**Лабораторная работа № 15**

Тема: «Cоздание виртуальных зашифрованных дисков (программное средство truecrypt)».

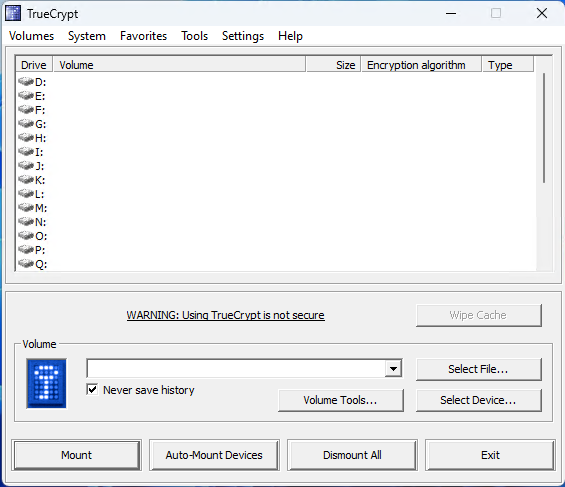
Цель: формирование умений шифрования жесткого диска или его частей и работы с виртуальными образами зашифрованной области.

TrueCrypt – это программная система для создания и использования шифруемого «на лету» тома (устройства хранения данных).

Шифрование и использование несистемного раздела диска.

Шаг 1. Запустите TrueCrypt, дважды щелкнув по значку TrueCrypt.exe, или вызовите его из меню Пуск.

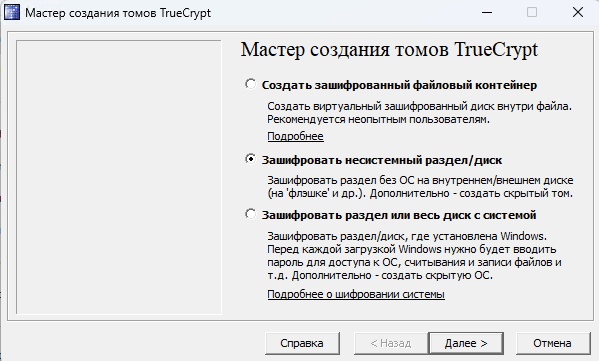
Шаг 2. На экране появится главное окно TrueCrypt (рисунок 1). Нажмите «Создать том».

Рисунок 1 – Главное окно.

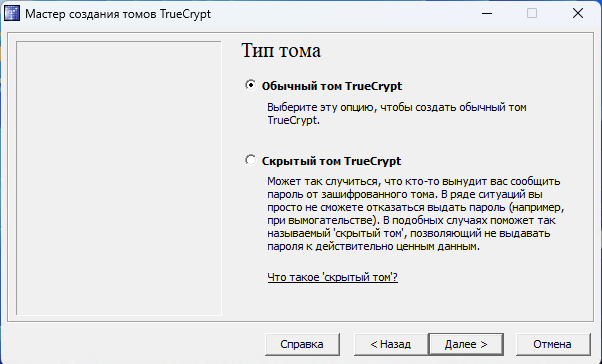
Шаг 3

На экране должно появиться окно «Мастера создания раздела TrueCrypt» (рисунок 2).

Выберите место, где нужно создать раздел TrueCrypt. Раздел TrueCrypt может быть размещен в файле, который также называют контейнером, в разделе диска или на дисковом устройстве. Зашифруйте запоминающее USB-устройство, выбрав вторую опцию «Зашифровать несистемный раздел/диск» и кликнув кнопку «Далее».

Рисунок 2 – Мастер создания раздела.

Шаг 4. На данном этапе предстоит выбрать, каким будет наш тип тома (рисунок 3).

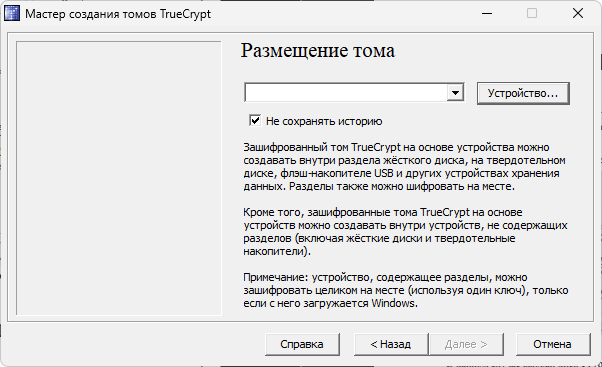
Рисунок 3 – Выбор типа тома.

Возможны два варианта: обычный том TrueCrypt, скрытый том TrueCrypt.

Выберите опцию Обычный том TrueCrypt.

П р и м е ч а н и е. Опцию Скрытый том TrueCrypt рассмотрим в шаге 12.

