. С помощью «AxCrypt» можно не только шифровать файлы, но и выполнять их безвозвратное удаление. Для этого файлы необходимо выделить и выполнить команду **ПКМ > AxCrypt >**

Уничтожить. После этого файлы будут полностью удалены с жесткого диска. Их нельзя будет восстановить через корзину или с помощью специализированных программ.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 3.4»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

1. Ознакомьтесь с теоретическими положениями, изложенными в настоящих рекомендациях и конспекте лекции № 3 «Аппаратное и программное обеспечение защищенных компьютерных систем» данной учебной дисциплины.
2. Создайте на диске **D:** папку **«Crypt_test»**. Создайте и скопируйте в эту папку несколько файлов произвольного содержания: *документ1.doc, документ2.doc, документ3.doc*.
3. Запустите программу «AxCrypt». Создайте с ее помощью файл ключа в формате *.txt. Сохраните его на рабочий стол под именем *File_key.txt*.
4. Файл *документ1.doc* зашифруйте без сохранения копии, с использованием ключевого файла *File_key.txt.* Придумайте и введите пароль, отвечающий необходимым требованиям безопасности. Зафиксируйте его в файл-отчете. Установите данный пароль в качестве пароля, используемого по умолчанию для шифрования последующих файлов.
5. Файл *документ2.doc* зашифруйте с сохранением копии, без использования ключевого файла.
6. Файл *документ3.doc* зашифруйте в формате исполняемого файла *.EXE, с использованием самостоятельно подготовленного ключевого файла произвольного формата, отличного от *.txt (например, *.doc, *.mp3, *.wav, *.jpg и др.).
7. Расшифруйте файл *документ1.doc*. При расшифровке включите кэширование пароля.
8. Расшифруйте остальные файлы.
9. Очистите память паролей. Объясните в файл-отчете необходимость выполнения данной операции.
10. С помощью программы «AxCrypt» осуществите *безвозвратное* удаление расшифрованных документов.
11. **Продемонстрируйте работу и файл-отчет преподавателю.**

12. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, в том числе зашифрованные; установите первоначальные настройки использованного программного обеспечения.

13. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое «закрытое» шифрование? В чем заключаются функциональные отличия программы «AxCrypt» и системы шифрования EFS? Приведите примеры их практического использования.
2. Что такое ключевой файл? В чем заключаются основные преимущества и недостатки его использования?
3. Что означает возможность создания зашифрованного *.EXE файла?
4. Что такое пакетное шифрование файлов?
5. Для чего используется кэширование паролей в программе «AxCrypt»? Приведите примеры его практического применения.
6. В чем именно заключается интеграция функциональных возможностей программы «AxCrypt» в контекстное меню Windows?

2. Создание и использование защищенных криптоконтейнеров TrueCrypt

Краткие теоретические сведения:

«TrueCrypt» – это программное обеспечение, предназначенное для создания томов (криптоконтейнеров) и работы с ними с использованием шифрования «на лету». Шифрование «на лету» означает, что данные автоматически шифруются или расшифровываются непосредственно при их чтении или сохранении, т. е. без какого-либо вмешательства пользователя. Никакие данные, хранящиеся в зашифрованном томе, невозможно прочитать (расшифровать) без правильного указания пароля или ключевых файлов. Полностью шифруется вся файловая система (имена файлов и папок, содержимое каждого файла, свободное место, метаданные и др.). Смонтированный том «TrueCrypt» подобен обычному логическому диску, поэтому с ним можно работать как с обычным устройством хранения информации.

Одна из примечательных возможностей «TrueCrypt» – обеспечение двух уровней правдоподобного отрицания наличия зашифрованных данных, необходимого в случае вынужденного открытия пароля пользователем. Создание скрытого тома позволяет задать второй пароль (и набор ключевых файлов) к обычному тому для доступа к данным, к которым невозможно получить доступ с основным паролем, при этом скрытый том может иметь любую файловую систему и располагается в неиспользованном пространстве основного тома.

Важной особенностью программы «TrueCrypt» является то, что она никогда не сохраняет на диске никаких данных в незашифрованном виде – такие данные временно хранятся только в 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 сбоя питания (без правильного завершения работы системы), хранящиеся в томе файлы останутся недоступными (и зашифрованными).

Алгоритм действий по созданию *обычного* тома «TrueCrypt» с созданием и использованием ключевого файла представляет собой следующую последовательность действий:

1. Запустите программу «TrueCrypt» (из папки, указанной преподавателем). Откроется главное окно программы.
2. Выберите из списка буквенное обозначение для создаваемого тома (например, **Y**). Нажмите на кнопку «Создать том» (рис. 21).

