МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2017 г.

ШИФРОВАНИЕ С ПОМОЩЬЮ ПРОГРАММЫ TRUECRYPT

Методические указания по выполнению лабораторных работ по дисциплинам «Методы и средства защиты компьютерной информации», для студентов направления подготовки бакалавров 09.03.04, «Информационная безопасность» для студентов направлений подготовки бакалавров 09.03.02, 09.03.03, 45.03.03.

Курск 2017

УДК 004.056.55(076.5)

Составитель: К.А. Тезик

Рецензент

Кандидат технических наук, доцент *Т. И. Лапина*

Шифрование с помощью программы TrueCrypt: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: К. А. Тезик, Курск, 2017. 20 с.: ил. 10, Библиогр.: с. 20.

Содержат краткие теоретические положения о шифровании информации и созданию скрытых томов с помощью программы TrueCrypt.

Методические указания соответствуют требованиям программы по направлению подготовки бакалавров: программная инженерия, информационные системы и технологии, прикладная информатика, фундаментальная и прикладная лингвистика.

Предназначены для студентов направления подготовки бакалавров 09.03.02, 09.03.03, 09.03.04, 45.03.03 дневной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать 24.10 Формат 60x84 1/16.
Усл. печ. л. 1,0 . Уч. – изд. л. 0,9 .Тираж 100 экз. Заказ. 1814 Бесплатно.
Юго - Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Лабораторная работа

Шифрование с помощью программы TrueCrypt

Введение

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделать их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: гарантию конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных. Основой большинства криптографических средств защиты информации является шифрование данных.

Кратко рассмотрим некоторые примеры программных средств криптографической защиты. Пакет «КРИПТОН Подпись» предназначен для использования инфраструктуры электронной цифровой подписи (ЭЦП) электронных документов. Система криптографической защиты информации «Верба-О» решает следующие задачи:

- шифрование/расшифрование информации на уровне файлов;
- генерация электронной подписи (ЭЦП);
- проверка ЭЦП;
- обнаружение искажений, вносимых злоумышленниками или вирусами в защищаемую информацию.

Комплекс «Inter-PRO» предназначен для криптографической защиты информационных систем, построенных на базе Web-технологий. Наиболее эффективно применение «Inter-PRO» в электронных платежных системах типа «Банк-Клиент», базирующихся на Web-технологиях и ориентированных на дистанционное обслуживание клиентов через Интернет, или в системах, где необходимо авторизованное подтверждение запроса клиента на обслуживание (в системах электронной торговли, электронного страхования,

платного информационного обслуживания.) Библиотека криптографических преобразований «Message-PRO» и одноименный исполняемый модуль предназначены разработчикам приложений и систем защищенного электронного документооборота, требующих высокого уровня безопасности. Основные характеристики «Message-PRO»:

- соответствие требованиям Федерального закона РФ № 1-ФЗ от 10.01.2002 г. «Об электронной цифровой подписи»;
- поддержка российских и зарубежных криптографических алгоритмов: ГОСТ Р34.10-94, ГОСТ Р34.10-2001, RSA, ГОСТ Р34.10-94, SHA-1, MD5, ГОСТ 28147-89;
- возможность формирования нескольких ЭЦП под одним документом;
- наличие процедуры генерации ключей;
- возможность хранения ключевой информации на различных носителях, включая USB Flash Hard Drive, eToken и Touch Memory;
- использование сертифицированного ФАПСИ программного датчика случайных чисел (ДСЧ);
- функционирование в операционных средах Windows, Linux, FreeBSD, Solaris, SCO Open Server.

«Доверенный удостоверяющий центр» - программно-аппаратный комплекс обладает устойчивостью к сетевым атакам за счет использования доверенной сертифицированной ФАПСИ операционной системы «Атликс» на базе ОС Linux и входящего в ее состав межсетевого экрана.

«Доверенный удостоверяющий центр» использует российские криптографические алгоритмы:

- ГОСТ Р34.10-94, ГОСТ Р34.10-2001 для формирования и проверки ЭЦП;
- ГОСТ 28147-89 для шифрования и имитозащиты;
- ГОСТ Р 34.11-94 для хэширования данных.

Краткие теоретические положения

Существует множество коммерческих программ для шифрования данных, наиболее известными из которых являются BestCrypt(http://www.jetico.com) и DriveCrypt(www.securstar.com). Однако лучшей программой, по мнению многих, является программаTrueCrypt(http://truecrypt.org) Достоинством TrueCrypt является, то, что она бесплатна и является свободным программным обеспечением, т.е всем желающим доступен ее исходный код, что дает возможность специалистам по безопасности убедиться, что TrueCrypt не содержит никаких"потайных ходов". Стандартно TrueCrypt имеет английский интерфейс, но на сайте программы можно скачать языковый пакет для перевода интерфейса на многие десятки других языков, в том числе присутствует пакет для русского языка.

Установка программы ничего сложно собой не представляет: запустите **TrueCrypt Setup.exe**, в появившемся окне нажмите кнопку **Install.** В конце установки программа предложит открыть инструкцию в интернете для начинающего пользователя TrueCrypt (на английском языке). Выбирайте да или нет по своему усмотрению. После установки не следует сразу запускать программу, потому что нам нужно ее ещё перевести на русский язык. Для этого необходимо извлечь из архива и скопировать языковой файл (Language.ru.xml) в каталог программы True Crypt (обычно это C:Program Files\TrueCrypt\). Теперь можно запускать программу из меню пуск или с помощью иконки на"Рабочем столе". В главном меню **Setting -> Language** надо выбрать русский язык.