Шаг 5. Выберите устройство, которое будет зашифровано (рисунок 4).

Рисунок 4 – Выбор устройства для шифрования.

В данном случае выбран диск E: (рис. 12.5). Затем перейдите к следующему шагу, нажав кнопку Далее.

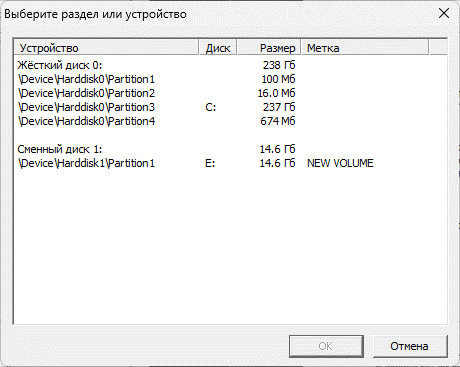
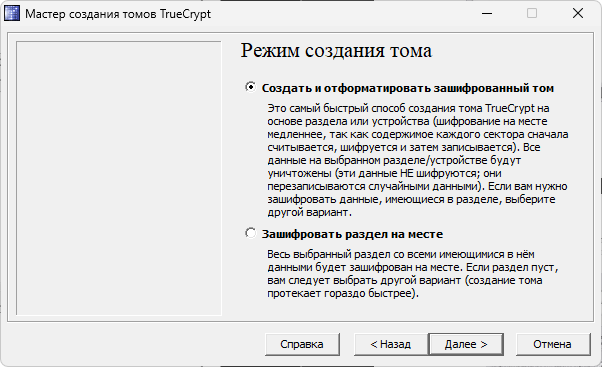
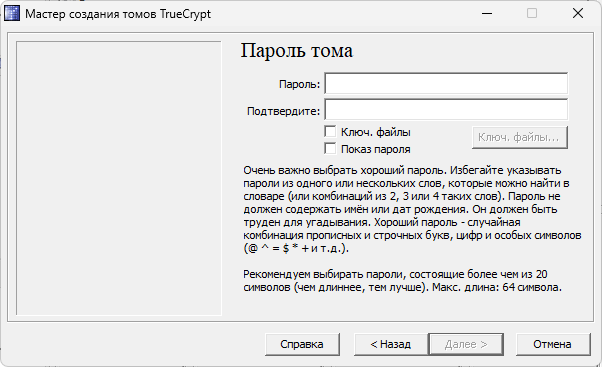


Рисунок 5 – .

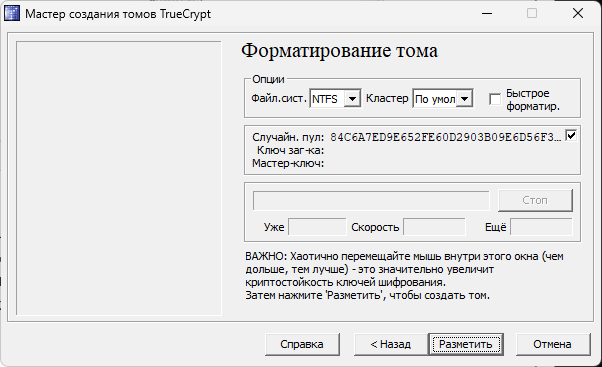
Шаг 6. На данном этапе выберите одну из двух опций (рис. 12.6): создать зашифрованный том и отформатировать его; зашифровать раздел на его месте.

Рисунок 6 – Выбор режима создания тома.

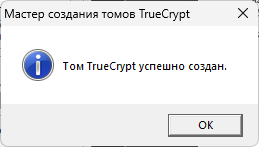
Настройка тома (рисунок 7).

Рисунок 7 – Пароль тома.

В окне Volume Creation Wizard как минимум 30 секунд случайно двигайте мышкой в разных направлениях, чем дольше вы будете ею двигать, тем значительно увеличите криптографическую силу ключей шифрования (которые, в свою очередь, усилят безопасность). Нажмите Разметить (8).

Рисунок 8 – Форматирование тома.

После завершения операции, появляется сообщение, что том создан (рисунок 9).

Рисунок 9 – Том создан.

Теперь нужно научиться им пользоваться. При обычной попытке доступа к зашифрованному устройству (Мой компьютер – Зашифрованное устройство), Windows предложит его отформатировать (после процесса форматирования устройство окажется пустым и незашифрованным). Для доступа к созданному тому откройте TrueCrypt и на главной форме выберите устройство, которое шифровали (на нашем примере это диск E: (рис. 10)).

