**Лабораторная работа № 11**

# **Создание виртуальных зашифрованных дисков (программное средство TrueCrypt)**

**1 Цель работы: изучить умение создания зашифрованных дисков программным средством TrueCrypt**

**Теоретические сведенья:**

## **Основные понятия**

**Общие замечания**

Программа TrueCrypt позволяет создавать полностью зашифрованный виртуальный диск, на котором после начального ввода пароля доступа данные будут автоматически зашифровываться и расшифровываться без вашего вмешательства.

TrueCrypt является международным проектом - некоммерческой свободно распространяемой программой с открытым исходным кодом, проверенным независимыми экспертами.

Защищенный виртуальный диск создается в виде файла, который можно скопировать на любой компьютер и смонтировать, введя пароль. Формат файла вы в процессе создания зашифрованного диска можете выбрать сами в зависимости от необходимого вам размера диска.

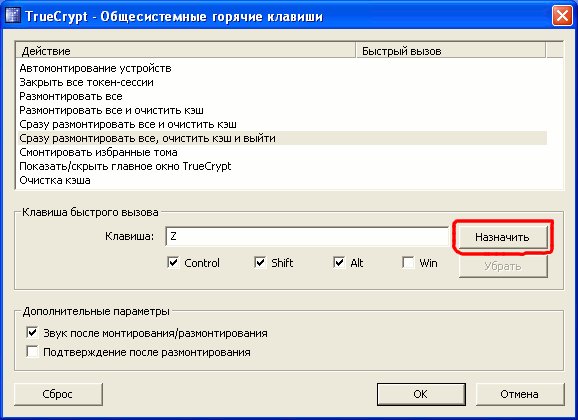
Еще одно достоинство данной программы в том, что ни один диск TrueCrypt не может быть идентифицирован. Защищенный диск, созданный с помощью TrueCrypt, невозможно отличить от набора случайных данных, то есть файл нельзя связать с TrueCrypt как с программой, его создавшей.

Дополнительно внутри данного диска (в терминологии TrueCrypt - внешнего тома) можно создать так называемый скрытый диск размером меньше оригинала (скрытый том). Идея заключается в том, что во внешнем томе вы можете разместить абсолютно нейтральные файлы, которые не содержат конфиденциальной информации. А вот на скрытом томе вы будете размещать именно конфиденциальную информацию. Решение, какой том монтировать, каждый раз принимаете вы сами, и оно зависит от применения того или иного пароля (у внешнего и скрытого томов свои пароли). В случае монтирования внешнего тома скрытый том с конфиденциальными файлами остается невидим.

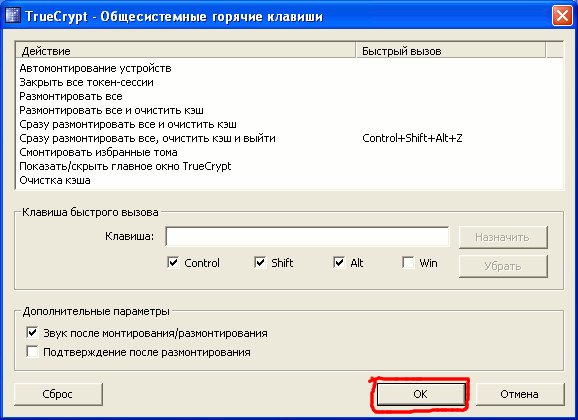
**Настройка TrueCrypt**

Для начала сконфигурируем TrueCrypt таким образом, чтобы можно было закрыть программу, размонтировать диски и очистить временный буфер моментально по сигналу тревоги. Для этого выполните следующие действия:

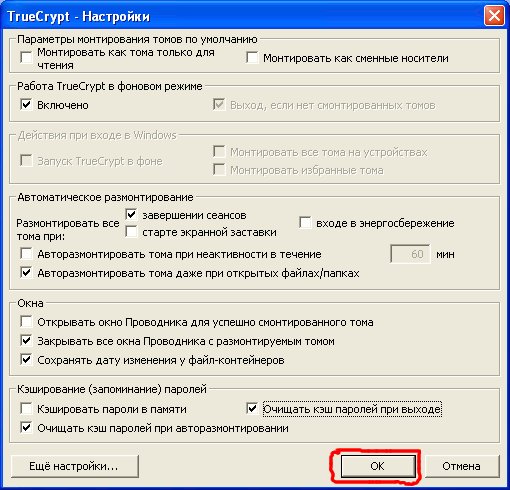
* Пройдите в меню программы Настройки - Горячие клавиши...  - В открывшемся окне выберите пункт "Сразу размонтировать все, очистить кэш и выйти".
* Установите курсор в поле "Клавиша" и нажмите на клавиатуре клавишу, которую вам удобно рассматривать как "горячую". В нашем примере это клавиша с буквой "Z". Вы также можете выбрать, какие клавиши использовать совместно с ней - Control, Shift, Alt, Win, установив или убрав флажок рядом с названием клавиши. Мы выбрали клавиши Control, Shift и Alt. Это означает, что при нажатии одновременно на клавиши Control, Shift, Alt и Z все TrueCrypt-диски будут размонтированы, временный буфер очищен и программа закроется.
* После выбора "горячих" клавиш нажмите кнопку "Назначить".



* Нажмите кнопку "ОК".



Затем установите остальные настройки:   
- Пройдите в меню программы Настройки - Настройки...   
- Установите все настройки так, как это указано на скриншоте. Нажмите кнопку "ОК".

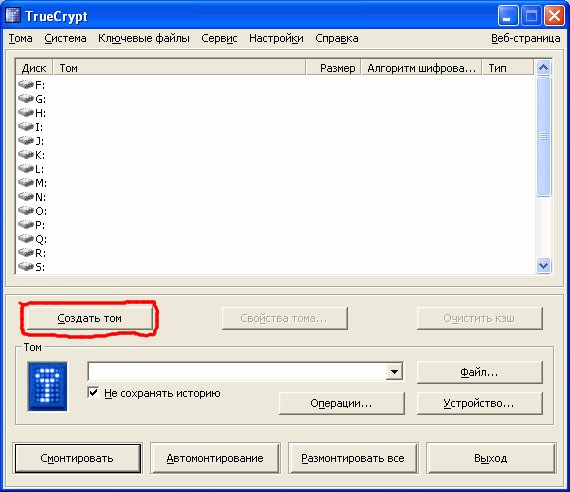


**Работа с программой TrueCrypt**

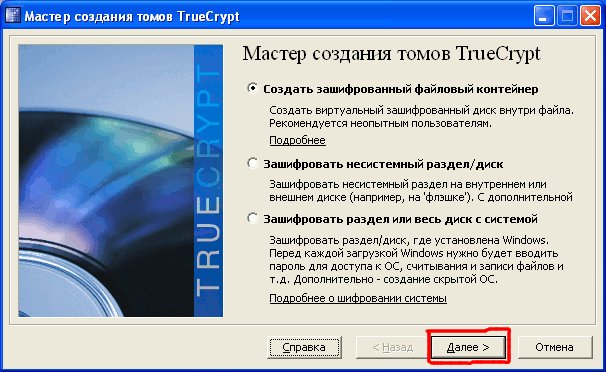
Итак, перейдем непосредственно к работе с программой. Для начала научимся создавать внешний том. Затем - скрытый том. После этого научимся монтировать и размонтировать тома.

**Создание внешнего тома TrueCrypt**

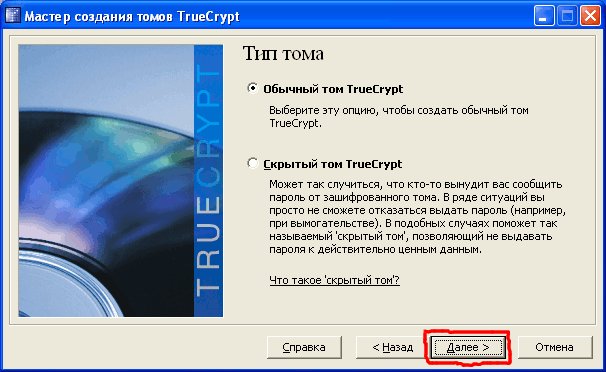
- В основном окне программы нажмите кнопку "Создать том". Запустится мастер создания томов.