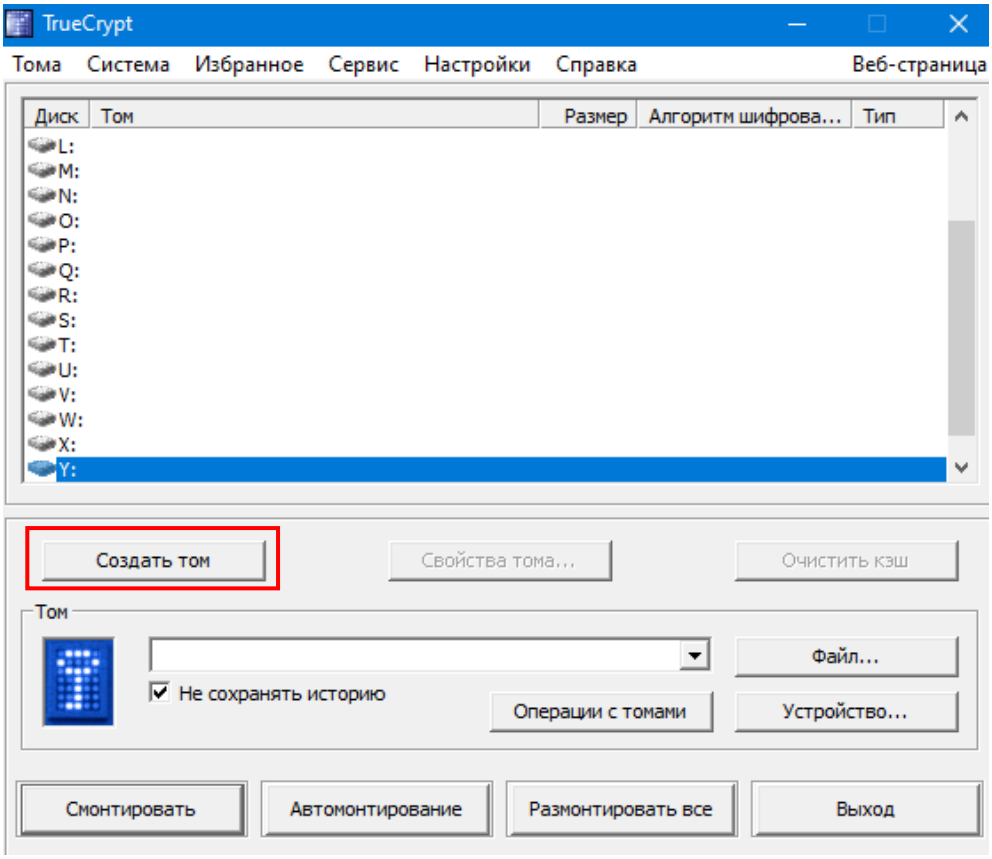

Рис. 21. Выбор буквенного обозначения зашифрованного диска

3. Укажите тип шифрования (**«Создать зашифрованный файловый контейнер»**) и нажмите кнопку «Далее» (рис. 22).
4. Укажите тип тома (**«Обычный том TrueCrypt»**) и нажмите кнопку «Далее» (рис. 23).

5. Укажите путь к физическому месторасположению зашифрованного тома и имя файла, который будет служить контейнером для зашифрованных данных (**Файл > Съемный диск D > Имя файла** (например, «*Container*»)→ **«Сохранить»**). Удостоверьтесь в том, что параметр «Не сохранять историю» включен (рис. 24).

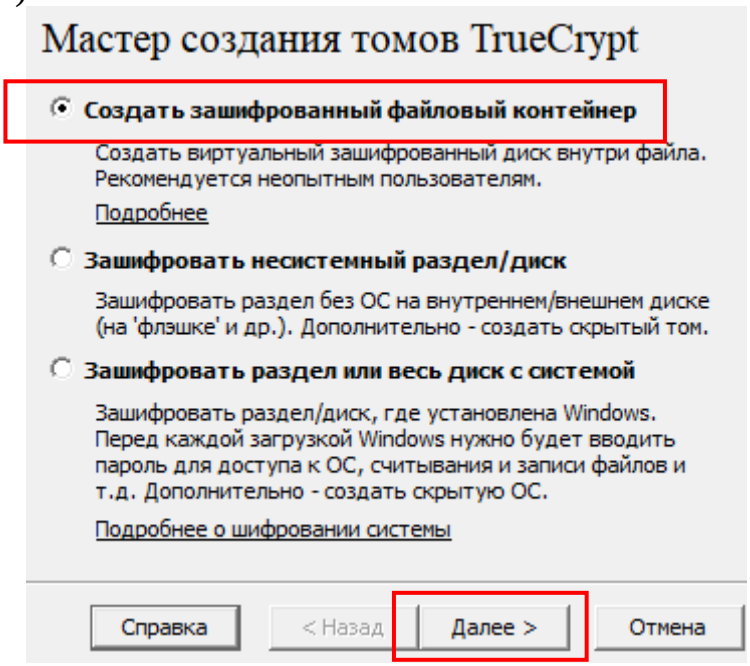

Рис. 22. Работа мастера создания томов «TrueCrypt»

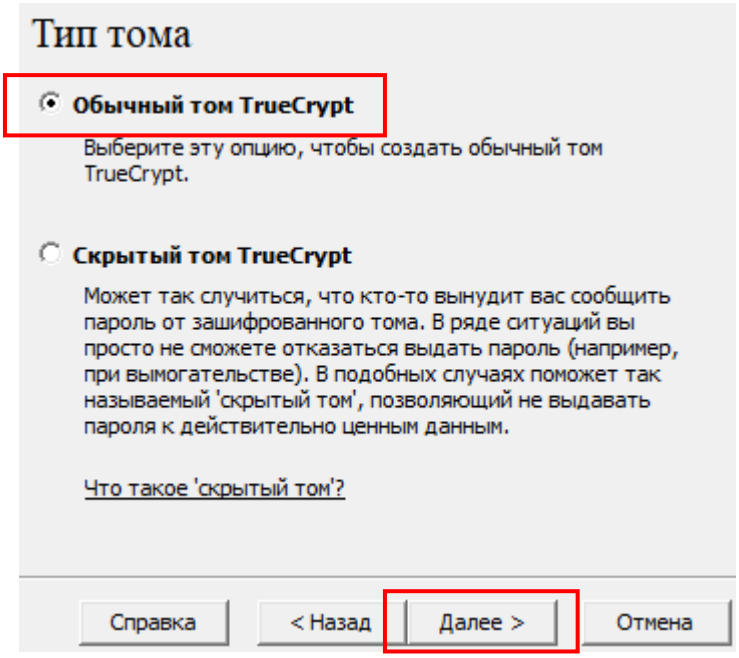

Рис. 23. Работа мастера создания томов «TrueCrypt»

6. Выберите алгоритм шифрования (**«AES»**), алгоритм хеширования (**«SHA-512»**) и нажмите кнопку «Далее» (рис. 25).