Перед вами предстанет окно, показанное, на рис. 1

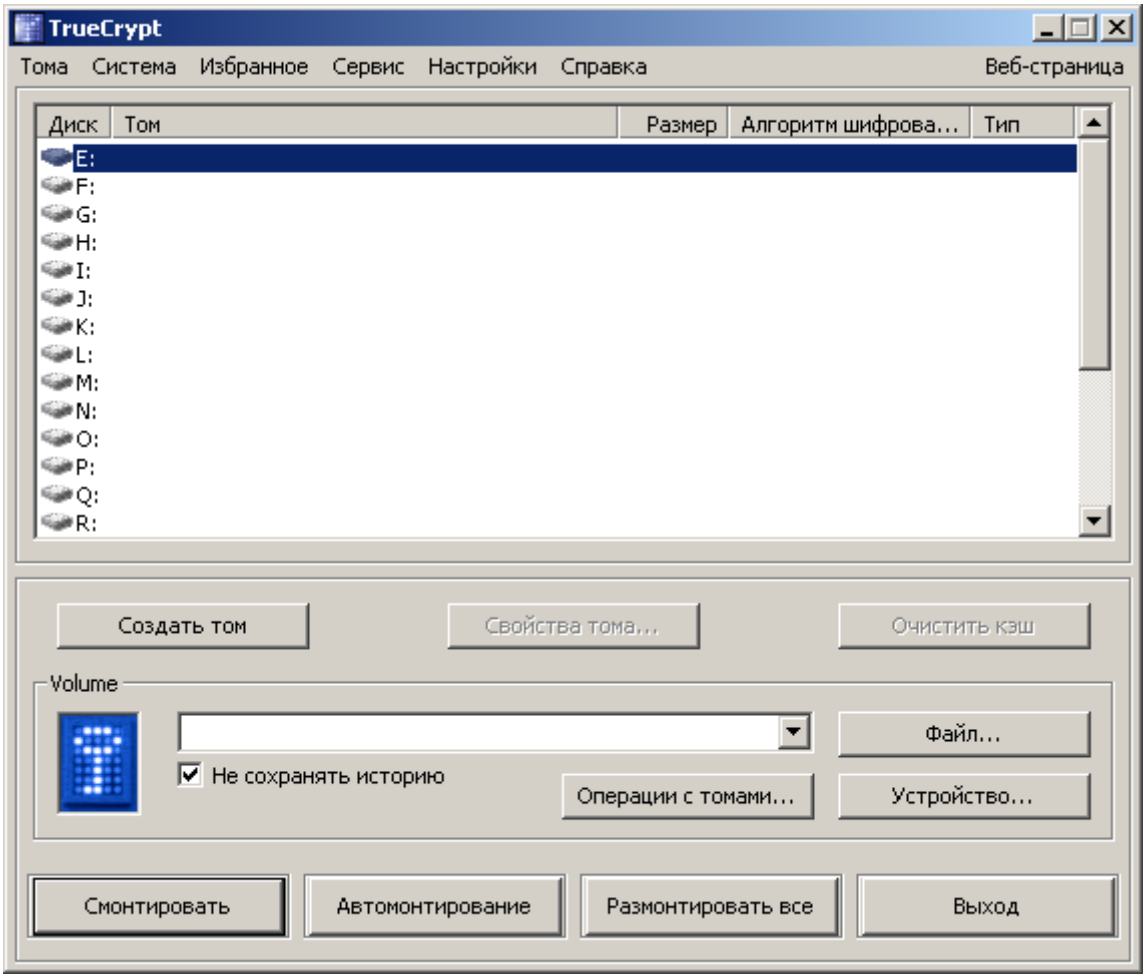

Рис. 1 Интерфейс программы TrueCrypt

Сначала мы должны создать новый том (называемый также *контейнером* или *зашифрованным хранилищем*) в котором будем хранить секретные данные. Для этого нажимаем кнопку **Создать том.**

В первом окне «Мастер создания томов TrueCrypt» (рис 2) будет предложено выбрать один из трех вариантов:

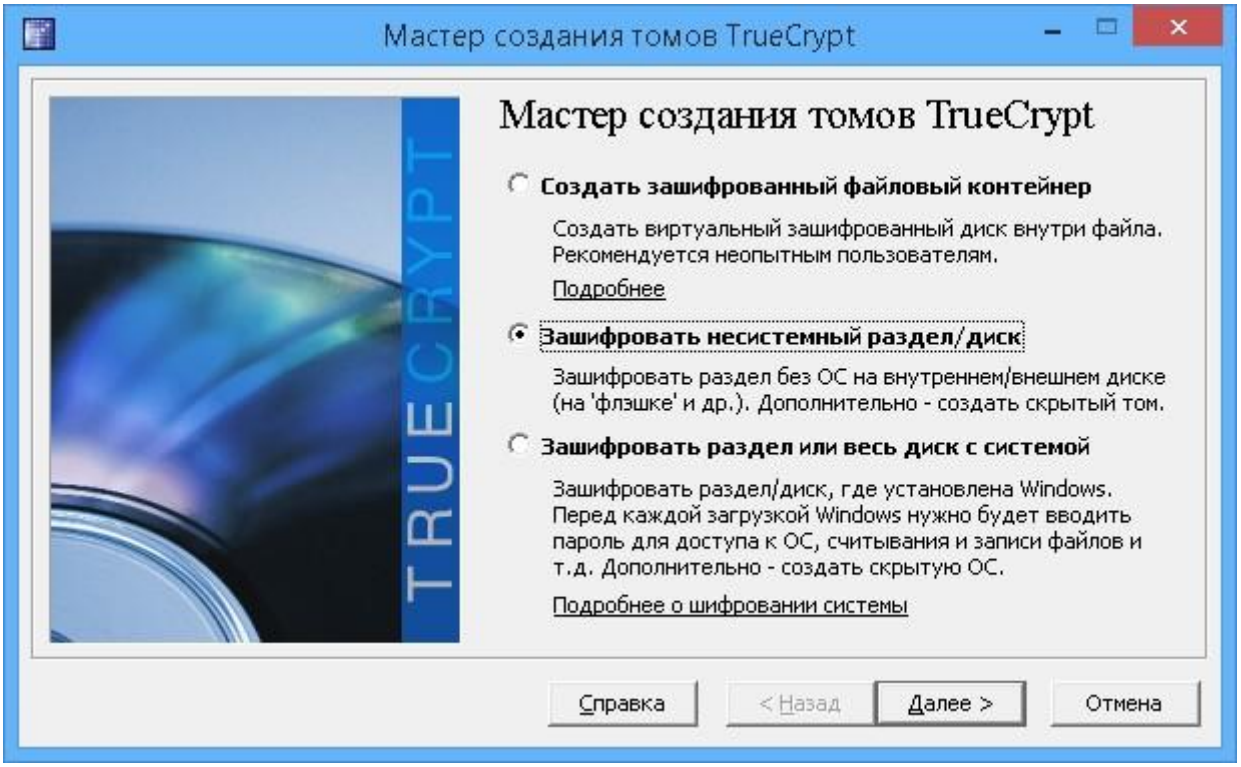

Рис. 2 Мастер создания томов

Создать файловый контейнер – будет создан виртуальный зашифрованный диск внутри любого файла. Это вариант рекомендуется неопытным пользователям.

