СВОБОДНО РАСПРОСТРАНЯЕМАЯ ПРОГРАММА ДЛЯ ШИФРОВАНИЯ ДИСКОВ VERACRYPT

1 Теоретическая часть

VeraCrypt – бесплатное программное обеспечение с открытым исходным кодом для шифрования файлов и дисков, использующая шифрование «на лету». Программа была создана на основе исходного кода программы TrueCrypt, которая когда-то была популярна, но проект был закрыт. На рисунке 1 показан общий вид интерфейса программы.

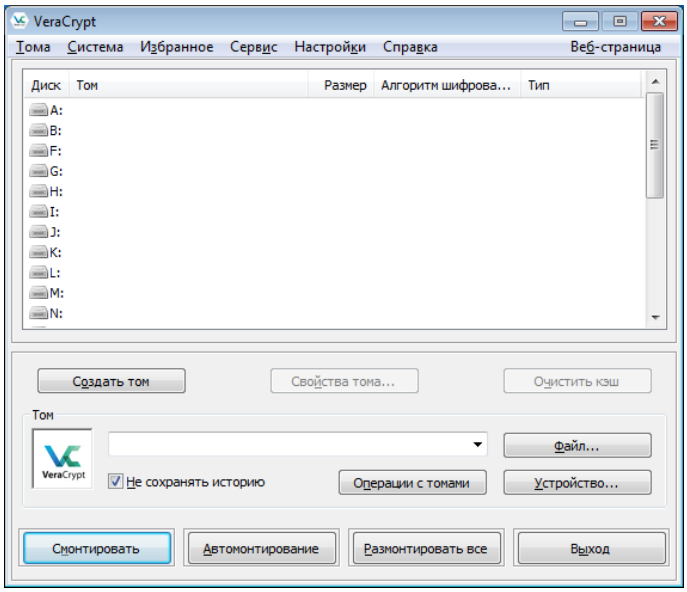

Рисунок 1 – Общий вид программы

Программа работает под операционными системами семейства Windows, Linux, MacOS X, FreeBSD 11. Выпускаются версии для установки и портативные, что не только упрощает работу с программой за счет кроссплатформенности и быстроты установки на новой системе, но и позволяет сразу избавиться от нее после завершения работы, что усложняет установку факта шифрования ею.

VeraCrypt использует следующие алгоритмы шифрования: AES, Serpent, Twofish, Camellia, Кузнечик, а также комбинации этих алгоритмов. Используемые криптографические хеш-функции: RIPEMD-160, SHA-256, SHA-512, Стрибог и Whirlpool. Ключ заголовка и вторичный ключ заголовка для режима XTS генерируются при помощи алгоритма PBKDF2 с использованием

512-битной криптографической соли, число итераций составляет от 327 661 до 655 331, в зависимости от используемой хеш-функции. Это позволяет выбрать пользователю предпочитаемый алгоритм шифрования и балансировать между производительностью и сложностью криптографических преобразований.

Программа может создавать файловые контейнеры и шифровать диски целиком, при этом имеется возможность создать дополнительно скрытые контейнеры и тома, которые будут находиться внутри других зашифрованных контейнерах и томах. Это позволяет выдать ключ для расшифрования файлов злоумышленнику, но при этом важные файлы будут все еще находиться в безопасности.

Также возможно зашифровать системный диск и создать скрытую операционную систему. В случаи вынужденной выдачи пароля, можно будет выдать пароль от операционной системы, которая не представляет ценности, в то время, как ваши файлы останутся в безопасности.

Для расшифровывания может использоваться пароль или ключевой файл.

2 Практическая часть

2.1 Создание зашифрованного файлового контейнера

Для создания зашифрованного файлового контейнера перейдите в меню программы – тома – создать новый том (рисунок 2).

В программе файловые контейнеры называются томами.

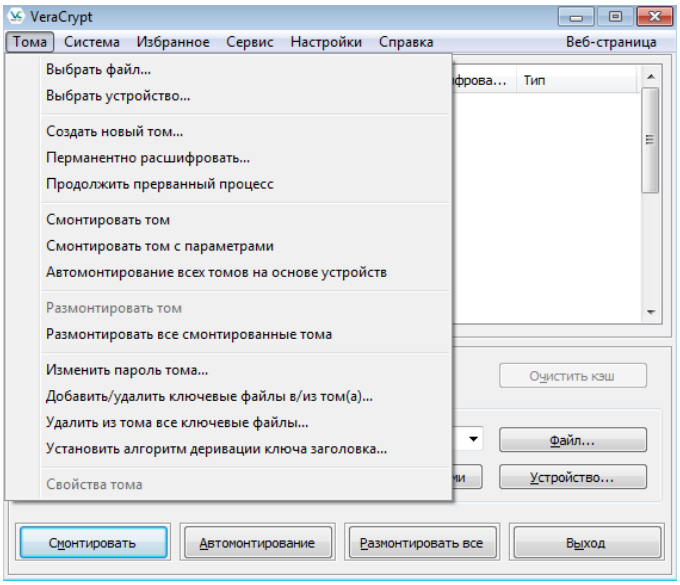

Рисунок 2 – Меню «Тома»

После этого высветится окно создания томов. Выберите пункт «Создать зашифрованный файловый контейнер» и нажмите кнопку «Далее» (рисунок 3).

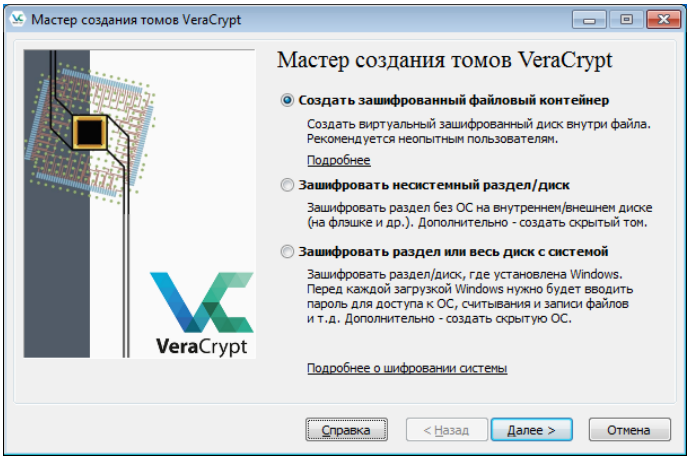

Рисунок 3 – Мастер создания томов

Далее нужно выбрать тип создаваемого тома. Если выбрать тип «Обычный том VeraCrypt», то контейнер будет просто зашифрован. Если же выбрать «Скрытый том VeraCrypt», то будут созданы два тома, один будет вложен в другой и вложенный будет скрыт. При этом не обязательно постоянно вводить оба пароля, достаточно ввести только один для тома, который хотите открыть.

Следует учитывать, что НЕ скрытый том динамически расширяется и если у вас контейнер занимает 10Гб, вы запишите в скрытый том 9Гб информации, а в не скрытый 2 Гб, то скрытый будет поврежден и сузится до 8Гб.

Выберем тип тома «Обычный том» (рисунок 4).

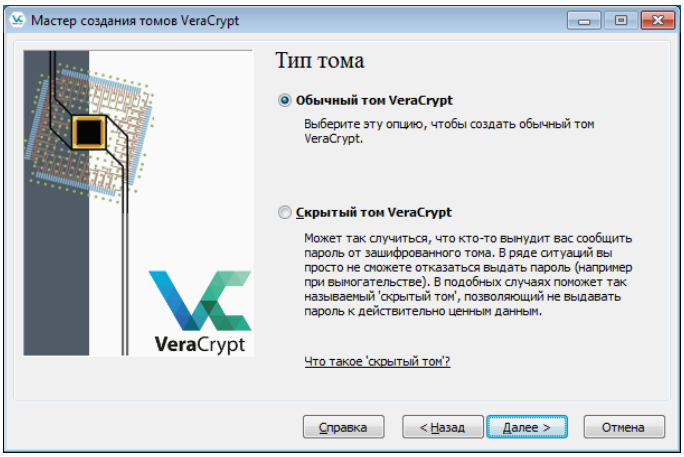

Рисунок 4 – Тип тома

Выберем путь, где будет располагаться контейнер, и название файла в соответствии с группой и инициалами (рисунок 5).