7. Выберите размер тома (например, **100 Мб**) и нажмите кнопку «Далее» (рис. 26).

8. Задайте и подтвердите пароль для доступа к зашифрованному диску (рис. 27)

Примечание: очень важно выбрать хороший пароль. Избегайте указывать пароли из одного или нескольких слов, которые можно найти в словаре (или комбинаций из 2,3 или 4 таких слов). Пароль не должен содержать имён или дат рождения. Он должен быть труден для угадывания. Хороший пароль – случайная комбинация прописных и строчных букв, цифр и особых символов (@ ^ = $ * + & # ! [ ]) и т. д. Рекомендуется выбирать пароли, состоящие более чем из 12 символов (чем длиннее, тем лучше). Максимальная длина пароля: 64 символа.

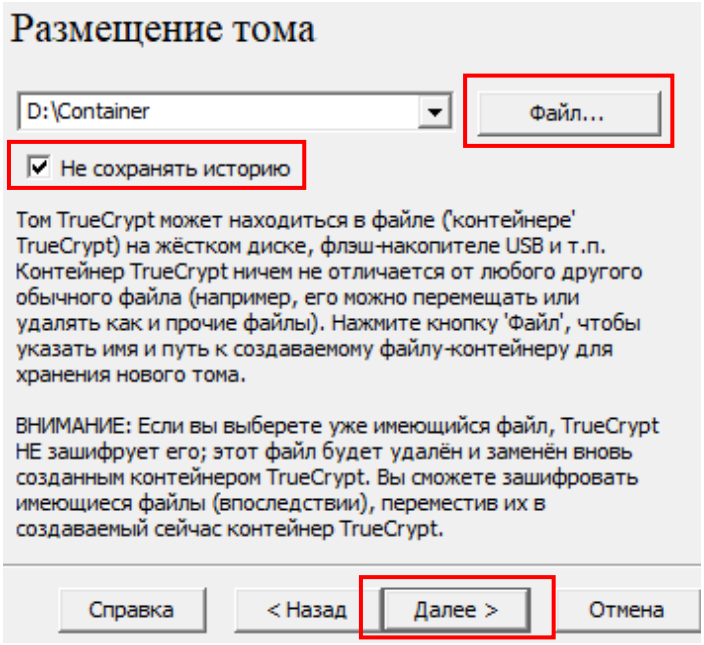

Рис. 24. Работа мастера создания томов «TrueCrypt»

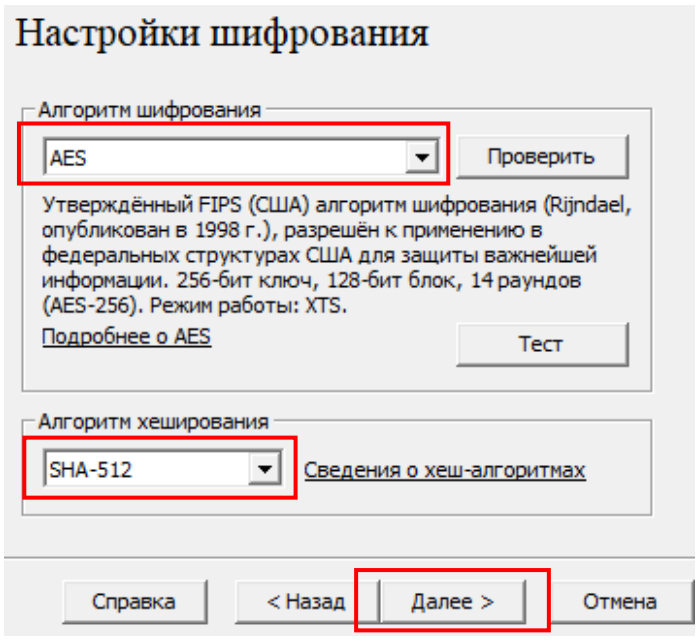

Рис. 25. Работа мастера создания томов «TrueCrypt»

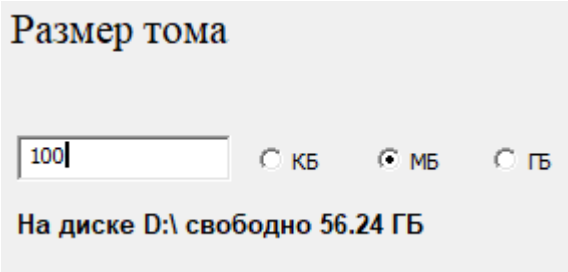

Рис. 26. Работа мастера создания томов «TrueCrypt»

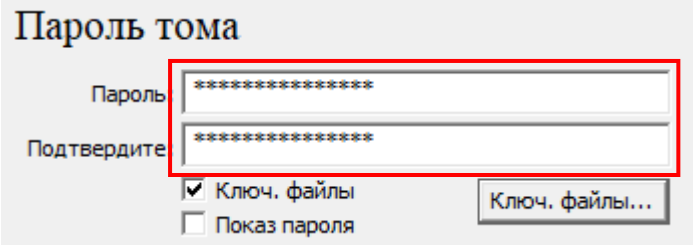

Рис. 27. Работа мастера создания томов «TrueCrypt»

9. Включите параметр «Ключ. файлы», а затем нажмите на кнопку «Ключ. Файлы». Откроется диалоговое окно выбора либо создания ключевого файла (рис. 28).

Примечание: «TrueCrypt» никогда не модифицирует содержимое ключевых файлов. Таким образом, можно использовать любое количество файлов произвольного форма (например, *.mp3, *.avi, *.doc и пр.) в качестве ключевых файлов TrueCrypt. При этом никакое инспектирование этих файлов не сможет выявить, что они используются в качестве ключевых.

Разрешается выбирать более одного ключевого файла; их последовательность значения не имеет.

10. Для того, чтобы создать ключевой файл средствами «TrueCrypt», нажмите на кнопку «Случайный ключевой файл». Откроется окно генератора ключевых файлов (рис. 29).