Создать том внутри несистемного раздела/диска– под зашифрованный контейнер будет использован целиком один из разделов жесткого диска, flash–карта или другое устройство хранения данных.

Зашифровать раздел или весь диск с системой - можно полностью зашифровать диск или раздел, на котором установлена и с которого грузится Windows. Перед каждой загрузкой Windows пользователю будет нужно вводить пароль для доступа к системе.

Мы рассмотрим работу программы на примере файлового контейнера, однако создание зашифрованных разделов и дисков осуществляется аналогичным образом.

Таким образом, после выбора опции "Создать файловый контейнер" и нажатия кнопки **Далее** появится следующее окно мастера, в котором следует выбрать обычный или скрытый том, который мы будем создавать (рис.3).

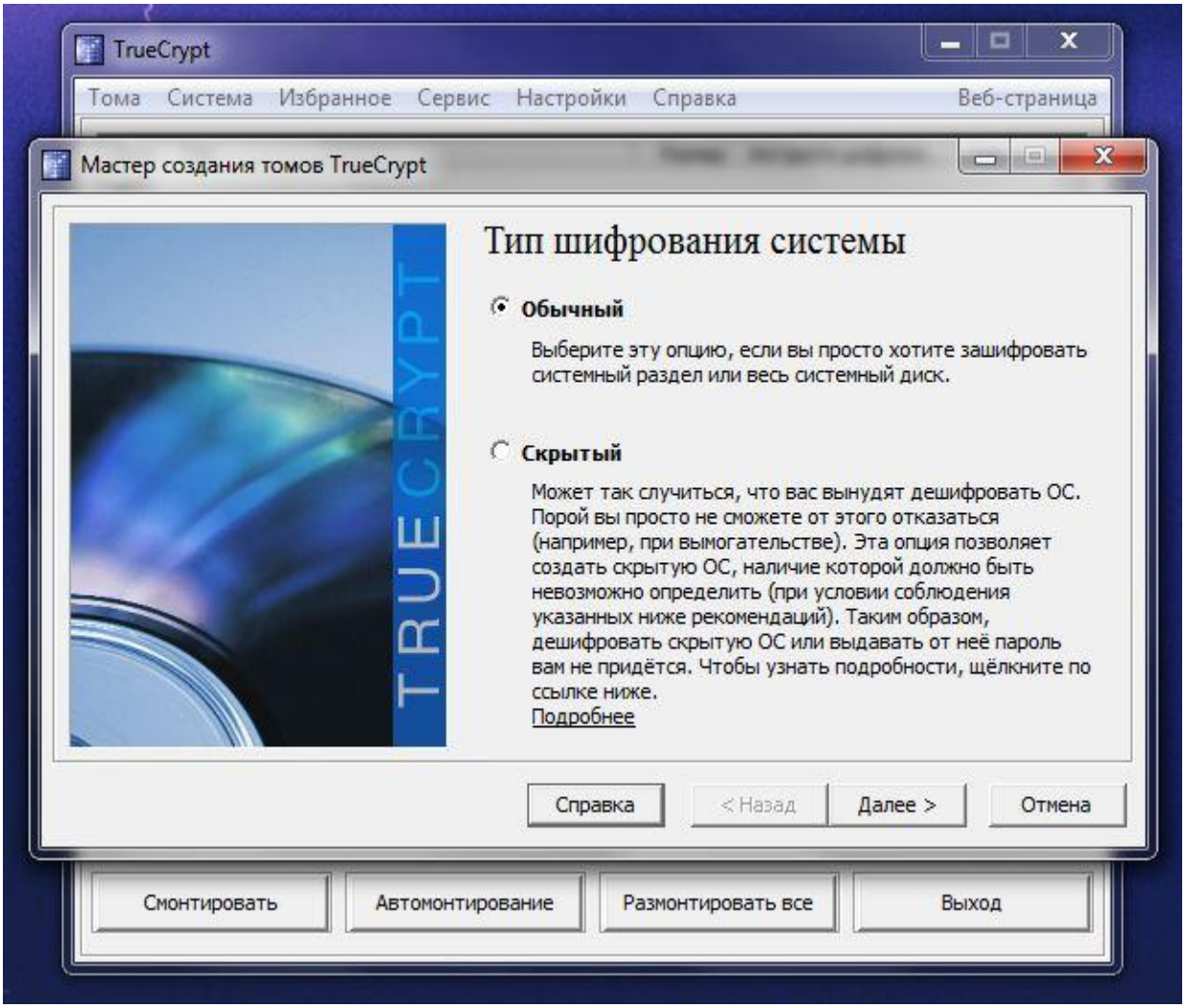

Рис. 3 Тип тома

Скрытый том - это дополнительная мера безопасности. Скрытый том всегда создается внутри обычного, доступ к скрытому тому может получить только тот, кто знает о его существовании. Даже если злоумышленник знает пароль к вашему обычному тому, то все равно он не сможет получить доступ к данным в скрытом томе. Сначала мы рассмотрим создание обычного тома, а потом работу со скрытым томом.

В третьем окне мастера нажмите кнопку **Файл,** чтобы указать имя и путь к создаваемому файлу для хранения нового тома или кнопку **Устройство**, чтобы выбрать раздел диска или накопитель для шифрования (рис. 4). Помните о том, что все находящиеся данные в выбранном файле или в выбранном разделе/устройстве будут уничтожены! Поэтому не стоит выбирать имя существующего файла, иначе TrueCrypt перепишет его своей информацией. В данном случае мы указываем имя несуществующего файла C:\mult.avi, программа TrueCrypt создаст его самостоятельно.