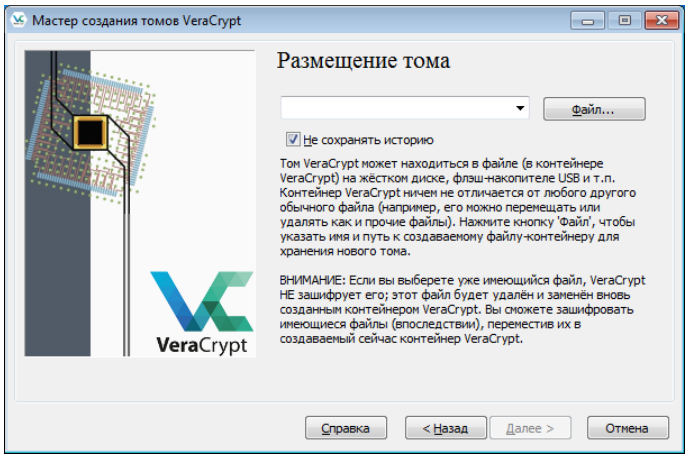

Рисунок 5 – Размещение тома

Выберите алгоритм шифрования в соответствии с вариантом (рисунок 6 и 7).

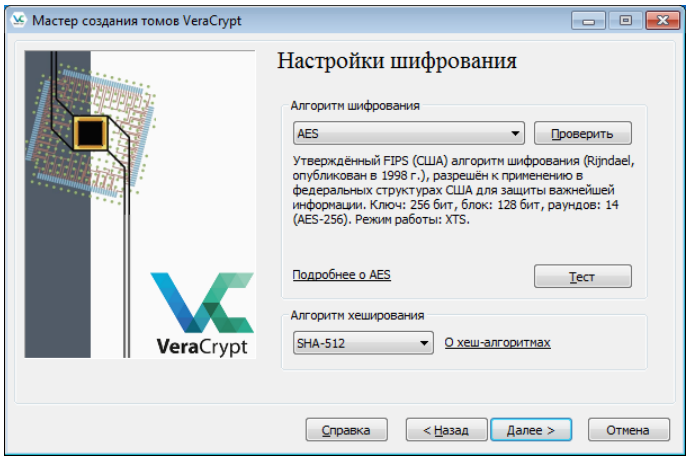

Рисунок 6 – Настройки шифрования

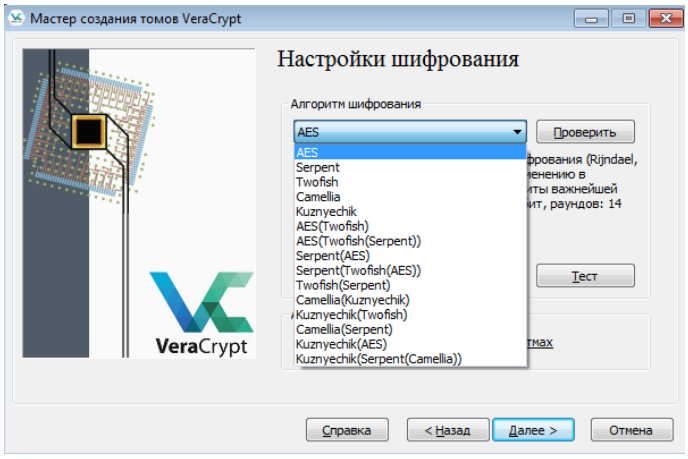

Рисунок 7 – Алгоритмы шифрования

Алгоритм хеширования оставим по умолчанию «SHA-512» (рисунок 8).

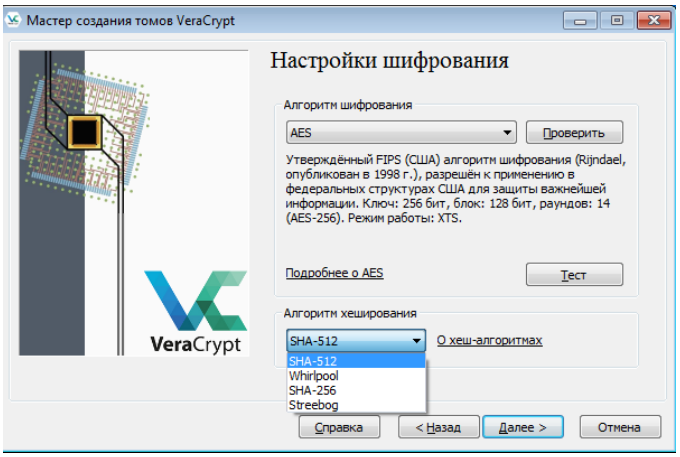

Рисунок 8 – Алгоритмы хеширования

Нажмите кнопку «Проверить» в разделе «Алгоритм шифрования». Выполните проверку выбранного алгоритма шифрования (рисунок 9).

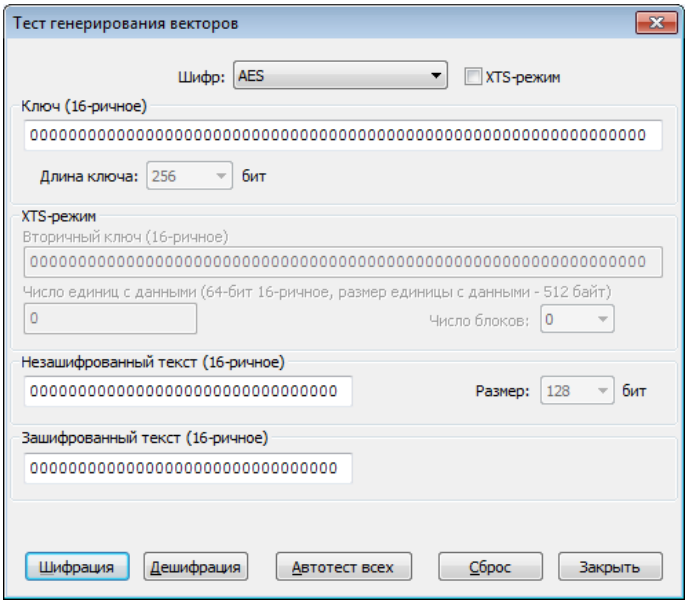

Рисунок 9 – Тестирования алгоритма шифрования

Выболните тест скорости алгоритмов шифрования нажав на кнопку «Тест» (рисунок 10). Проанализируйте полученные данные.

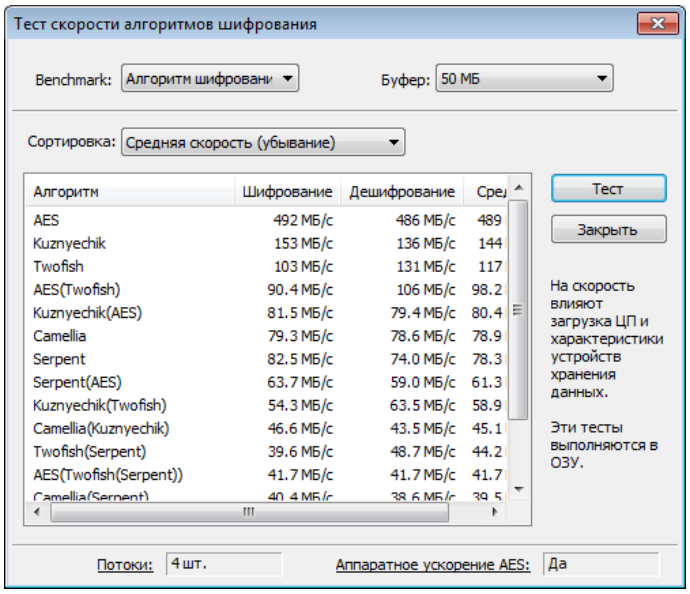

Рисунок 10 – Тест скорости алгоритмов шифрования

Выберите размер создаваемого файлового контейнера (рисунок 11).

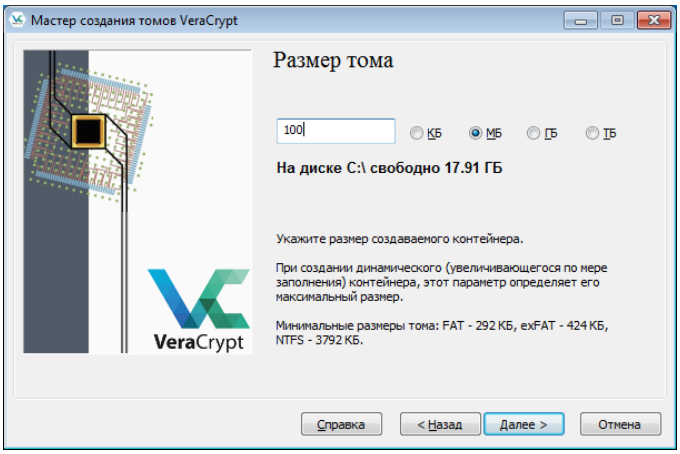

Рисунок 11 – Размер тома

Далее необходимо создать ключевые файлы для создаваемого контейнера. Для этого поставим отметку в пункте «Ключ. Файлы» и нажмем на кнопку «Ключ. Файлы» (рисунок 12).