11. В течение некоторого времени (от 10 секунд до 1 минуты) хаотично перемещайте мышь внутри окна генератора ключевых файлов. После этого нажмите на кнопку «Создать и сохранить файл». Укажите имя и место сохранения созданного ключевого файла (например, **D:\мой ключевой файл**). Закройте окно генератора ключевых файлов.

12. В диалоговом окне «Ключевые файлы» нажмите на кнопку «Файлы…» и укажите местоположения используемого ключевого файлы (например, **D:\мой ключевой файл**). Информация о ключевом файле создаваемого тома «TrueCrypt» появится в диалоговом окне (рис. 30).

13. Для продолжения нажмите на кнопку «Ок». В диалоговом окне «Мастер создания томов TrueCrypt» нажмите на кнопку «Далее». При этом, если вы задали недостаточно длинный пароль, программа выдаст соответствующее предупреждение (рис. 31).

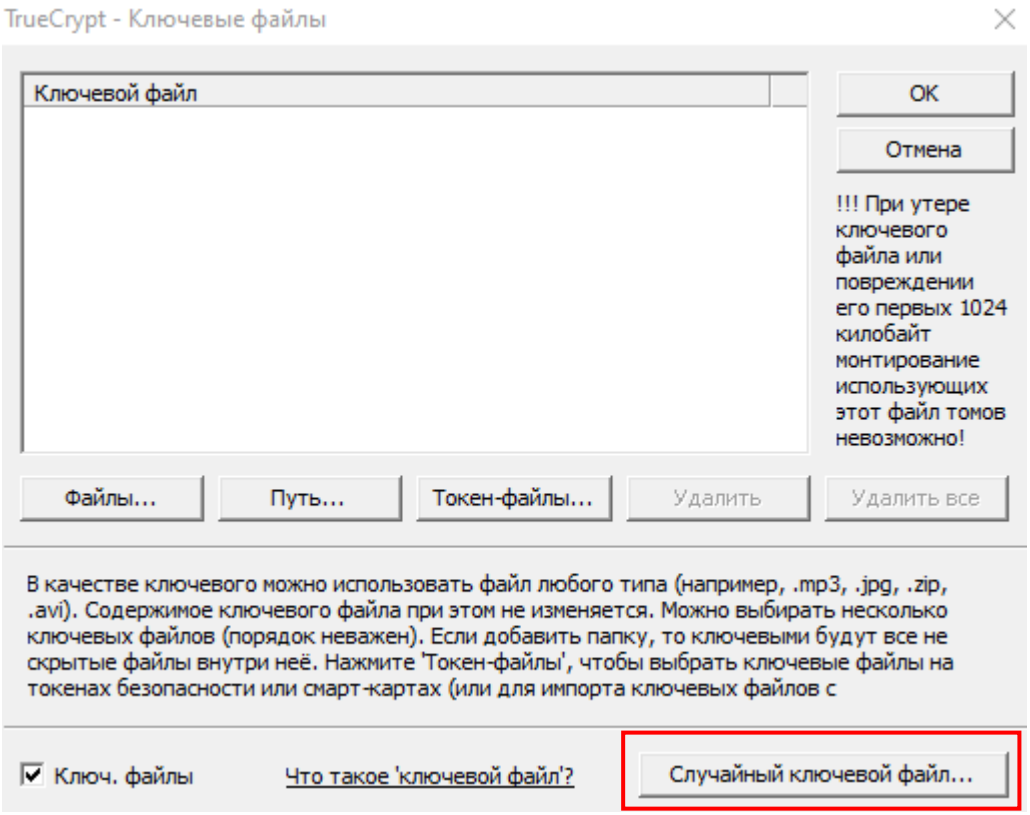

Рис. 28. Работа мастера создания томов «TrueCrypt»