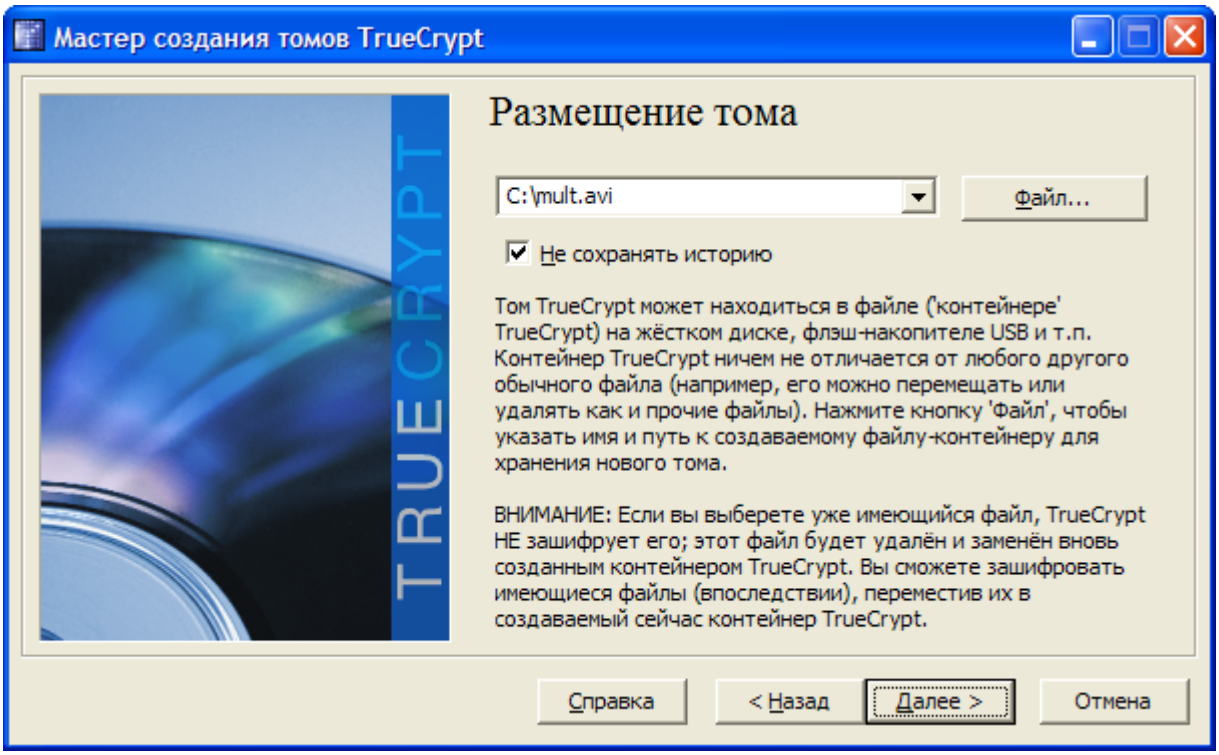

Рис. 4 Размещение тома

Вы можете указать любое название файла и любое расширение. Файл можно хранить в любом месте и на любом носителе (например, на USB-флешке).

Что означает поле "Не сохранять историю"? Можно указать, чтобы программа (в целях безопасности) не запоминала имена файлов, которые вы создавали в качестве тома. Убедимся, что в этом поле стоит галочка. Нажимаем **"Далее".**

В следующем окне (рис. 5) нужно выбрать алгоритм шифрования тома.

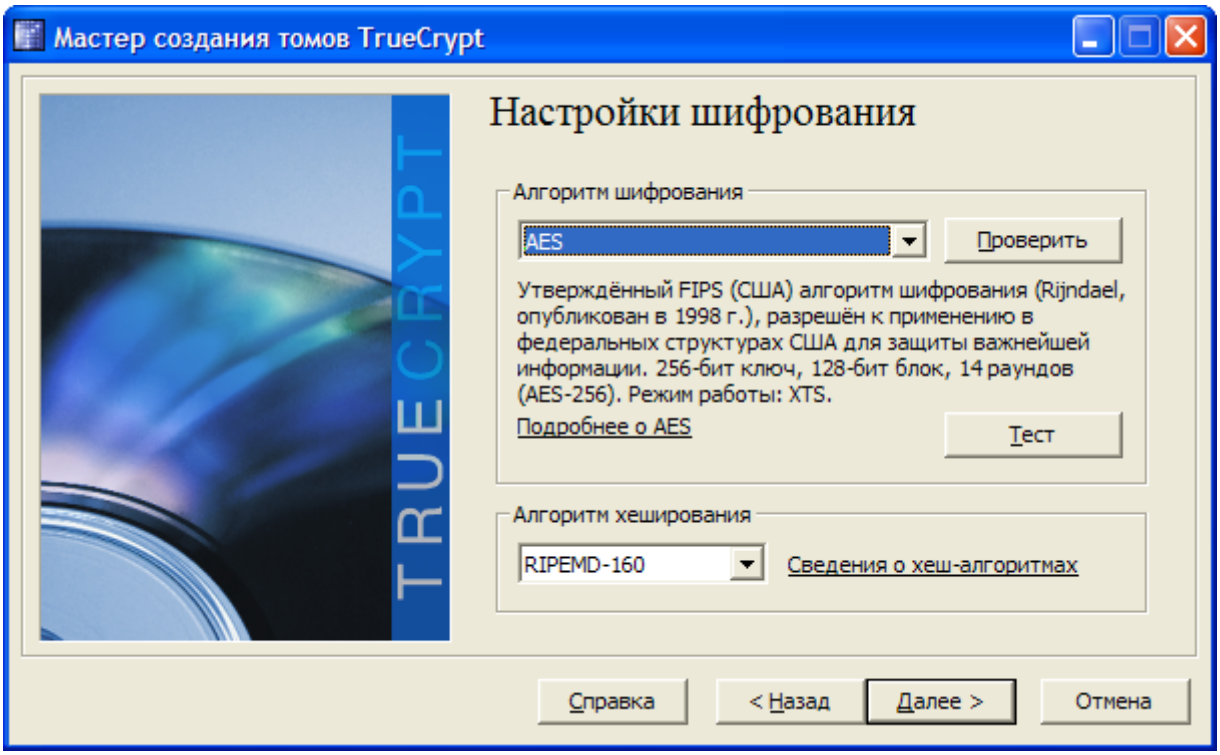

Рис. 5 Настройка шифрования

TrueCrypt предлагает несколько алгоритмов шифрования. Хэш-алгоритм нужен для того, чтобы тщательно "перемешать" наши данные и защитить их от подделки. Каждый из предложенных алгоритмов шифрования для наших целей может считаться вполне надежным. Наиболее быстрым является AES (по умолчанию), его и выберем. Нажимаем **"Далее".**