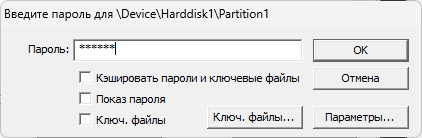
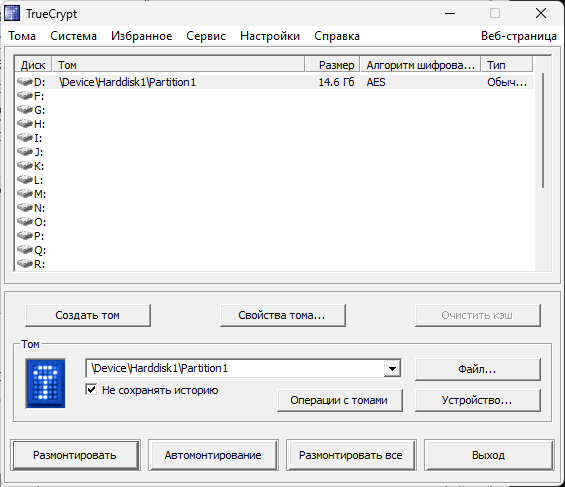


Рисунок 10 – Ввод пароля.

Если пароль правильный, то раздел будет смонтирован. Зашифрованное устройство успешно смонтировано как виртуальный диск D: (рис. 11).

Рисунок 11 – Том смонтирован.

Выберите раздел из списка смонтированных разделов в главном окне TrueCrypt и затем нажмите Размонтировать.

Расшифровка устройства.

Если потребуется обратно расшифровать устройство, выполните следующие действия: проверьте, что зашифрованное устройство размонтировано; зайдите в Мой компьютер; найдите в списке дисков зашифрованный (тот, который хотите расшифровать); кликните правой кнопкой по выбранному диску; выберите из списка контекстного меню пункт Форматировать. По окончании форматирования диск будет расшифрован и доступен так же, как и раньше.

Шаг 12.

Для создания скрытого тома повторите шаги один–три и на четвертом выберите пункт Скрытый том TrueCrypt (рис. 12).

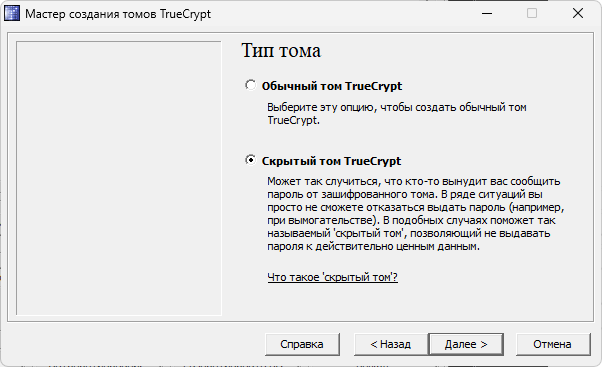
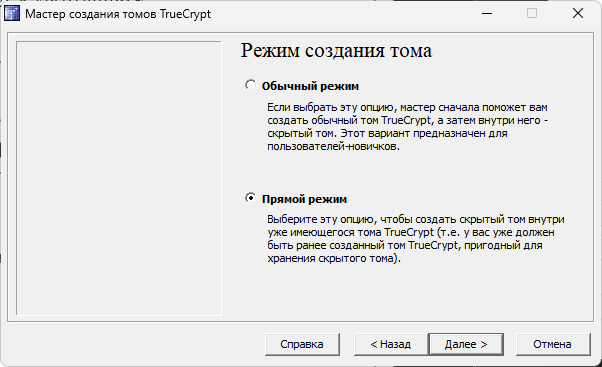


Рисунок 12 – Скрытый том.

Шаг 13.

Выбираем прямой режим создания тома (рисунок 13).

Рисунок 13 – Создание тома.

Шаг 14.

Выберите устройство (диск) или каталог, в котором нужно создать скрытый том (рис. 14).

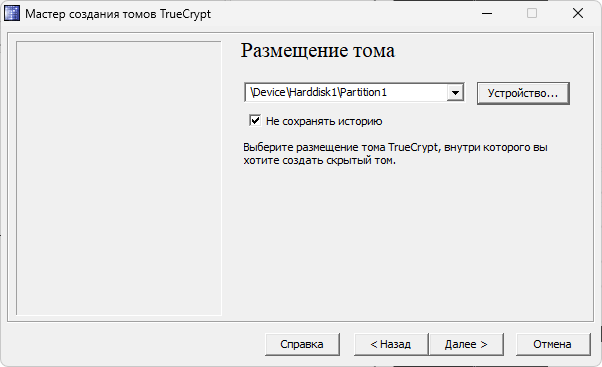


Рисунок 14 – Размещение тома.

Шаг 15.

На этом шаге введите пароль, который применяется в обычном томе (этот пароль был использован в шаге 9. После ввода пароля кликните Далее.