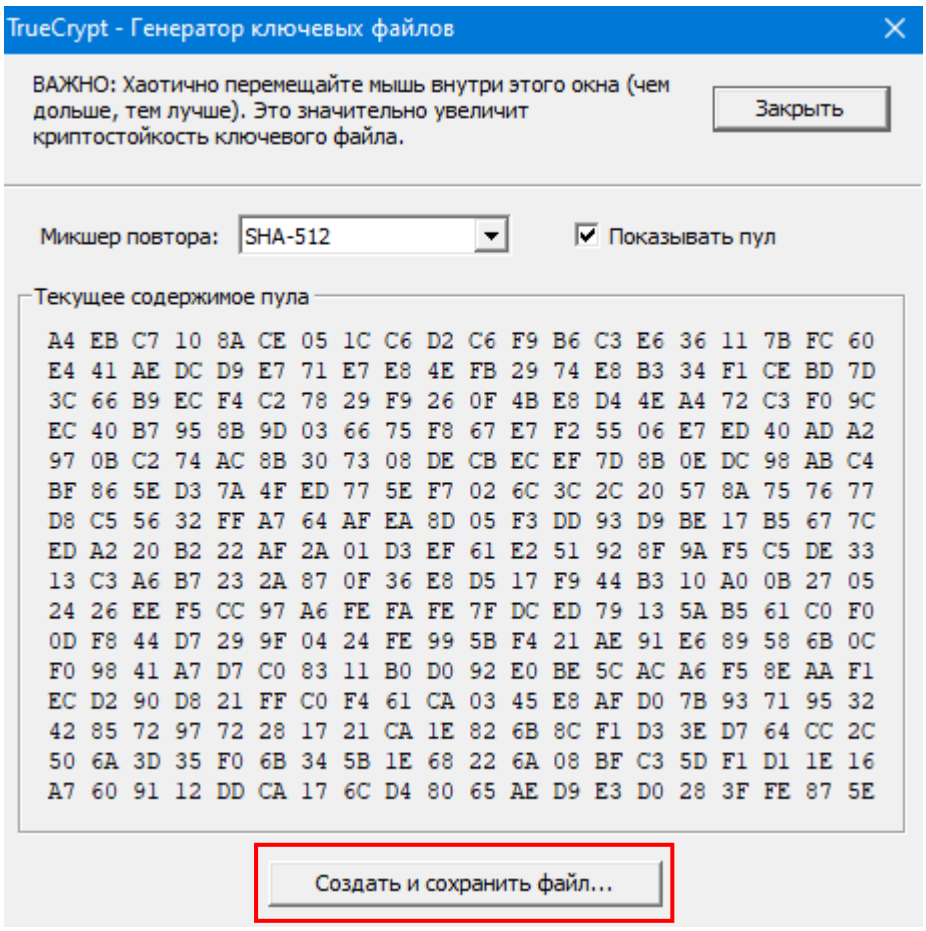

Рис. 29. Работа мастера создания томов «TrueCrypt»

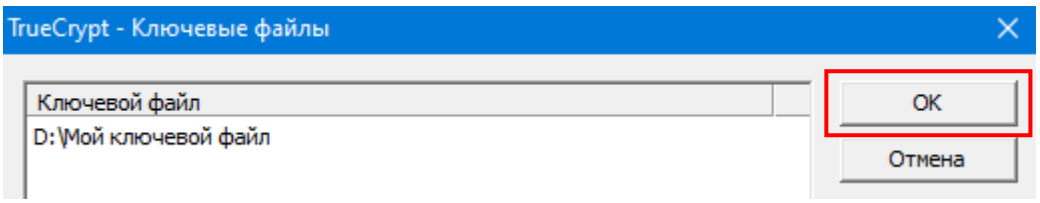

Рис. 30. Работа мастера создания томов «TrueCrypt»

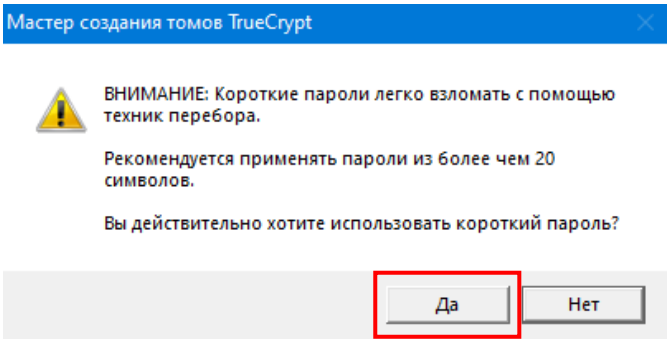

Рис. 31. Работа мастера создания томов «TrueCrypt»

14. Установите следующие опции форматирования тома: файловая система – **FAT** (*для томов размером не более 4 Гб, в противном случае том следует форматировать в формате NTFS*), размер кластера – **по умолчанию** (рис. 32). Затем в течение некоторого времени хаотично перемещайте мышь внутри окна «Форматирование тома», а затем нажмите кнопку «Разметить».

15. После успешного создания и форматирования тома (рис. 33), откроется логический диск под буквенным обозначением **Y**.

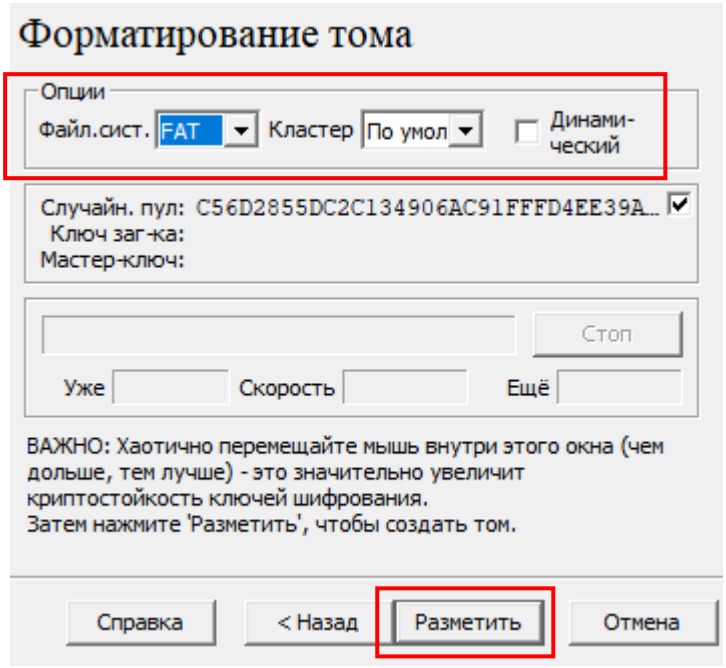

Рис. 32. Работа мастера создания томов «TrueCrypt»

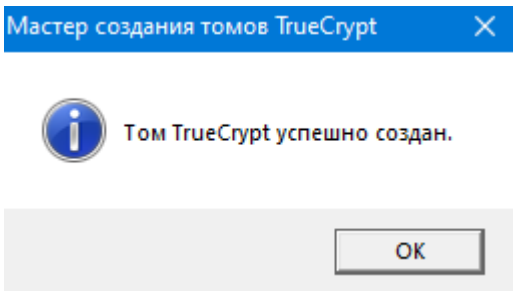

Рис. 33. Работа мастера создания томов «TrueCrypt»

Алгоритм действий по созданию *скрытого* тома «TrueCrypt» отличается от предыдущего набора операций лишь незначительно. Для того, 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».

Примечание: принцип скрытого тома состоит 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, так как свободное место в любом томе «TrueCrypt» всегда заполняется случайными данными при создании тома, и никакую часть (не смонтированного) скрытого тома нельзя отличить от случайных данных. При этом «TrueCrypt» никак не модифицирует файловую систему (информацию о свободном месте и т. д.) внутри внешнего тома.

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.