Теперь нужно указать размер нашего файла (тома) (рис.6). Размер (объем) тома определяет, сколько информации он вместит. Довольно часто резервные копии данных создаются на компакт-дисках. Есть смысл задать размер тома чуть меньше 700 Мб (чтобы он гарантированно уместился при записи на CD). Нажимаем **"Далее".**

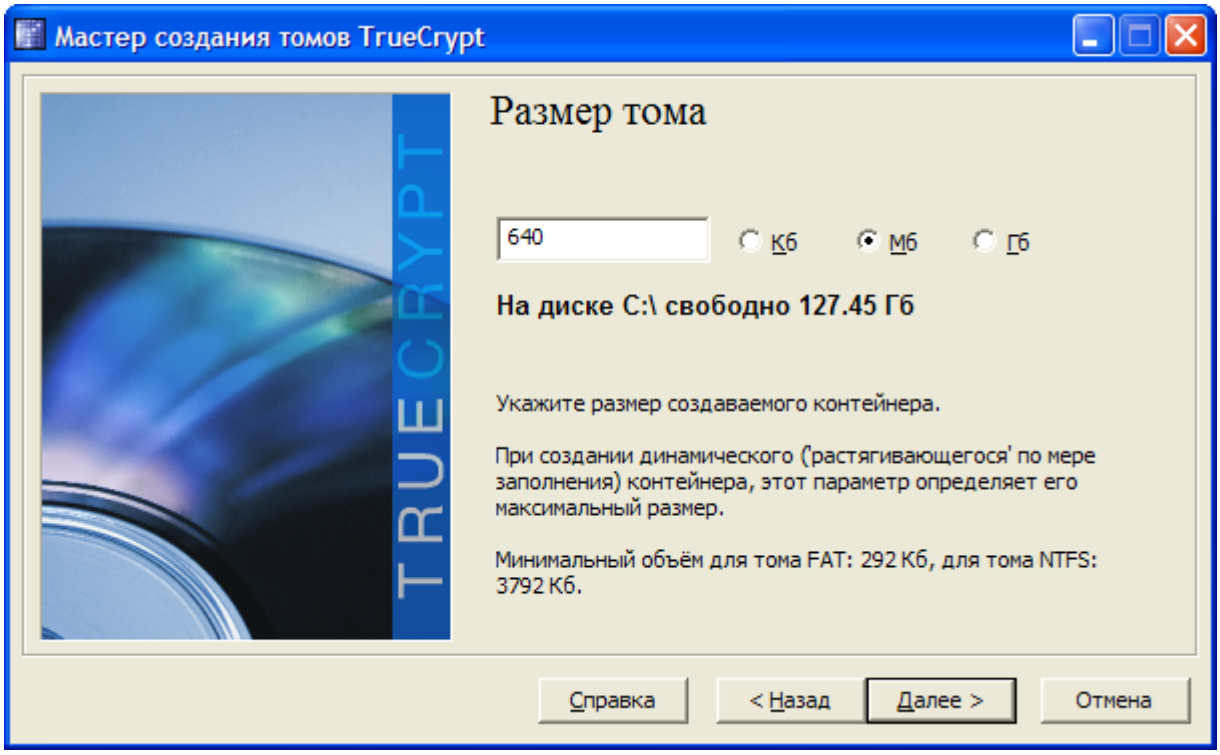

Рис. 6 Размер тома

Далее нужно выбрать пароль на доступ к тому (рис.7).