Шаг 16

Внимательно прочитайте уведомление (рисунок 15).

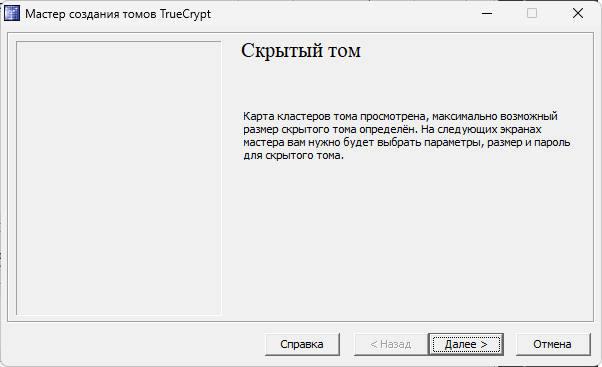


Рисунок 15 – Скрытый том.

Шаг 17.

Данный шаг аналогичен шагу 7.

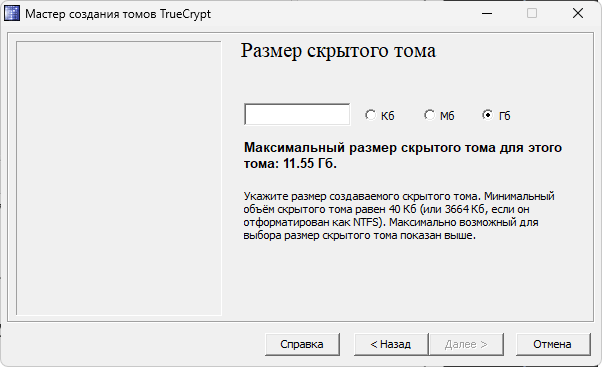


Рисунок 16 – Размер тома.

Шаг 18.

Выбираем размер скрытого тома.

Шаг 19.

Этот шаг аналогичен шагу 9.

Шаг 20.

Данный шаг аналогичен шагу 10. Прочитайте уведомление (рисунок 17).

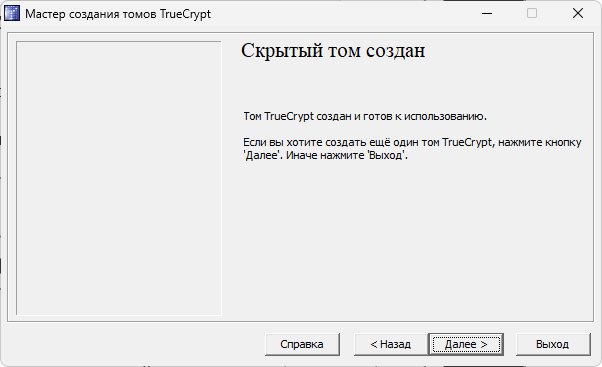


Рисунок 17 – Скрытый том создан.

Шаг 21

Работа со скрытым томом аналогична работе с внешним. Отличие лишь в том, что для доступа к скрытому тому необходимо вводить пароль из шага 19, а не из шага 9.

Контрольные вопросы.

1. Что значит термин шифрование «на лету»?

Шифрование "на лету" означает, что данные шифруются или дешифруются непосредственно в момент их записи на диск или чтения с диска, без необходимости сохранения данных в открытом виде на промежуточном этапе. Это позволяет обеспечить защиту данных в реальном времени, что особенно полезно при работе с конфиденциальной информацией.

2. Какие есть режимы работы программы TrueCrypt?

Программа TrueCrypt имеет несколько режимов работы, включая:

Режим шифрования целого диска или устройства, который позволяет зашифровать все данные на диске целиком.

Режим шифрования раздела, который позволяет зашифровать отдельный раздел на диске.

Режим создания скрытого зашифрованного раздела, который позволяет создать дополнительный зашифрованный раздел на диске, который будет скрыт от посторонних.

3. Как удалить зашифрованный раздел?

Чтобы удалить зашифрованный раздел, необходимо:

Открыть программу TrueCrypt.

Выбрать зашифрованный раздел, который нужно удалить.

Нажать кнопку "Демонтировать" или аналогичную, чтобы размонтировать раздел.

После этого можно удалить раздел из программы TrueCrypt, указав соответствующую опцию.

4. Перечислите преимущества данного программного средства.

Преимущества программы TrueCrypt включают:

Мощное шифрование данных, обеспечивающее высокий уровень безопасности.

Возможность шифрования как целых дисков, так и отдельных разделов.

Наличие функции создания скрытых зашифрованных разделов для повышения конфиденциальности.

Кросс-платформенная поддержка, что позволяет использовать программу на различных операционных системах.

Бесплатность и открытый исходный код, что обеспечивает прозрачность и возможность проверки безопасности программы.