Алгоритм действий по монтированию (использованию) созданных томов (в том числе и скрытых) «TrueCrypt» представляет собой следующую последовательность действий:

1. Запустите программу «TrueCrypt». Откроется главное окно программы.
2. Выберите из списка буквенное обозначение для зашифрованного тома (например, **Y**). После чего нажмите на кнопку «Файл» и укажите местоположения созданного тома (криптоконтейнера).
3. В открывшемся окне введите пароль и (при необходимости) укажите местоположения ключевого файла (файлов).
4. В случае успешного выполнения вышеперечисленных действий откроется логический диск под буквенным обозначением **Y**.

Примечание: скрытый том монтируется так же, как и обычный том «TrueCrypt»: в главном окне программы нажмите кнопку «Файл», укажите местоположение тома (важно: убедитесь, что этот том не смонтирован). Затем нажмите кнопку «Смонтировать» и введите пароль и (при необходимости) ключевой файл (файлы) для скрытого тома.

Какой том будет смонтирован – скрытый или внешний – определяется только указанным паролем (и ключевым файлом, если таковой имеется). Это означает то, что если введён пароль для внешнего тома, то будет смонтирован внешний том, а если указать пароль для скрытого, то смонтируется скрытый том.

Рассмотрим особенности настройки программы «TrueCrypt», необходимые для ее безопасного функционирования.

Для доступа к основным параметрам настройки в главном окне программы выберите пункт меню **«Настройки» > «Параметры»**.

Откроется соответствующее диалоговое окно (рис. 34).

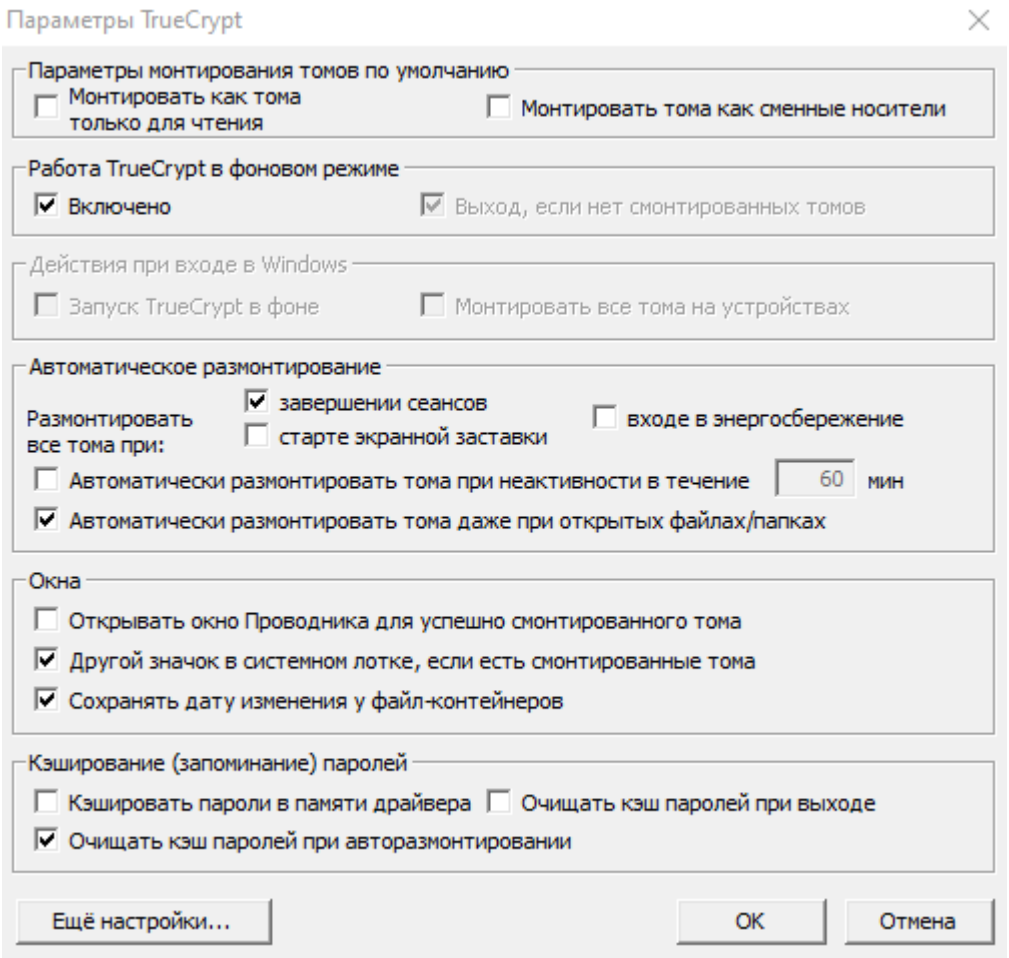

Рис. 34. Настройка основных параметров безопасности «TrueCrypt»

Нажав на кнопку «Еще настройки», откроется еще одно окно программы с доступом к дополнительным параметрам безопасности (рис. 35).

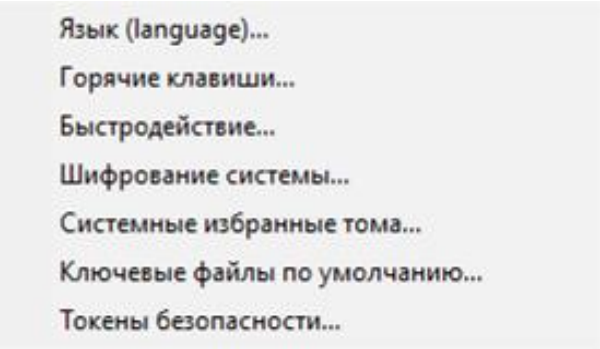

Рис. 35. Настройка дополнительных параметров безопасности «TrueCrypt»

Для того, чтобы том (криптоконтейнер) автоматически монтировался на конкретную (заранее заданную) букву диска, либо автоматически монтировался при подключении к компьютеру устройства с этим томом (например, на флэш-накопителе USB или внешнем жёстком диске, подключаемом по шине USB), данный том следует сделать *избранным*.