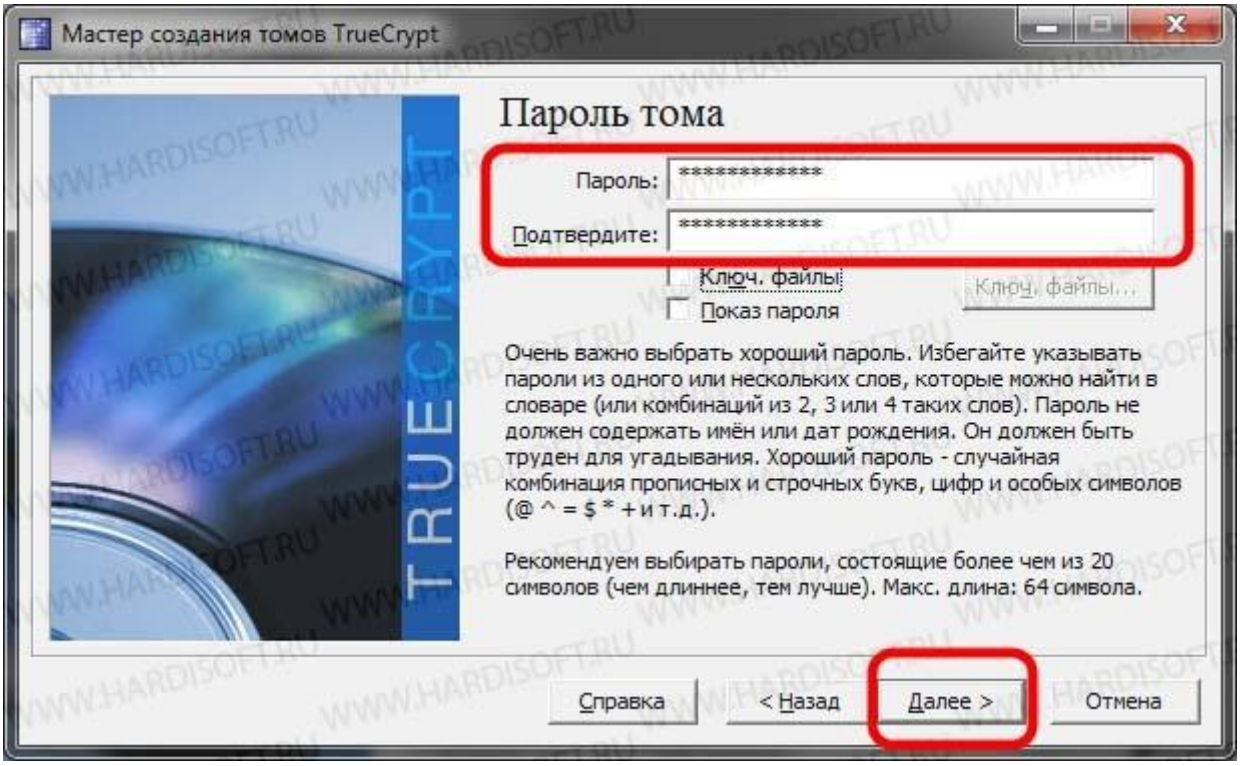

Рис. 7 Пароль тома

От его надежности зависит безопасность данных. Пароль нужно вводить всякий раз при открытии тома. Придумываем пароль, вводим его повторно (в остальных полях галочки сейчас не нужны) и нажимаем **"Далее"**.

Программа рекомендует выбирать пароль не менее чем из 20 знаков. Если ваш пароль показался недостаточно длинным, программа сообщит об этом (рис. 8). Хотите сменить пароль — можете ответить **"Нет"** и ввести новый пароль, а если хотите продолжить — **"Да"**.

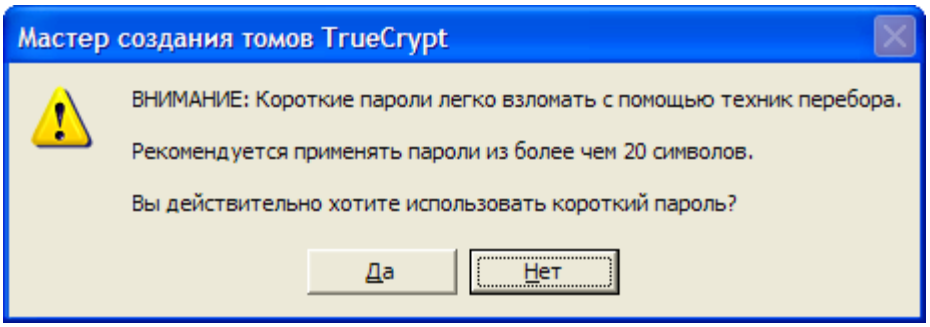

Рис. 8 Предупреждение о надёжности пароля

Далее нужно указать файловую систему, которая будет использоваться внутри тома (рис. 9). Выбор файловой системы тома не зависит от файловой системы реального диска, на котором вы создаете том. Размер кластера можете оставить **По умолчанию.**

При нажатии кнопки **Разметить** контейнер под видом обычного файла будет создан. При этом он будет отформатирован и заполнен случайными данными. Сразу после этого программы предложит создать еще один том. Если вам не нужен еще один контейнер, то нажимаем **Выход.** Созданный контейнер вы можете копировать и переносить на любых носителях, то есть поступать с ним как с самым обычным файлом.

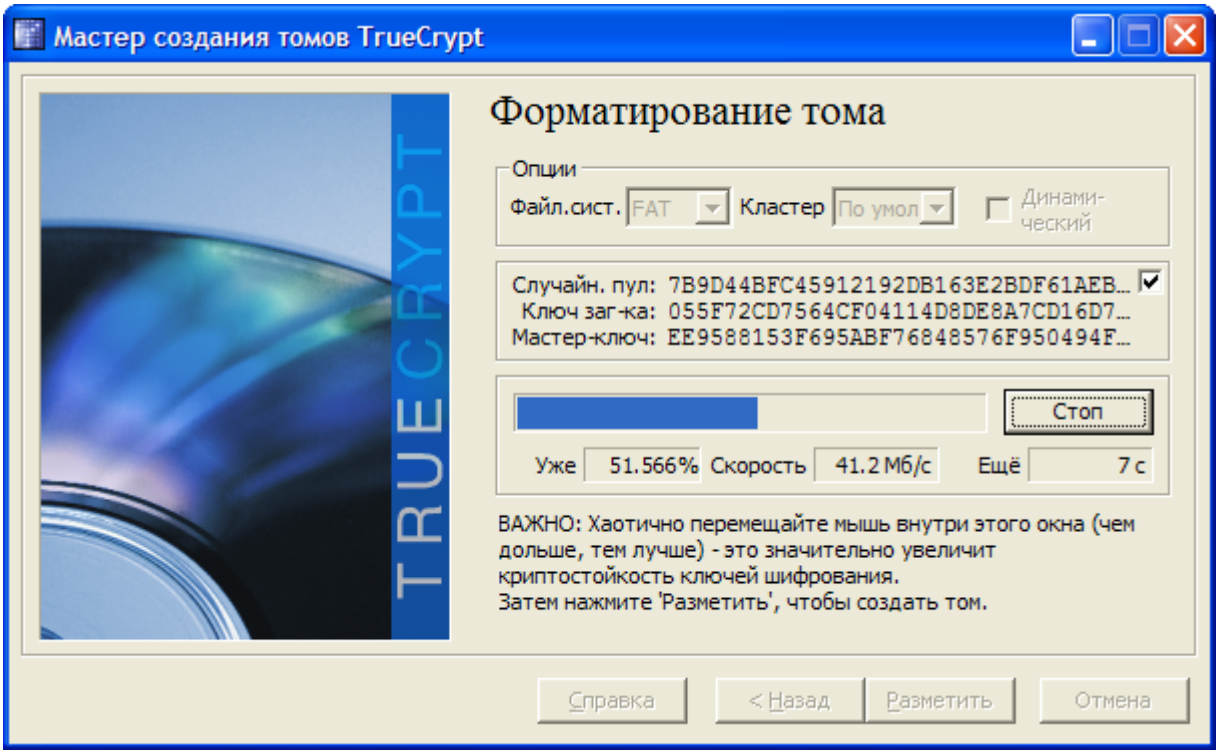

Рис. 9 Форматирование тома

А теперь посмотрим, как использовать контейнер (сохранять в него секретные данные). Для этого его сначала нужно подключить (примонтировать) к системе. В главном окне программы TrueCrypt выбираем имя будущего логического диска. Программа предлагает имена дисков, которые не используются в вашей системе. После выбора имени диска (например N) укажите том, то есть файл который мы создали, это можно сделать с помощью кнопки **Файл** и далее нажмите кнопку **Смонтировать**. После верного ввода пароля в системе появится новый диск N – это и есть примонтированный том. Теперь с ним можно работать как с обычным диском.