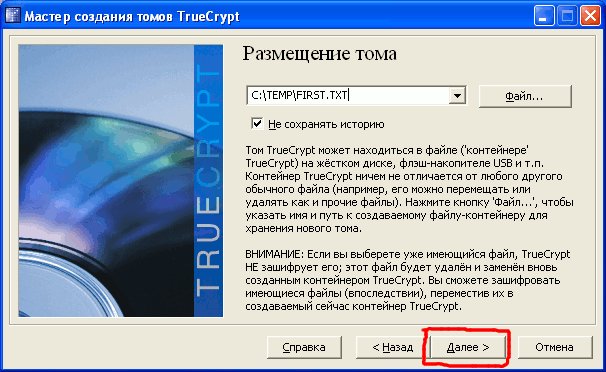
- В появившемся окне выберите пункт "Создать зашифрованный файловый контейнер" и нажмите кнопку "Далее".



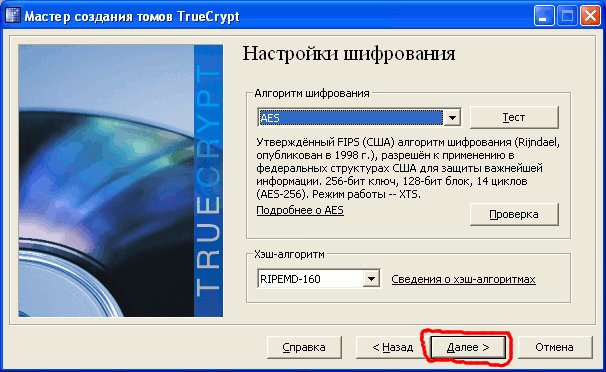
- Выберите пункт "Обычный том TrueCrypt" и нажмите кнопку "Далее".



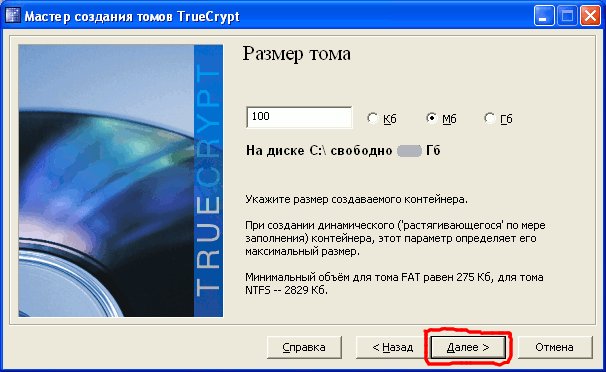
- Введите путь размещения файла, его имя и расширение. В нашем примере это C:\TEMP\FIRST.TXT. Этот файл будет создан и именно под него будет замаскирован том TrueCrypt. Убедитесь, что установлен флажок "Не сохранять историю". Нажмите кнопку "Далее". Если вы выберете уже имеющийся файл, то TrueCrypt не зашифрует его; этот файл будет удален и заменен созданным контейнером TrueCrypt. Впоследствии вы сможете зашифровать имеющиеся файлы, переместив их в контейнер TrueCrypt.



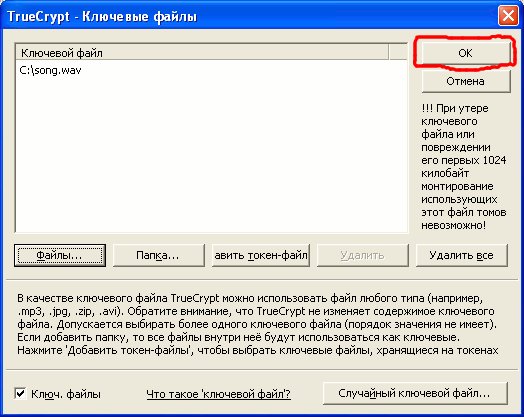
- В следующем окне вы можете выбрать алгоритм шифрования (по умолчанию - AES) и хэш-алгоритм (по умолчанию - RIPEMD-160). Установленные по умолчанию значения вполне надежны и обеспечивают приемлемую скорость шифрования/дешифрования информации. Поэтому мы рекомендуем оставить именно их. Нажмите кнопку "Далее".