Также возможно использовать пароль и PIM, но сейчас мы это делать не будем.

PIM – персональный умножитель итераций. Эта функция усложняет взлом перебором. При использовании PIM, при вводе пароля, потребуется постоянно его использовать.

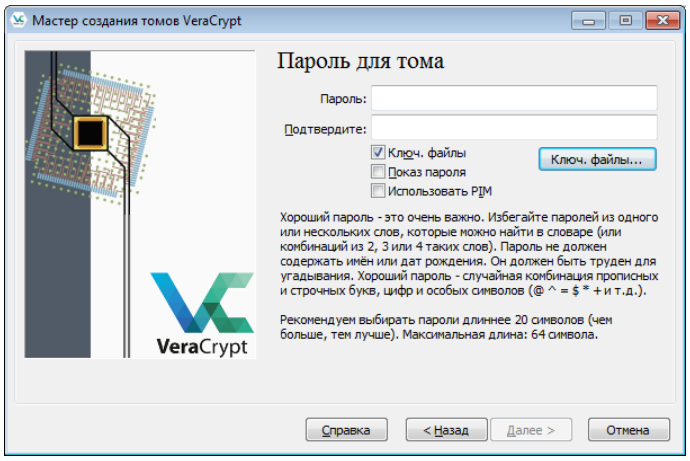

Рисунок 12 – Настройка доступ к тому

Создайте любой файл осмысленного содержимого, например, картинку, в любом месте диска виртуальной машины. Файл может иметь любое содержимое и расширение. В интерфейсе программы на кнопку «Файл» и выберите созданный файл. Нажмем кнопку «Ок» и «Далее» (рисунок 13).

Файлов может быть несколько, иметь различный формат и содержимое, располагаться в любом месте, включая флеш-диск и электронный ключ. Но учтите, что, потеряв его, вы больше никогда не сможете получить доступ к зашифрованным файлам.

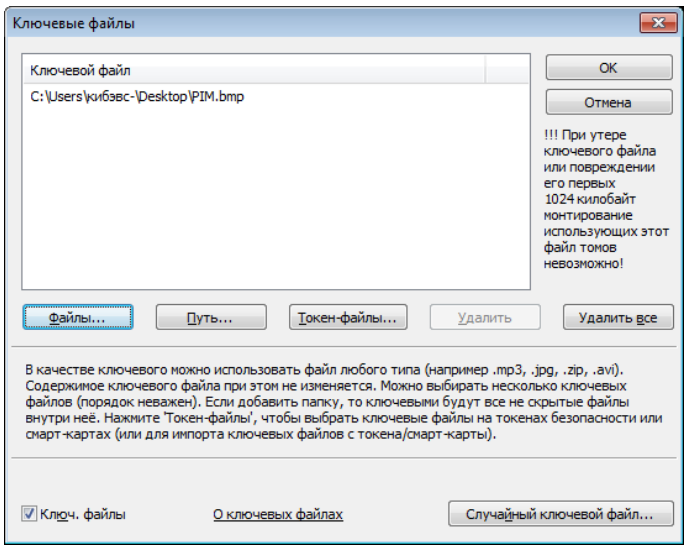

Рисунок 13 – Добавление ключевого файла

Далее выберем файловую систему FAT. Соберем энтропию, для этого будем случайно перемещать мышь по интерфейсу окна программы. В процессе будет заполняться шкала «Собрано энтропии из перемещений мыши». Чем

больше будет заполнена шкала – тем сложнее будет взломать ваш зашифрованный том.

По окончании сбора энтропии нажмите кнопку «Разметить» (рисунок 14).

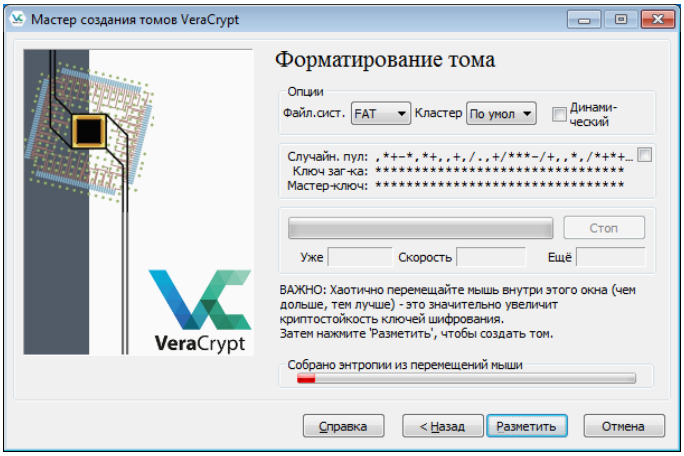

Рисунок 14 – Разметка тома

После завершения разметки будет выдано сообщение о успехе (рисунок 15).

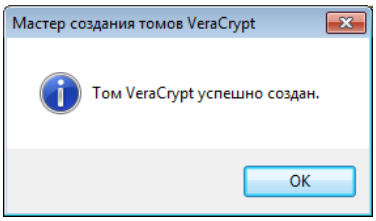

Рисунок 15 – Успешное создание тома

Перейдем в основной интерфейс программы. Для открытия созданного контейнера необходимо выбрать любую из доступных в интерфейсе программы букв диска, нажать кнопку «Файл» и выбрать контейнер. Далее необходимо нажать кнопку «Смонтировать» (рисунок 16).

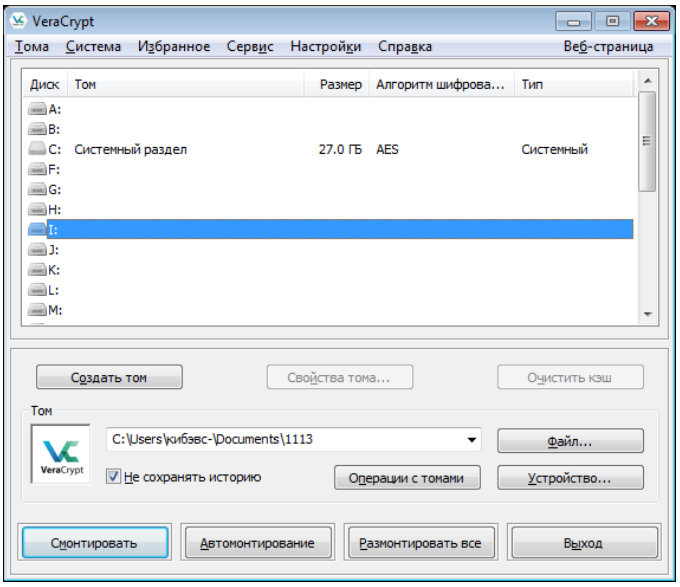

Рисунок 16 – Монтирования тома

Далее высветится окно, где необходимо выбрать ключевой файл и нажать «Ок» (рисунок 17).

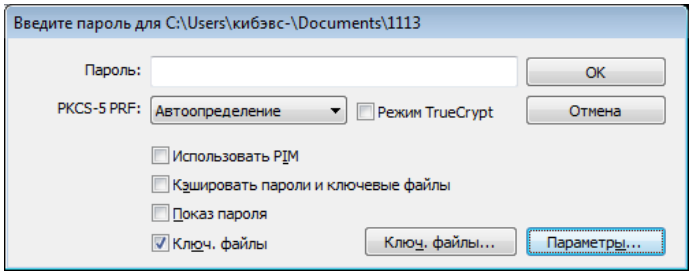

Рисунок 17 – Выбор ключевого файла

Дождитесь завершение монтирования тома. После того, как процесс завершится, диск станет доступен и его можно использовать как обычный локальный диск (рисунок 18).

Бывают ситуации, когда диск необходимо смонтировать том как сменный носитель. Для этого необходимо поставить отметку в окне параметров, нажав кнопку «Параметры» в окне ввода пароля.