Чтобы сконфигурировать том «TrueCrypt» как избранный, необходимо выполнить следующую последовательность действий:

1. Смонтировать том (на ту букву диска, на которую вы хотите его монтировать всегда).
2. В главном окне «TrueCrypt» правой клавишей мыши кликнуть по смонтированному тому и выбрать команду «Добавить в избранные».
3. В появившемся окне упорядочивания избранных томов настроить необходимые параметры для этого тома и нажать на кнопку «Ок».

Для настройки общесистемных «горячих» клавиш[4] в программе «TrueCrypt» предусмотрены соответствующие настройки в меню **«Настройки» > «Горячие клавиши»** (рис. 36).

Примечание: «горячие» клавиши работают только когда «TrueCrypt» запущен или работает в фоновом режиме.

Чтобы изменить пароль тома «TrueCrypt», нажмите кнопку «Файл» в главном окне программы, укажите местоположение криптоконтейнера, выполните команду **«Тома» > «Изменить пароль тома»**.

Для того, чтобы очистить историю использования (открытия) криптоконтейнеров, выполните команду **«Сервис» > «Очистить историю томов»**. Данная команда очищает список с именами файлов (если использовались тома на основе файлов) и путями последних двадцати успешно смонтированных томов.

Полный перечень рекомендуемых настроек программы «TrueCrypt» представлен в официальном руководстве пользователя (www.truecrypt.org).

[4] «Горячие» клавиши – сочетания клавиш на клавиатуре, которым назначены (запрограммированы) определенные действия – команды (операции), исполняемые системой. «Горячие» клавиши особенно широко используются в случаях, в которых важна скорость выполнения операции либо получения определенного результата.

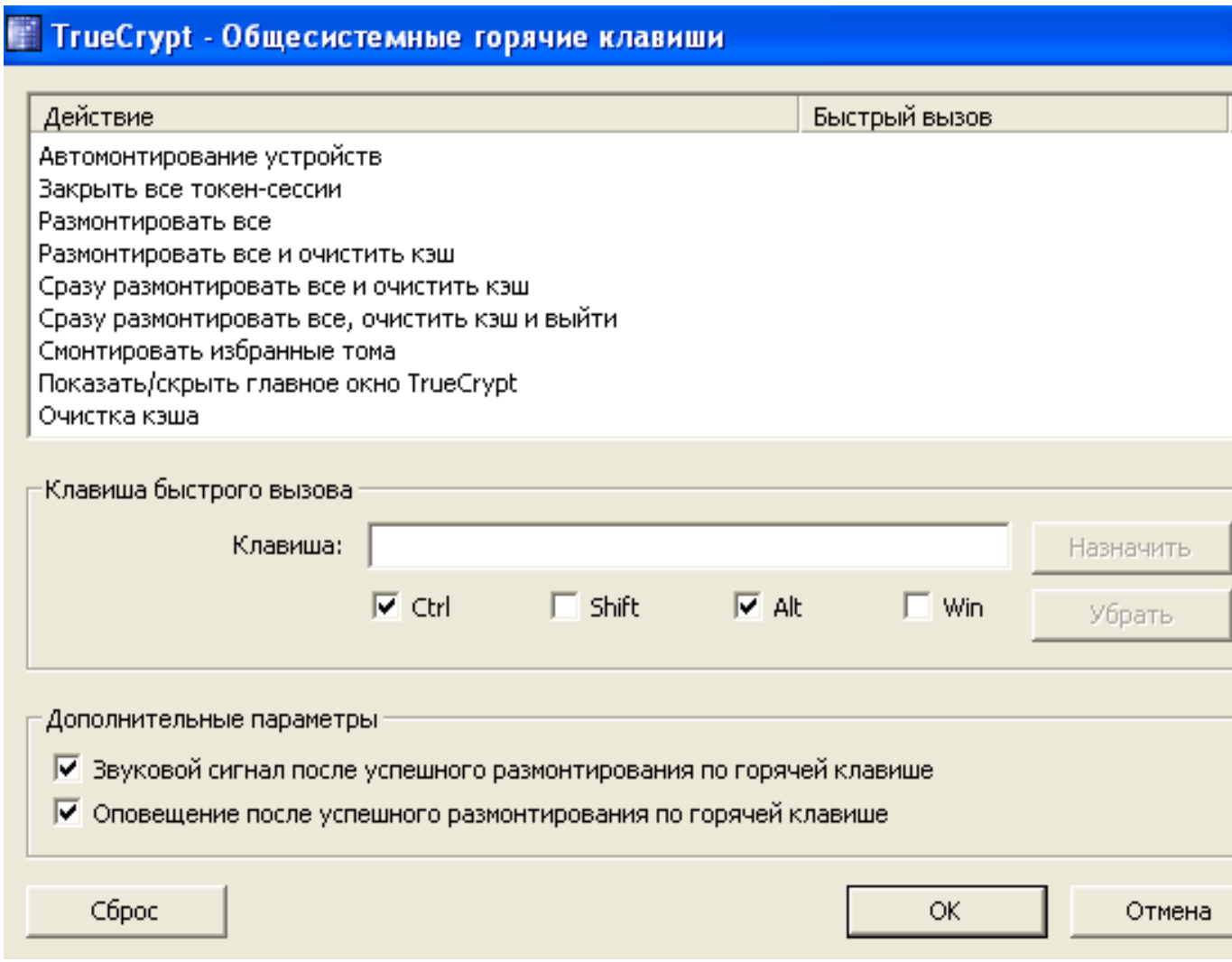

Рис. 36. Настройка общесистемных «горячих» клавиш программы «TrueCrypt»