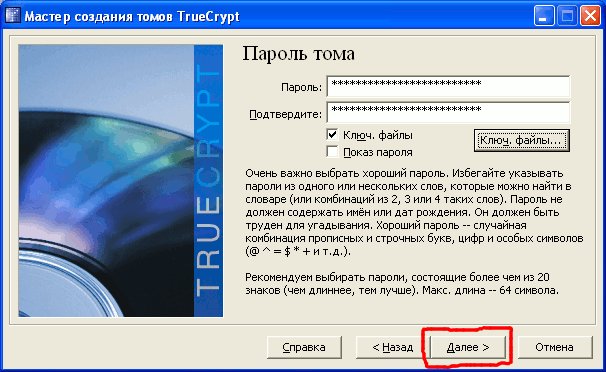
- Выберите размер тома и нажмите кнопку "Далее". При этом учтите, что скрытый том TrueCrypt, который мы будем создавать впоследствии, будет меньше, чем внешний том. В данном примере мы будем создавать внешний том размером 100 Мб.



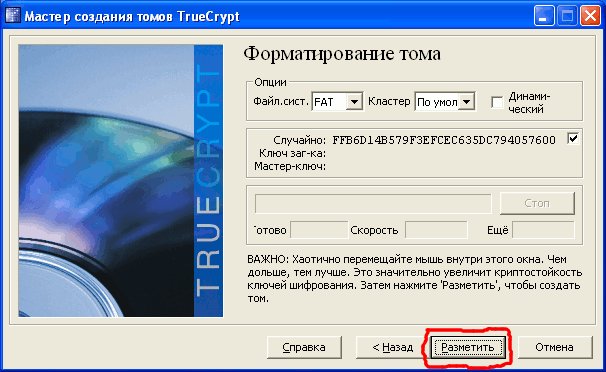
- Введите пароль и подтвердите его. Максимальная длина пароля - 64 символа. Постарайтесь выбрать пароль, состоящий не менее, чем из 20 знаков.   
Также мы рекомендуем выбрать ключевые файлы, т.е. файлы, которые вам нужно будет указывать каждый раз, когда вы будете монтировать том TrueCrypt. В качестве ключевых файлов подойдут любые, их расширение значения не имеет. Однако впоследствии вам нужно будет следить за тем, чтобы файлы, выбранные вами в качестве ключевых, не были повреждены. Иначе вы не сможете смонтировать том TrueCrypt и получить доступ к данным.   
Для выбора ключевых файлов установите флажок "Ключ. файлы" и нажмите кнопку "Ключ. файлы...". В открывшемся окне нажмите кнопку "Файлы..." и выберите ключевые файлы. При этом учтите, что запоминается путь, а не только имена файлов. Для того, чтобы том мог быть смонтирован, файлы должны располагаться в той же директории, что и при их выборе в качестве ключевых во время создания тома. Если добавить папку, нажав на кнопку "Папка", то все файлы внутри нее будут использоваться как ключевые.   
В нашем примере мы выбрали файл song.wav. Полный путь к файлу, который будет указан - C:\song.wav. Вы можете выбрать любое количество файлов. Для большей секретности файлы могут располагаться на USB флеш-накопителе или диске. Нажмите кнопку "ОК".



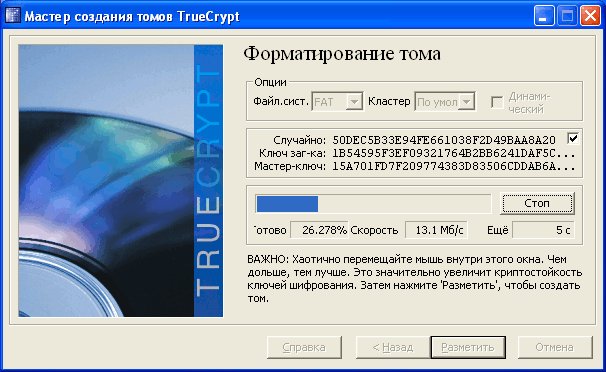
В окне "Мастер создания томов TrueCrypt" нажмите кнопку "Далее".