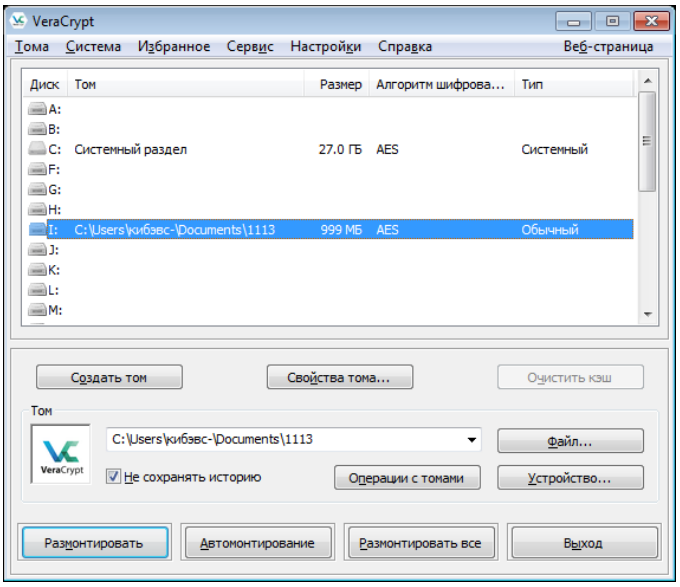

Рисунок 18 – Смонтированный раздел

После завершения работы с контейнером, его следует размонтировать в целях повышения безопасности.

Откройте ваш ключевой файл и убедитесь, что файл не был изменен.

2.2 Шифрования раздела жесткого диска

Откроем мастер томов, как и в разделе 2.1, и выберем «Зашифровать несистемный раздел/диск» (рисунок 19).

Программа может шифровать не только раздел жесткого диска или полностью жесткий диск, но и внешние накопители.

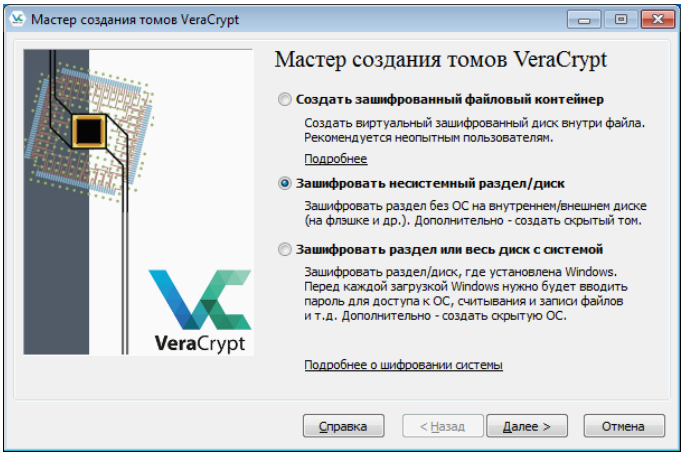

Рисунок 19 – Мастер создания томов

В этот раз выберем «Скрытый том VeraCrypt» (рисунок 20).

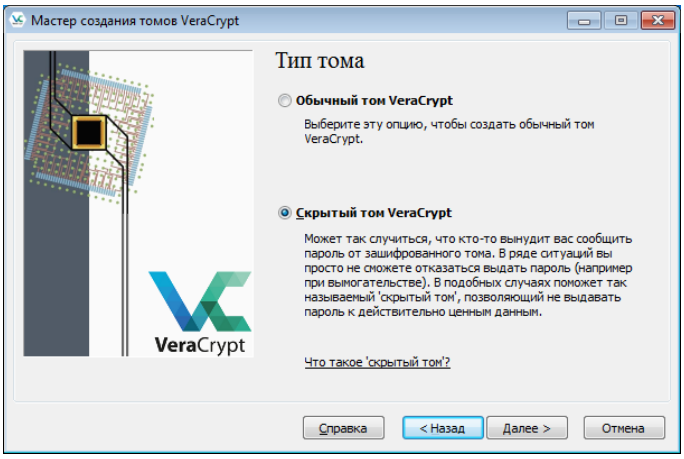

Рисунок 20 – Тип тома

Выберем обычный режим (рисунок 21).

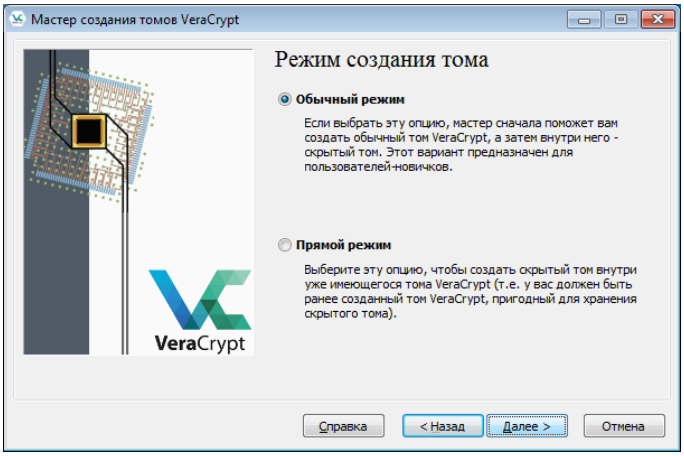

Рисунок 21 – Выбор режима

Выберем диск, который будем шифровать (рисунок 22). В нашем случаи — это диск E.

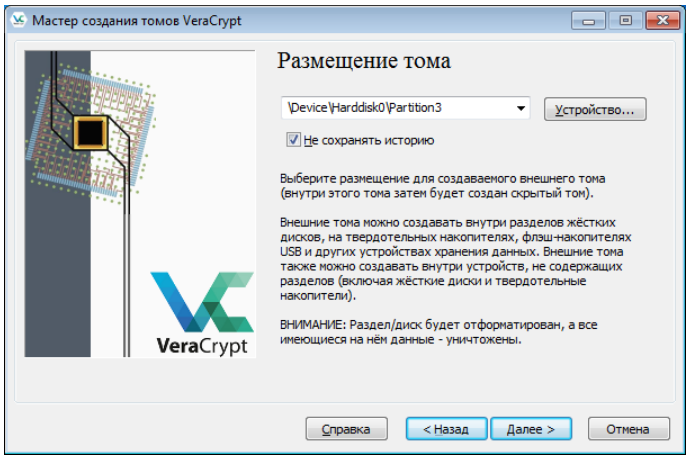

Рисунок 22 – Выбор диска

Нажмем кнопку «Далее» (рисунок 23).

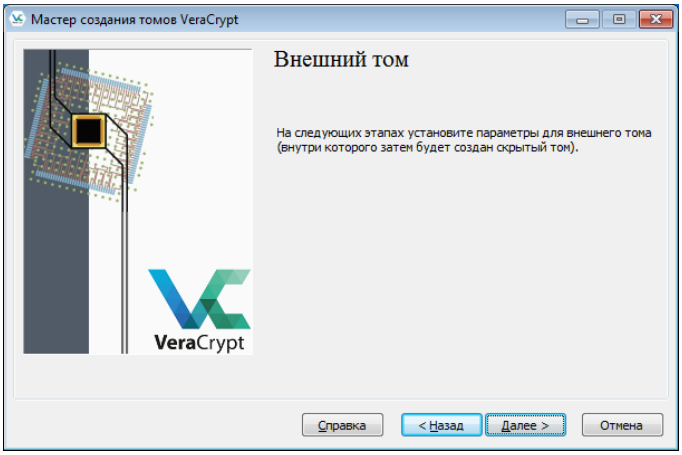

Рисунок 23 - Предупреждение

Выберем алгоритм шифрования в соответствии с вариантом и проверим алгоритм, как в пункте 2.1 (рисунок 24).

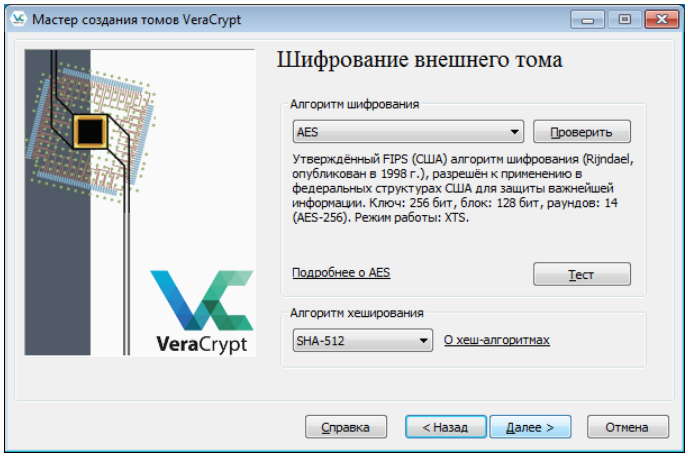

Рисунок 24 – Алгоритм шифрования

Внешний том нанимает все доступное пространство. Нажмем кнопку «Далее» (рисунок 25).