После того как вы переписали в контейнер все файлы, которые хотите скрыть, диск можно размонтировать (кнопка **Размонтировать** в главном окне программы). При этом его содержимое будет автоматически зашифровано. Теперь файл **mult.avi** можно копировать, переносить с компьютера на компьютер, пересылать

по почте. Вам нужна только программа TrueCrypt, чтобы контейнер можно было монтировать и работать с секретными данными.

Теперь рассмотрим, как сделать скрытый том. Скрытый том служит для дополнительной защиты данных, при этом внешний том служит лишь прикрытием, потому что все важные данные будут находиться в скрытом томе.

Чтобы создать скрытый том в окне выбора типа тома (рис. 3) выбираем “**Скрытый том TrueCrypt**”. И в следующим окне выбираем один из двух вариантов:

Прямой режим – скрытый том будет создан внутри уже имеющегося тома.

Обычный режим – будет создан обычный новый том, а внутри него скрытый том (рис. 10)

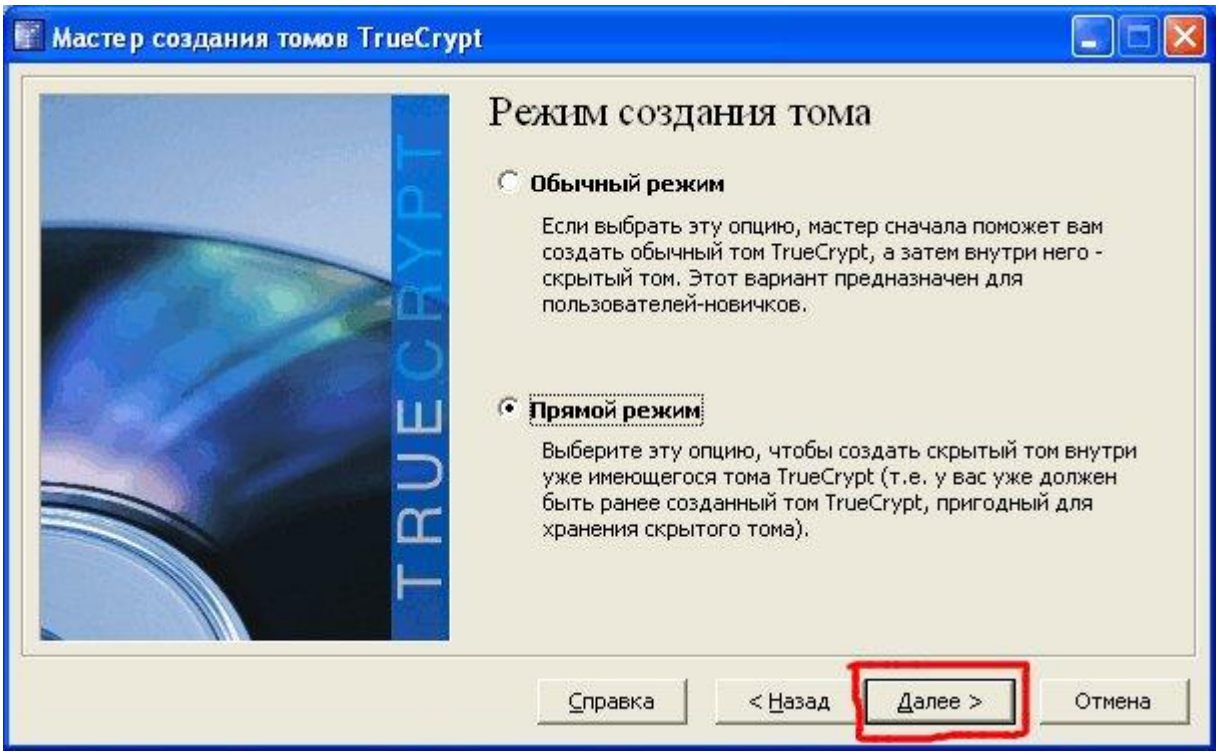

Рис. 10 Создание скрытого тома TrueCrypt.

Мы в качестве примера создадим скрытый том внутри имеющегося, поэтому выбираем опцию прямой режим. Далее указываем

наш файл и вводим пароль на доступ к этому контейнеру (он будет называться внешним или открытым томом). В следующих окнах вам нужно будет указать размер скрытого тома в пределах свободного места внешнего тома и задать пароль на доступ к скрытому тому. В качестве файловой системы для скрытого тома программа TrueCrypt позволит указывать только FAT.

Перед созданием скрытого тома вам следует переписать во внешний том какие-нибудь файлы, которые будут служить для отвлечения внимания. Но после создания скрытого тома записывать во внешний том больше ничего нельзя, иначе вы можете повредить данные, находящиеся в скрытом томе.

При монтировании контейнера у вас предварительно будет запрашиваться пароль. Если вы введете пароль на доступ к внешнему тому, то попадете во внешний том. Если вы введете пароль на доступ к скрытому тому, то попадете в скрытый том. Узнать, что в контейнере имеется скрытый том практически невозможно, потому что он при создании заполнен случайными данными и зашифрован.

Вместо пароля на доступ к тому вы можете использовать так называемый ключевой файл. Ключевой файл - это случайно сгенерированный пароль, который хранится в файле. Перед созданием тома ключевой файл следует создать с помощью меню **Ключевые файлы->Создать случайный ключевой файл**. Для указания ключевого файла вместо пароля имеются соответствующие кнопки.

Вы всегда можете изменить первоначальный пароль тома, в том числе поменять пароль на ключевой файл и наоборот. Это можно сделать с мощью кнопки **Операции** в главном окне программы.