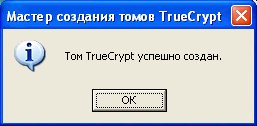
- В следующем окне вы можете выбрать тип файловой системы создаваемого тома. Для внешнего тома мы рекомендуем использовать файловую систему FAT, чтобы скрытый том можно было создать максимально возможного размера. Тип кластера установите "По умолчанию". Не устанавливайте флажок "Динамический".   
После этого поводите курсором мыши по этому окну. Вы заметите, что при движении курсора случайный код меняется быстрее. Такое броуновское движение курсором улучшает случайность шифровки этого тома. Когда наиграетесь с курсором, нажмите кнопку "Разметить".



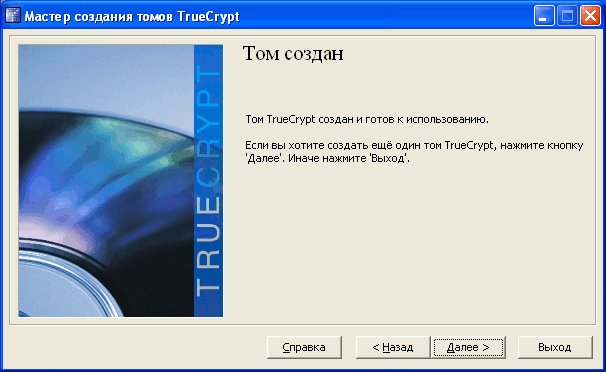
- После этого будет запущен процесс создания внешнего тома TrueCrypt. Дождитесь, пока он будет завершен.



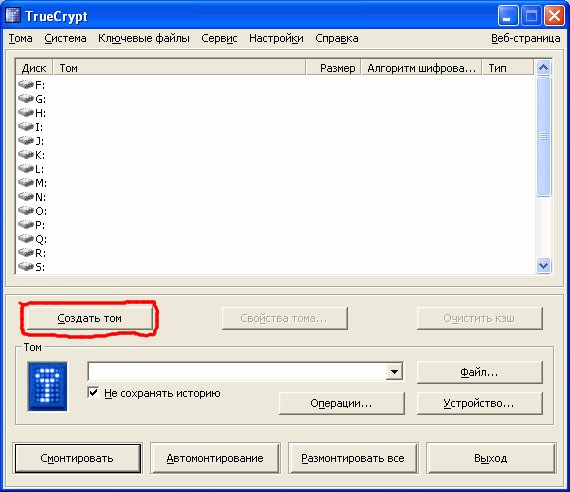
- После создания тома появится сообщение о его успешном создании. Нажмите кнопку "ОК".



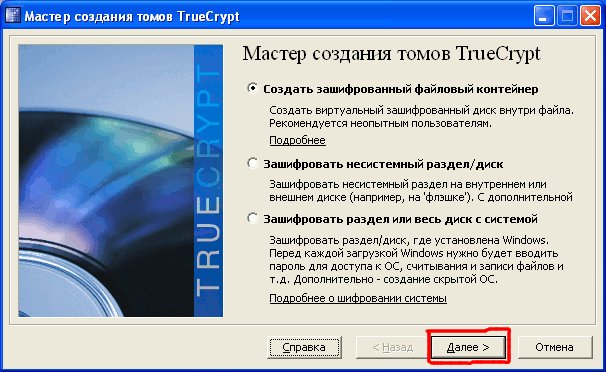
- В следующем окне нажмите кнопку "Далее", если хотите продолжить процесс создания томов, или кнопку "Выход".



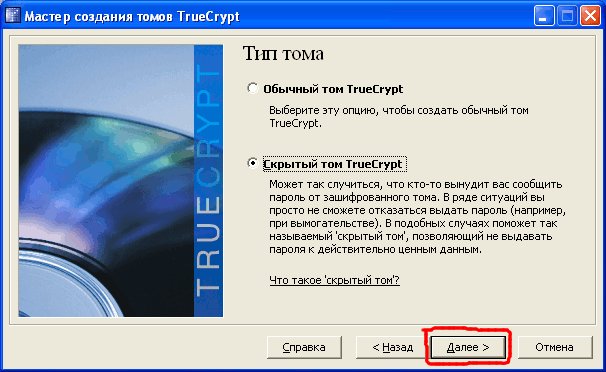
**4.2. Создание скрытого тома TrueCrypt**  
После того, как создан внешний том TrueCrypt, можно перейти к созданию скрытого тома.   
  