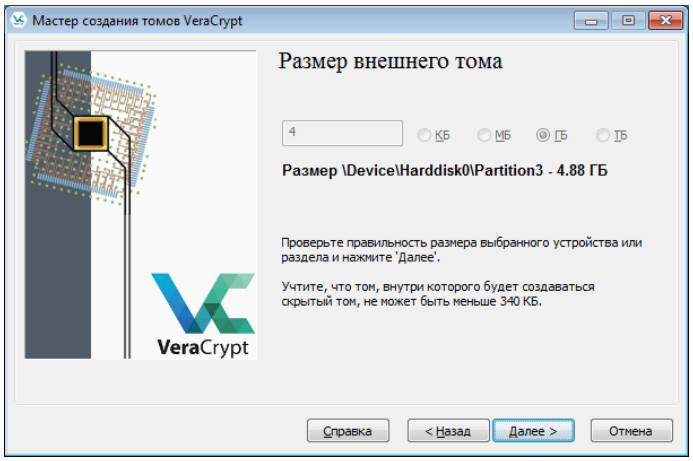

Рисунок 25 – Выбор размера тома

В этот раз введем просто пароль (рисунок 26).

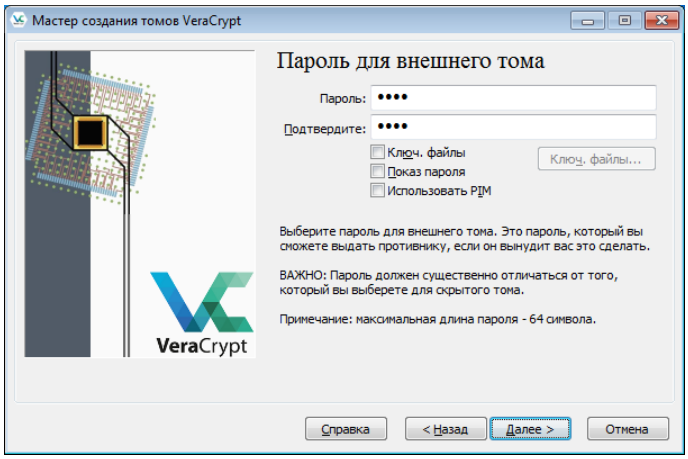

Рисунок 26 – Ввод пароля

Прочтем предупреждение и поставим отметку «Да» (рисунок 27).

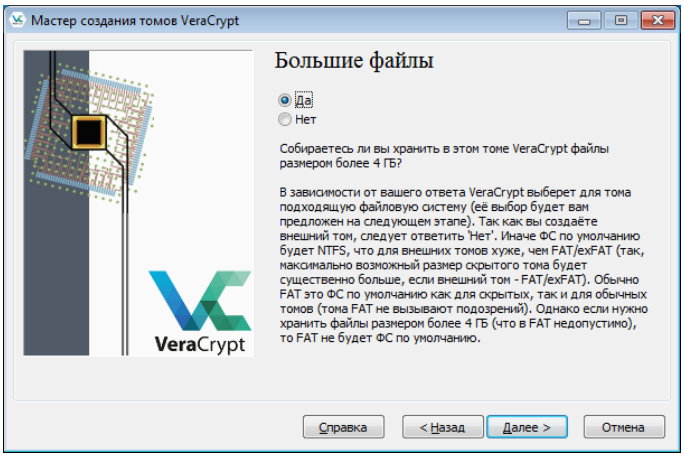

Рисунок 27 - Предупреждение

Выберите файловую систему NTFS, заполните энтропию и нажмите кнопку «Разметка» (рисунок 28).

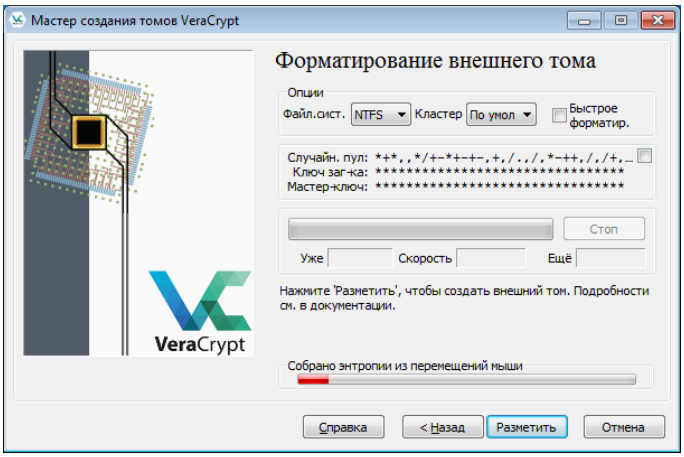

Рисунок 28 - Разметка

Прочтите предупреждение и нажмите кнопку «Да» (рисунок 29).

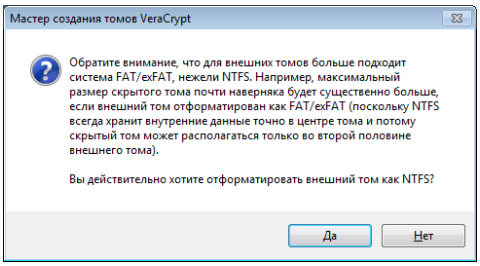

Рисунок 29 - Предупреждение

Дождитесь завершения разметки диска (рисунок 30).

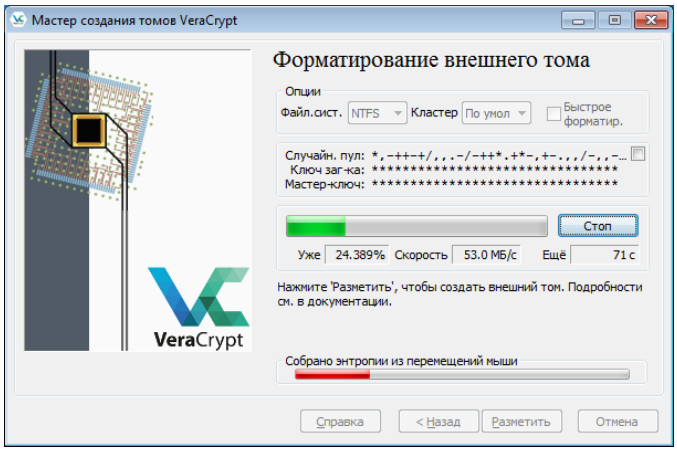

Рисунок 30 – Процесс разметки диска

После завершения разметки будет показан информационный раздел о работе с внешним томом. Нажмите кнопку «Далее» (рисунок 31).

Рисунок 31 – Информационная страница

Далее мастер создания томов предложит настроить скрытый том. Нажмите кнопку «Далее» (рисунок 32).

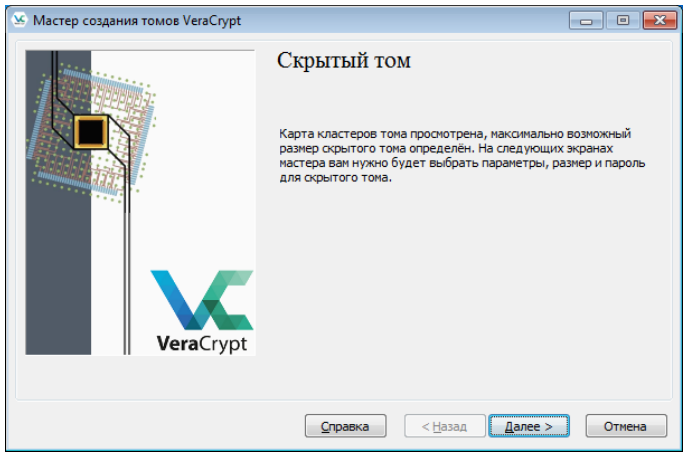

Рисунок 32 – Скрытый том

Выберите алгоритм шифрования, который выбрали для внешнего тома, и нажмите «Далее» (рисунок 33).

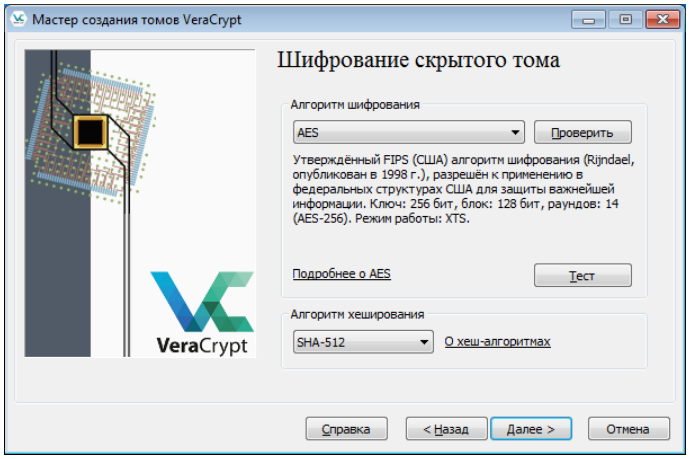

Рисунок 33 – Шифрование скрытого тома

Далее введите пароль, отличный от пароля для внешнего тома, и нажмите кнопку «Далее» (рисунок 34).