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ:

1. Создайте в папке «C:\Documents and Settings\All Users\Документы» зашифрованный двухуровневый файловый криптоконтейнер «TrueCrypt» со следующими параметрами:

буквенное обозначение – **L** (сконфигурируйте как ***избранный***);

алгоритм шифрования – «**Twofish**»;

алгоритм хеширования – «**SHA-512**»;

имя файла криптоконтейнера – *Case 1*;

размер внешнего тома – **250 Мб**, файловая система – **FAT**;

размер скрытого тома – **50 Мб**, файловая система – **FAT**;

наличие двух отдельных ключевых файлов для каждого из томов: 1) файл, созданный генератором программы – для внешнего тома; 2) самостоятельно подготовленный либо найденный файл произвольного формата (например, *.wav) – для скрытого тома;

пароли к каждому из томов криптоконтейнера должны удовлетворять необходимым требованиям безопасности (зафиксируйте их в файл-отчете);

автоматическое размонтирование томов криптоконтейнера при неактивности в течение 5 минут.

2. Заполните каждый из томов криптоконтейнера *Case 1* произвольными файлами.

3. Назначьте комбинации клавиш для монтирования/размонтирования разделов (в том числе и быстрого размонтирования со стиранием ключа в памяти, закрытием окна и очисткой истории), отображения и сокрытия окна (и значка) «TrueCrypt». Опишите их в файл-отчете.

4. Размонтируйте созданный в п.1 задания криптоконтейнер *Case 1* и скопируйте его в новую папку под именем *Case 2*.

5. Измените пароль от внешнего тома криптоконтейнера *Case 2*. Последовательность действий зафиксируйте в файл-отчете.

6. Поменяйте ключевой файл от внешнего тома криптоконтейнера *Case 2* на файл, созданный генератором программы «TrueCrypt». Последовательность действий зафиксируйте в файл-отчете.

7. Решите следующие практические задачи[*]:

7.1. Задача №1. Большинство операционных систем (включая Windows) настроено таким образом, что при возникновении ошибки (сбоя системы, «синего экрана») выполняется 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. Это связано с тем, 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 необходимо учитывать, что когда смонтирован том «TrueCrypt», его мастер-ключ хранится незашифрованным в ОЗУ.

ВОПРОС: Какие действия необходимо предпринять, чтобы избежать утечки информации в вышеуказанных условиях?

Выполните решение задачи и оформите его в файл-отчете.

7.2. Задача №2. Когда компьютер переходит в состояние гибернации (или входит в режим энергосбережения), содержимое его ОЗУ записывается в так называемый файл гибернации на жёстком диске. В ряде случаев «TrueCrypt» не может надёжно препятствовать сохранению в файле гибернации в незашифрованном виде содержимого конфиденциальных файлов, открытых в ОЗУ. Когда вы открываете хранящийся в томе «TrueCrypt» файл, например, в текстовом редакторе, содержимое этого файла в незашифрованном виде

[*] *Задание повышенной сложности (возможно выполнение за дополнительную оценку)*

помещается в ОЗУ (и может оставаться в ОЗУ незашифрованным, пока не будет выключен компьютер).

ВОПРОС: Какие действия необходимо предпринять, чтобы избежать утечки информации в вышеприведенной ситуации?

Выполните решение задачи и оформите его в файл-отчете.

8. Контрольный тест:

Выделите правильные варианты ответа для следующего утверждения:

№ п/п	**TrueCrypt – это компьютерная программа, в чьи основные цели входят:**	**Вариант ответа** (да/нет)
1.	Гарантия выбора пользователями криптостойких паролей и ключевых файлов	
2.	Защита данных в компьютере, если атакующий имеет привилегии администратора в среде операционной системы, установленной в этом компьютере	
3.	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)	
4.	Защита данных в компьютере, если у атакующего был к нему физический доступ до или во время работы «TrueCrypt»	
5.	Защита данных в компьютере, если у атакующего есть физический доступ к нему между временем завершения работы «TrueCrypt» и временем, необходимым для безвозвратного стирания всей информации, её перезаписи другими данными или утраты из модулей временной памяти, подключённых к компьютеру (включая модули памяти в периферийных устройствах)	
6.	Защита данных в компьютере, содержащем какое-либо вредоносное ПО (например, вирус, «троянского коня», шпионскую программу) или любую часть ПО (включая «TrueCrypt» или компонент ОС), которая была изменена, создана или может быть подконтрольна атакующему	
7.	Защита данных путём их шифрования перед записью на диск	
8.	Защита любого аппаратного компонента компьютера или всего компьютера	
9.	Предотвращение анализа трафика при передаче зашифрованных данных по сети	
10.	Расшифровка зашифрованных данных после их считывания с диска	
11.	Сохранение/контроль целостности или аутентичности зашифрованных и расшифрованных данных	
12.	Шифрование или защита любой области ОЗУ (оперативной памяти ПК)	

Результаты выполнения теста оформите в файл-отчете

9. Продемонстрируйте работу и файл-отчет преподавателю.

10. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, в том числе зашифрованные; установите первоначальные настройки использованного программного обеспечения.

11. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какие типы шифрования предоставляет программа «TrueCrypt»?
2. Что означает двухуровневая защита смонтированного с помощью «TrueCrypt» тома?
3. Какие алгоритмы шифрования использует программа «TrueCrypt»? Дайте их сравнительный анализ.
4. Какие действия следует предпринять, чтобы криптоконтейнер автоматически монтировался на конкретную (заранее заданную) букву диска, либо автоматически монтировался при подключении к компьютеру устройства с этим томом (например, на флэш-накопителе USB или внешнем жёстком диске, подключаемом по шине USB)?
5. Перечислите возможные каналы утечки информации при использовании программы «TrueCrypt». Сформулируйте перечень действий по их нейтрализации (минимизации).