Обратите внимание, что скрытый том будет спрятан внутрь только что созданного внешнего тома. Отсюда следует, что скрытый том не может быть больше внешнего тома. В нашем примере это 100 Мб для внешнего тома и 70 Мб для скрытого. Такая разница нужна для того, чтобы мы могли впоследствии разместить во внешнем томе несколько файлов с посторонней информацией для маскировки. Вы можете создать несколько скрытых томов внутри одного внешнего тома. Главное, чтобы суммарный объем всех скрытых томов не превышал размера внешнего тома.   
  
Также обратите внимание, что для создания скрытого тома нужно ввести пароль, который вы ранее использовали для внешнего тома, а в окне "Пароль скрытого тома" - новый пароль для скрытого тома (дважды - в полях "Пароль" и "Подтвердите").   
  
- В основном окне программы нажмите кнопку "Создать том". Запустится мастер создания томов.



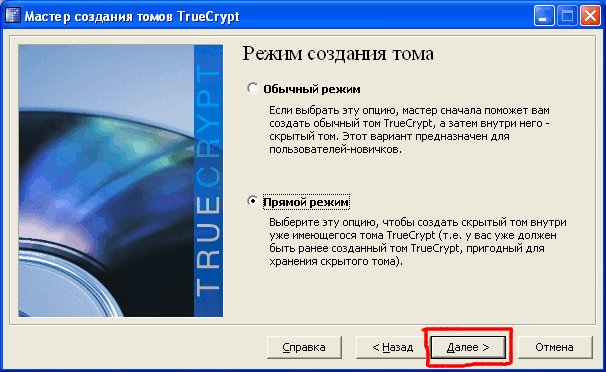
- В появившемся окне выберите пункт "Создать зашифрованный файловый контейнер" и нажмите кнопку "Далее".



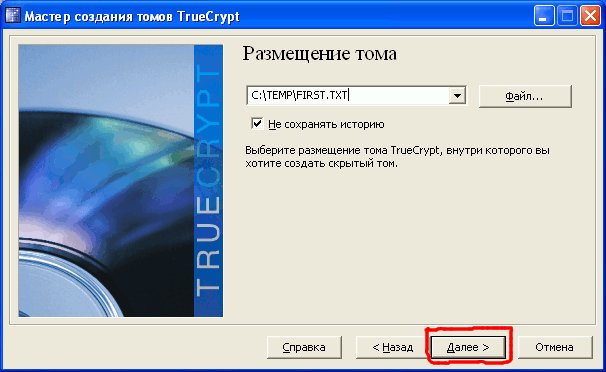
- Выберите пункт "Скрытый том TrueCrypt" и нажмите кнопку "Далее".



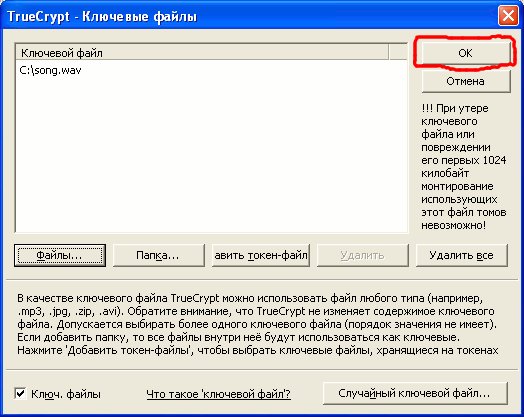
- Выберите пункт "Прямой режим" и нажмите кнопку "Далее".



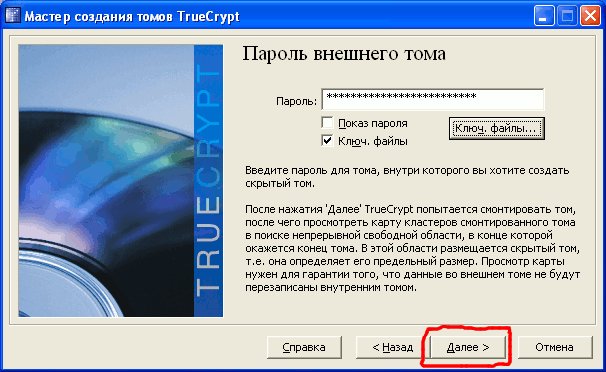
- Укажите путь к файлу, который маскирует внешний том TrueCrypt. Внутри этого внешнего тома будет создан скрытый том TrueCrypt. В нашем примере этот путь - C:\TEMP\FIRST.TXT. Убедитесь, что установлен флажок "Не сохранять историю". Нажмите кнопку "Далее".