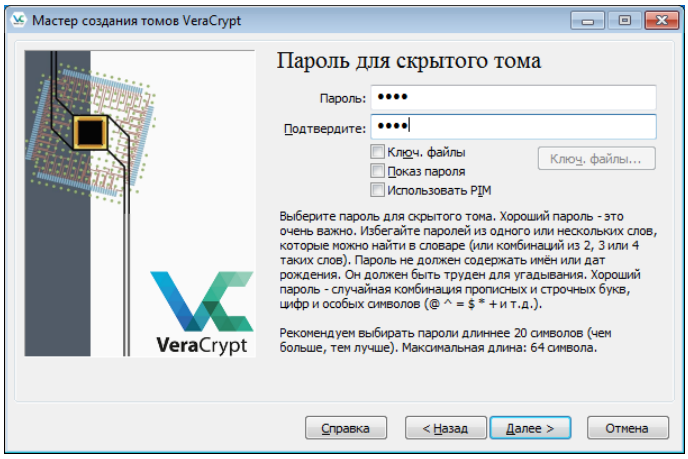

Рисунок 34 – Пароль для скрытого тома

Соберите энтропию и выполните разметку тома (рисунок 35).

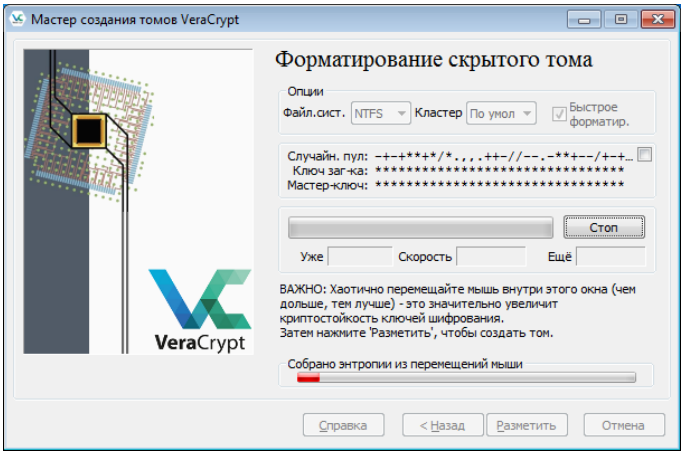

Рисунок 35 – Форматирование скрытого тома

Далее прочитайте выпадающие сообщения и согласитесь с ними. После этого будет выдано окно успешного создания скрытого тома (рисунок 36).

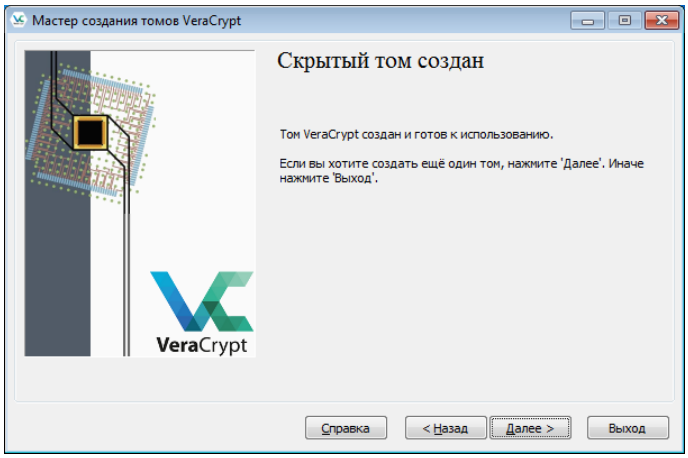

Рисунок 36 – Успешное создание скрытого тома

Работа с внешним и скрытым томом аналогична работе с файловым контейнером, но при инициализации тома необходимо ввести пароль от тома, который хотите открыть, от внешнего или скрытого.

2.3 Шифрование системного диска

В окне создания томов выберите раздел «Шифровать раздел или весь диск с системой» (рисунок 37).

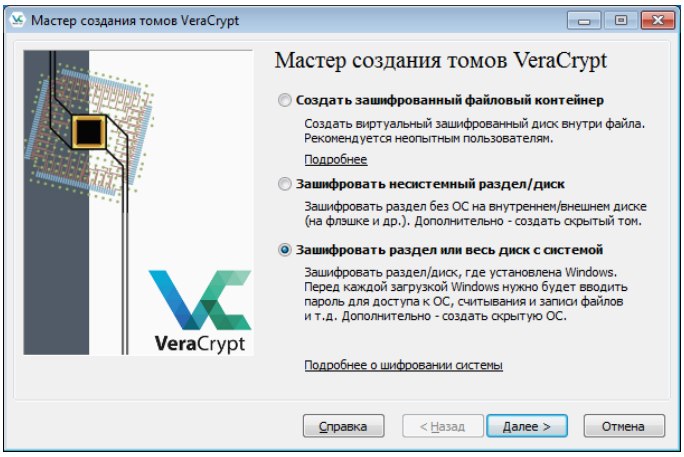

Рисунок 37 – Шифрование системного диска

Есть два типа шифрования системы – скрытый или обычный. В случаи с обычным типом системный диск будет полностью зашифрован и при загрузке компьютера будет предложено ввести пароль.

В случаи с скрытым будет создан поддельный системный раздел куда пользователь должен установить систему и загрузить неважные файлы.

Главное отличие этих двух типов в том, что если вас вынудят сообщить пароль, то вы можете сказать пароль от поддельного системного диска. В этом случаи злоумышленнику потребуется гораздо больше усилий (а может это все еще невозможно на текущий момент), чтобы понять, что существует еще одна система.

Мы выберем обычный тип шифрования (рисунок 38).

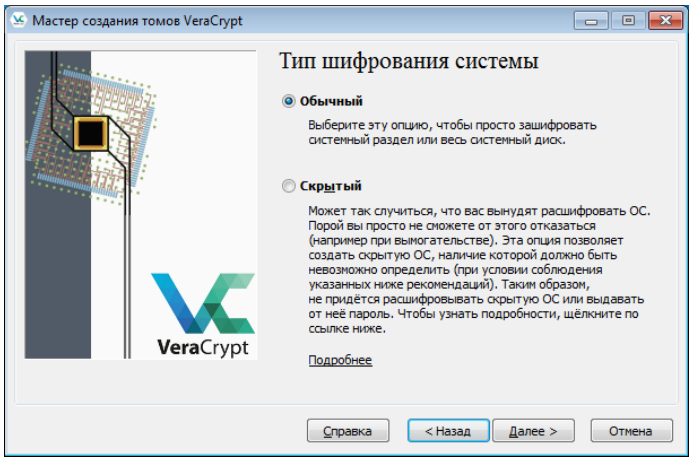

Рисунок 38 – Тип шифрования системы

Далее необходимо выбрать пункт «Зашифровать систем раздел Windows» и нажать кнопку «Далее» (рисунок 39).

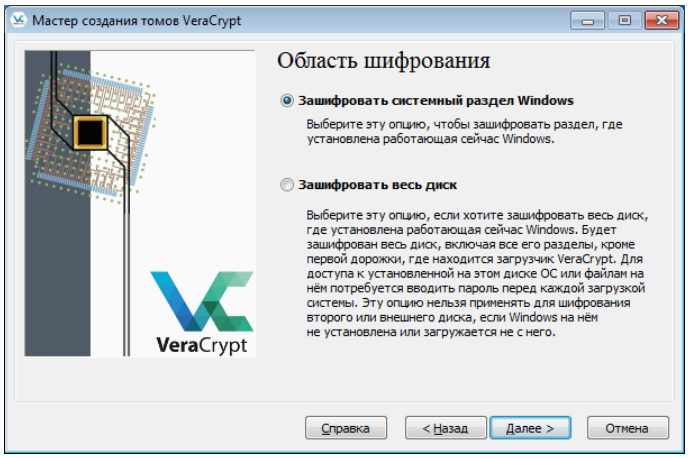

Рисунок 39 – Область шифрования

В нашем случаи установлена одна Windows, следовательно, нужно выбрать пункт «Одиночная загрузка» (рисунок 40).