В начале каждого тома (обычного и скрытого) содержится специальная информация, называемая заголовком тома. Если она по каким-либо причинам будет повреждена, то вы не сможете примонтировать том, а значит, все ваш данные будут утеряны (если,

конечно, вы не сделали до этого резервную копию тома). Специально на этот случай TrueCrypt предоставляет сделать резервную копию заголовка тома, которую при повреждении можно восстановить. Создание резервной копии и восстановление заголовка осуществляется с помощью кнопки **Операции** в главном окне программы или с помощью меню **Инструменты**. Обычно копию одного заголовка делают в том случае, если контейнер занимает большой объем.

Однако даже в случае удачного монтирования может оказаться поврежденной файловая система тома. Восстанавливать файловую систему можно точно также как и на обычном диске например с помощью стандартной утилиты chkdsk.exe. Можно восстанавливать и случайно удаленные файлы на томе с помощью утилит для восстановления данных. Возможно даже осуществить дефрагментацию присоединенного тома TrueCrypt.

Практическое задание

Цель работы: изучить методику создания файлового контейнера с помощью программы TrueCrypt.

Порядок выполнения работы:

1) Создайте в текстовом редакторе Word три файла text1.docx, text2.docx и text3.docx.
2) Создайте файл **mult.avi** для хранения нового тома.
3) Выберите алгоритм шифрования тома **AES** и произвольный алгоритм хеширования**.**
4) Укажите размер тома, например **50 Мб.**
5) Укажите пароль на доступ к тому.
6) Укажите файловую систему, которая будет использоваться внутри тома, например **FAT**.

7) Создайте файловый контейнер по нажатию кнопки **Разметить**.

8) Выберите имя будущего логического диска, например **N**.

9) Примонтируйте файловый контейнер, то есть файл **mult.avi** к системе.

10) Перепишите два файла text1.docx и text2.docx в файловый контейнер, то есть на диск N.

11) Размонтируйте файловый контейнер. Убедитесь в том, что информация скрыта. Откройте папку **Мой компьютер** и убедитесь, что логического диска N нет в системе.

12) Выберите режим создания скрытого тома. При этом используйте **Прямой режим** для того, чтобы создать скрытый том внутри имеющегося.

13) Выберите размещение тома TrueCrypt (**файл c:\mult.avi**), внутри которого вы хотите создать скрытый том.

14) Задайте пароль для внешнего тома.

15) Выберите алгоритм шифрования тома **AES** и произвольный алгоритм хеширования для скрытого тома**.**

16) Укажите размер скрытого тома в пределах свободного места внешнего тома.

17) Выберите пароль для скрытого тома.

18) В качестве файловой системы для скрытого тома необходимо использовать **FAT**.

19) Создайте скрытый том по нажатию кнопки **Разметить**.

20) Запишите в скрытый том файл text3.docx.

21) Примонтируйте файл **mult.avi** к логическому диску, например **N** и укажите пароль для доступа к скрытому тому. Убедитесь в том, что доступен файл text3.docx, который записан в скрытый том.

22) Размонтируйте файловый контейнер.

23) Удалите файл **c:\mult.avi.**

Список контрольных вопросов

1) Какие преимущества имеют программы для шифрования данных по сравнению с EFS (встроенное средство Windows для шифрования данных)?

2) Приведите несколько примеров программ для шифрования данных. Какие из них являются платными, а какие бесплатными?

3) Достоинством программы TrueCrypt является то, что она является свободным программным обеспечением. Объясните, что это значит? Какое это имеет значение с точки зрения информационной безопасности?

4) На каких операционных системах работает программа TrueCrypt?

5) Поддерживает ли программа TrueCrypt русский интерфейс? Если поддерживает, то какие дополнительные действия необходимы при настройке программы?

6) Какие три варианта создания новых томов для хранения секретных данных поддерживает программа TrueCrypt?

7) Какие алгоритмы шифрования поддерживает программа TrueCrypt?

8) Что означает флажок “**не сохранять историю**” в программе TrueCrypt?

9) Если мы используем файл в качестве тома, каково может быть имя и расширение файла?

10) Если мы используем файл в качестве тома, по какой причине рекомендуется создать новый файл, а не использовать уже имеющийся файл?

11) Если мы используем файл в качестве тома, то из каких соображений следует выбрать размер файла?

12) Какую длину пароля рекомендует выбрать программа TrueCrypt?

13) Обязательно ли должны совпадать файловые системы диска и тома?

14) Объясните, что значит «примонтировать контейнер к системе» в программе TrueCrypt?

15) С какой целью в программе TrueCrypt можно создать скрытый том?

16) Чем отличается прямой и обычный режим при создании скрытого тома?

17) Сколько скрытых томов позволяет создать программа TrueCrypt?

18) Что такое ключевой файл в программе TrueCrypt?

19) Какие возможности резервного копирования предусмотрены в программе TrueCrypt?

20) Если файловая система тома повреждена, как можно ее восстановить?

Список литературы

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с. : ил.

2. Фергюсон Н. Практическая криптография. / Н. Фергюсон, Б. Шнайер. - М.: Вильямс, 2005. - 424 с.

3. Смарт Н. Криптография. /Н. Смарт; перевод с англ. С. А. Кулешова, под ред. С. К. Ландо. - М.: Техносфера, 2006. - 528 с.

4. Баричев С. Г., Гончаров В. В. , Серов Р. Е. Основы современной криптографии: Учебной курс. – 3-е изд., стереотип. – М.: Горячая линия – Телеком, 2011. -175 с.: ил.

5. Черчхауз Р. Коды и шифры. Юлий Цезарь, «Энигма » и Интернет/ Пер. с англ. – М.: Издательство «Весь Мир», 2009 – 320 с.

6. Исагулиев К. П. Справочник по криптологии. / К. П. Исагулиев. – Мн.: Новое знание, 2004. – 237 с.

7. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

8. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: учебное пособие / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. - 528 с.

9. Нестеров С. А. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие.- СПб.: Изд-во Политехн. ун-та, 2009. -126 с. /Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru

10. Скляров И. С. Хакерские фишки. – М.: Лори, 2008. – 384 с.