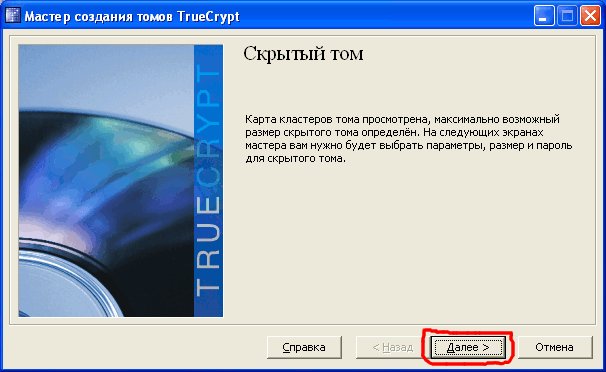
- В следующем окне введите пароль внешнего тома. Если вы при создании внешнего тома указывали ключевые файлы, необходимые для монтирования тома, то установите флажок "Ключ. файлы" и нажмите на кнопку "Ключ. файлы...".   
В открывшемся окне нажмите кнопку "Файлы..." и выберите файлы, которые вы указывали в качестве ключевых при создании внешнего тома. В нашем примере это C:\song.wav. После того, как будут указаны все ключевые файлы, нажмите кнопку "ОК".



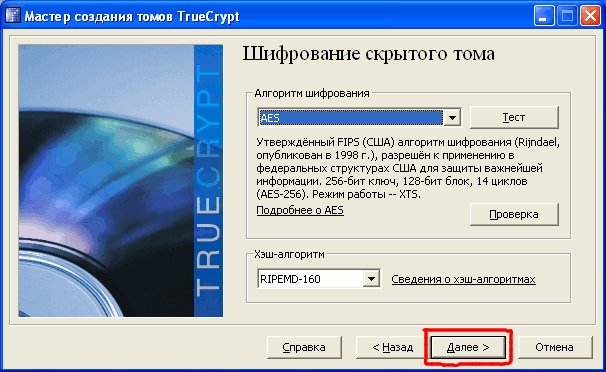
В окне "Мастер создания томов TrueCrypt" нажмите кнопку "Далее".



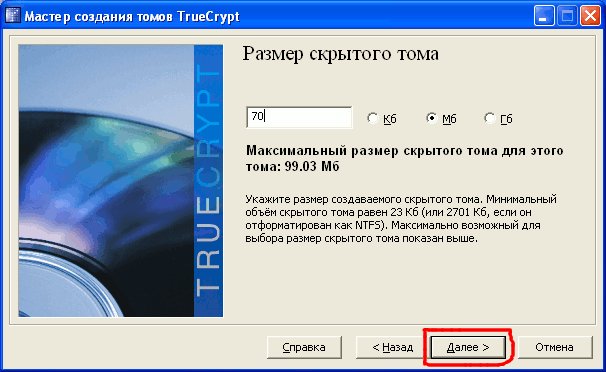
- В следующем окне нажмите кнопку "Далее".



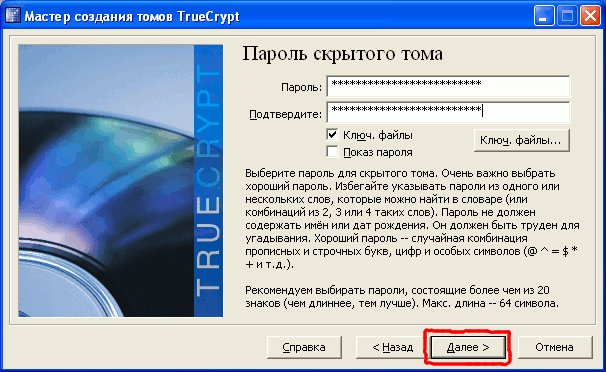
- В следующем окне вы можете выбрать алгоритм шифрования и хэш-алгоритм скрытого тома. Мы рекомендуем оставить те значения, которые установлены по умолчанию. Нажмите кнопку "Далее".