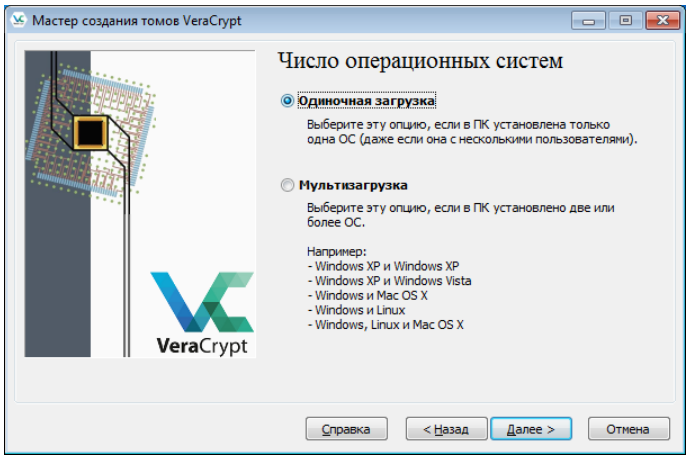

Рисунок 40 – Число операционных систем

Далее следует оставить настройки шифрования по умолчанию (рисунок 41).

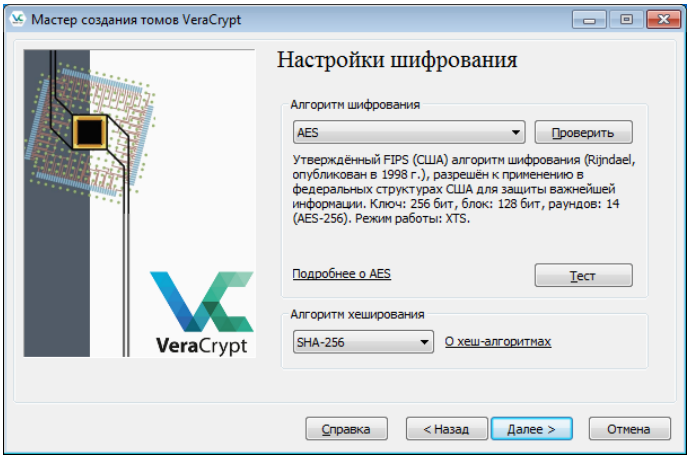

Рисунок 41 – Настройки шифрования

Поставьте галочку на пункте «Использовать PIM» и введите пароль и PIM (рисунок 42).

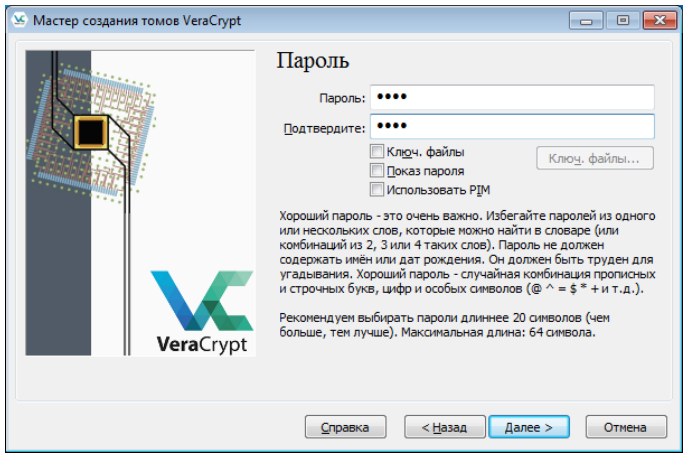

Рисунок 42 – Ввод пароля

Дайте программе собрать энтропию и нажмите кнопку «Далее» (рисунок 43).

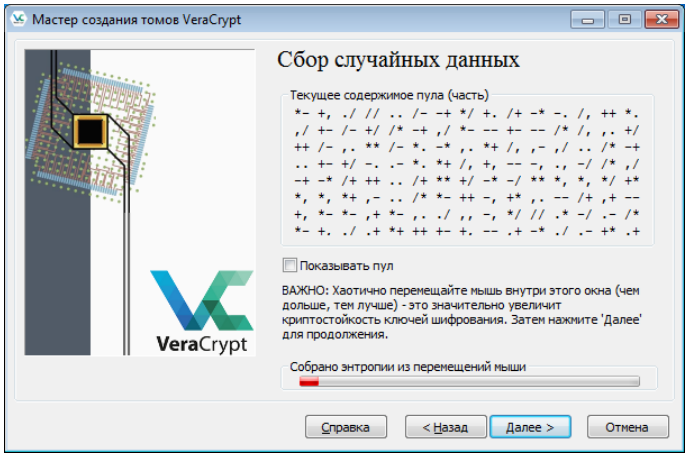

Рисунок 43 – Сбор случайных данных

В случаи успешного создания ключей, нажмите кнопку «Далее» (рисунок 44).

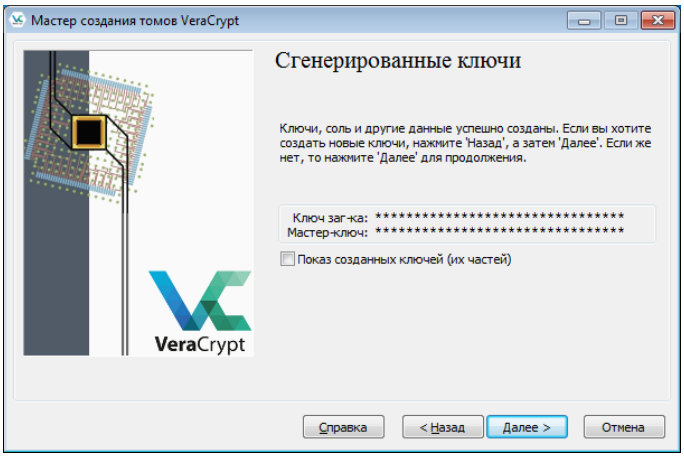

Рисунок 44 – Сгенерированные ключи

В случаи, если утрачен доступа к системе, необходимо будет предоставить диск восстановления для восстановления доступа. Рекомендуется тщательно спрятать его.

Для создания выберете путь хранения диска и нажмите «Далее» (рисунок 45).

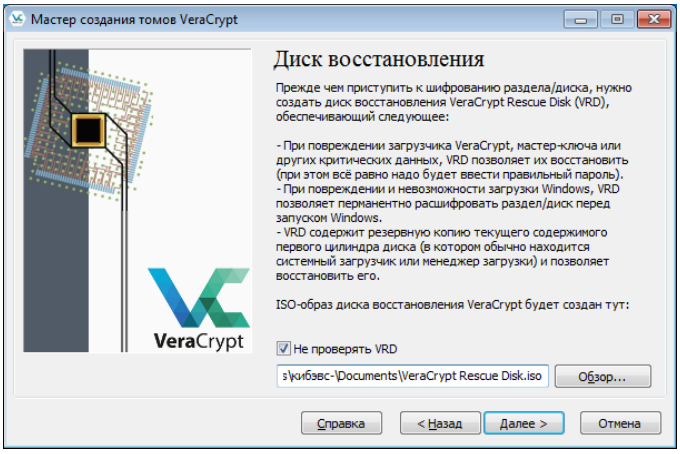

Рисунок 45 – Создания диска восстановления

После успешного создания диска восстановления будет показано соответствующее окно, где будет предложено прожечь диск восстановления на компакт-диск. Нажмите кнопку «Далее» (рисунок 46).

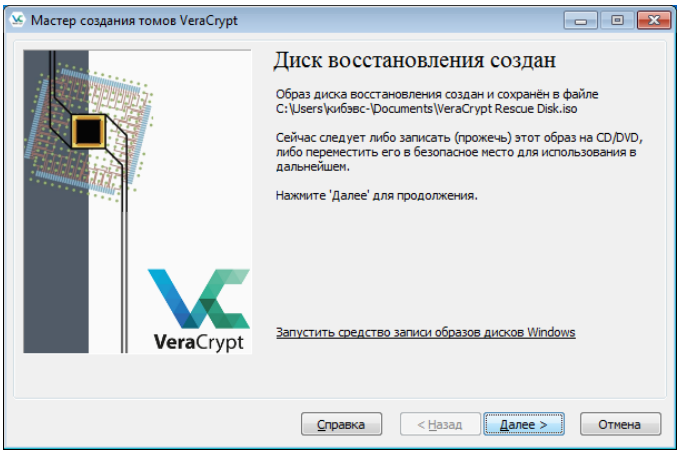

Рисунок 46 – Успешное создание образа восстановления

Внимательно ознакомьтесь с предупреждением и нажмите кнопку «Да» (рисунок 47).