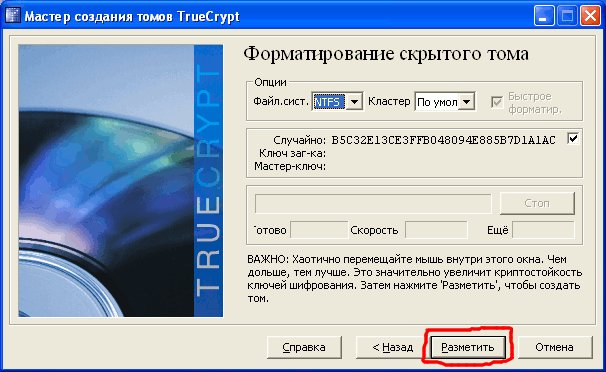
- В следующем окне будет указан максимально возможный размер скрытого тома. Укажите размер скрытого тома. В нашем примере мы выбрали размер 70 Мб. Нажмите кнопку "Далее".



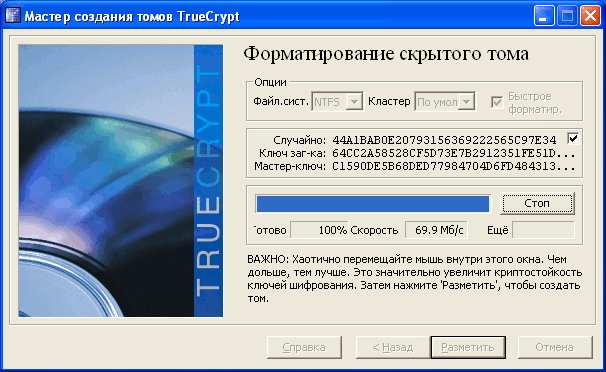
- Введите пароль скрытого тома и подтвердите его. Максимальная длина пароля - 64 символа. Постарайтесь выбрать пароль, состоящий не менее, чем из 20 знаков.   
Также выберите и укажите ключевые файлы так, как вы это уже умеете. Нажмите кнопку "Далее".



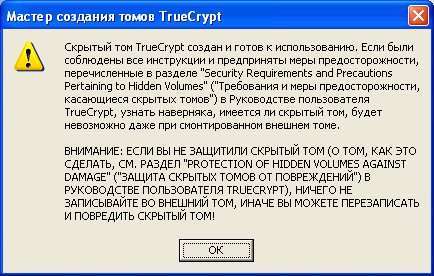
- В следующем окне вы можете выбрать тип файловой системы создаваемого тома. Для скрытого тома мы рекомендуем использовать файловую систему NTFS. Тип кластера установите "По умолчанию".   
После этого поводите курсором мыши по этому окну, как и при создании внешнего тома. Потом нажмите кнопку "Разметить".



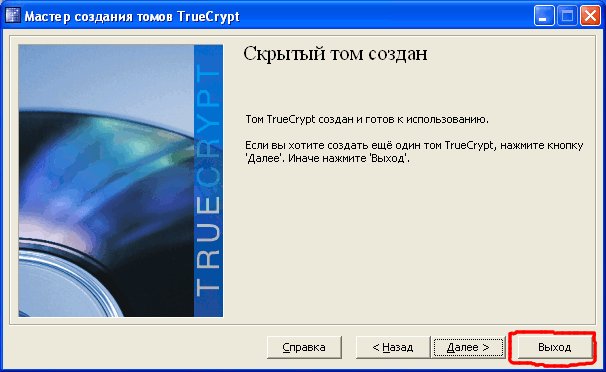
 Будет запущен процесс создания скрытого тома TrueCrypt. Дождитесь, пока он будет завершен.



- После окончания процесса создания скрытого тома появится окно, предупреждающее о разумности защиты скрытых томов при монтировании внешнего тома. Если вы об этом забудете, вы можете случайно затереть информацию на скрытом томе, когда размещаете файлы на внешнем томе. В этом окне нажмите кнопку "ОК".



- В следующем окне нажмите кнопку "Выход".



**Задание №1**

В лабораторной работе необходимо создать виртуальный зашифрованный диск. Наполнить его небольшим количеством файлов. Создать скрытый том. Попробовать прочесть созданный файл тома. Размонтировать и снова смонтировать том.

**Оформите отчет.**