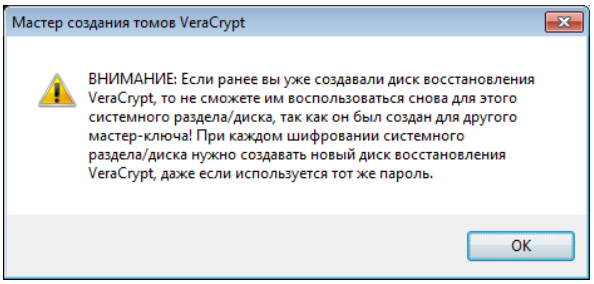

Рисунок 47 – Предупреждение

Следующим шагом будет выбор режима очистки диска. Очистка необходима в связи с особенностью хранения информации на диске. При удалении какого-либо файла с диска, фактически он не удаляется, а обнуляются только указатели на этот файл. Процедура очистки заключается в многократной перезаписи псевдослучайной информации в ячейки памяти жесткого (или какого-либо другого) диска, что затрудняет считывание остаточной незашифрованной информации с диска. Следовательно, если не провести эту процедуру, то физически на диске останутся незашифрованные данные.

В нашем случаи необходимо отказаться от очистки, выбрав из выпадающего меню пункт «Нет» (рисунок 48).

Следует учесть, что сейчас очень популярны SSD накопители. Они имеют меньше циклов записи. В связи с этим стоит подумать, нужно ли вам выполнять эту процедуру, если, например, была переустановлена ОС, но до

этого системный диск был зашифрован программой VeraCrypt и доступ не был скомпрометирован.

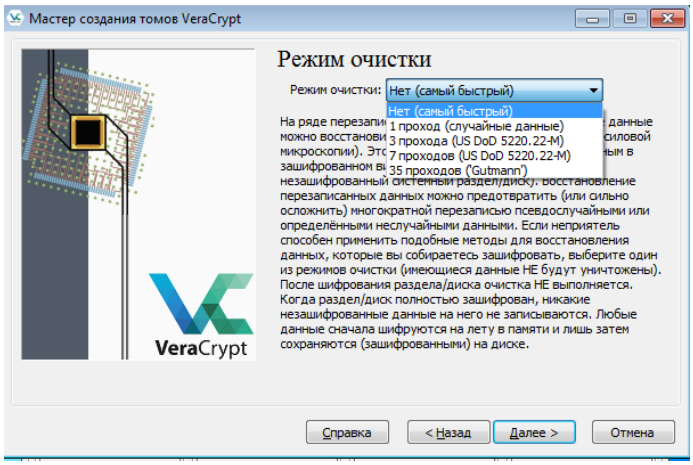

Рисунок 48 – Режим очистки

Следующим шагом необходимо провести тестирование на ошибки, которые могут возникнуть во время шифрования. Нажмите кнопку «Тест» (рисунок 49) и прочитайте предупреждение. Нажмите кнопку «Да» в окне предупреждения (рисунок 50).

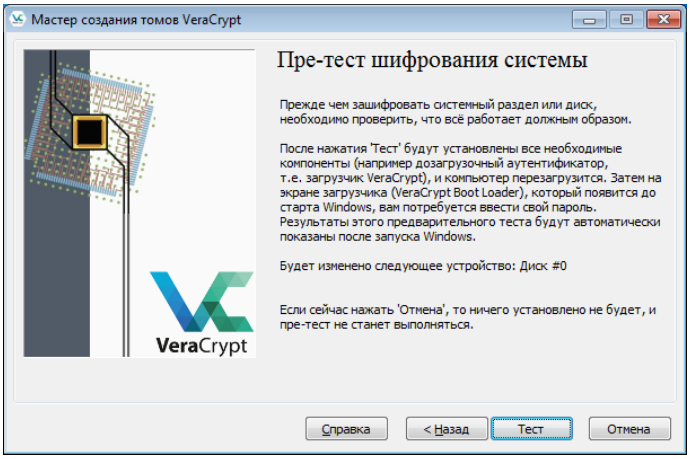

Рисунок 49 – Пре-тест

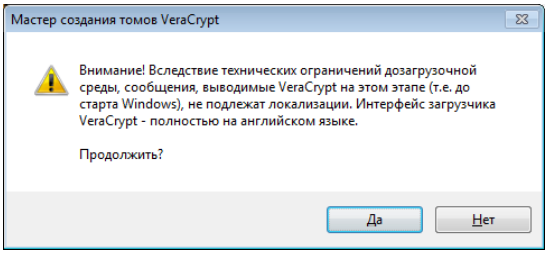

Рисунок 50 – Предупреждение

Прочитайте информационное сообщение и нажмите кнопку «ОК» (рисунок 51).

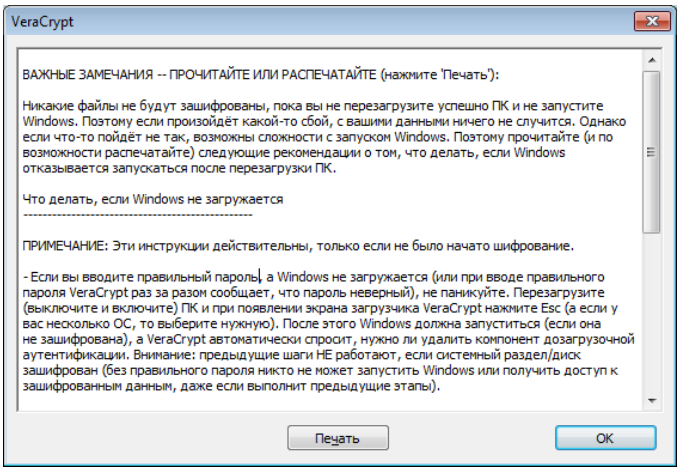

Рисунок 51 – Информационное сообщение

Выполните перезагрузку нажав кнопку «Да» (рисунок 52).

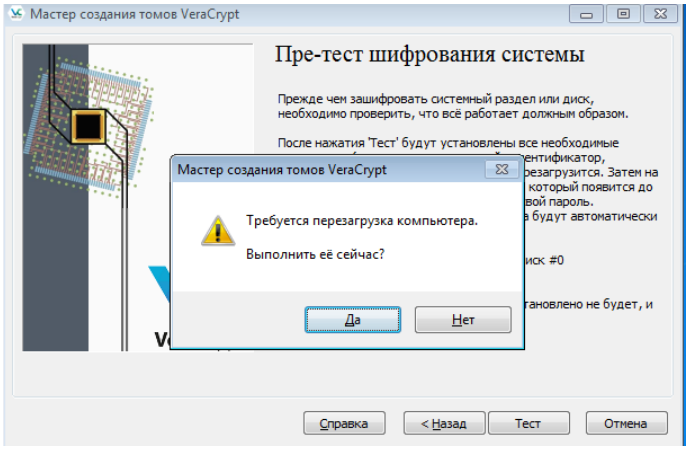

Рисунок 52 – Перезагрузка

В окне, показанном на рисунке 53, введите пароль и PIM от системы шифрования.

Рисунок 53 – Ввод паролей

Дождитесь, пока система не загрузится (рисунок 54).

Вам будет казаться, что все подвисло и ничего не работает, но это не так. Обязательно дождитесь загрузки системы или ошибки.

Рисунок 54 – Пароли введены

После того, как система будет загружена, появится сообщение о успешном прохождении пре-теста. Прочитайте информационное сообщение и нажмите на кнопку «Шифрация» (рисунок 55).

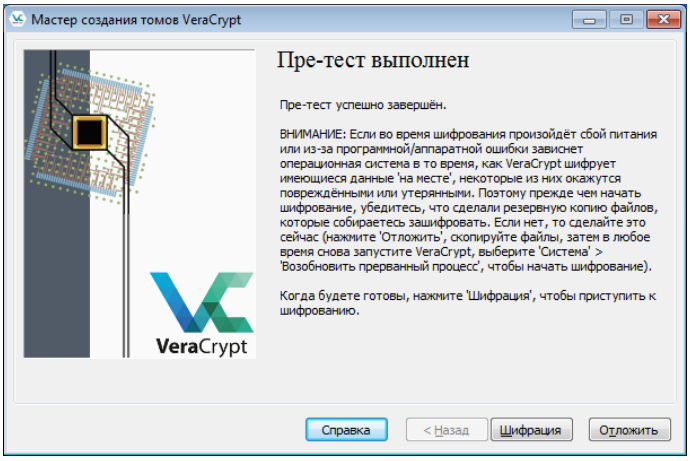

Рисунок 55 – Успешное выполнение пре-теста

Шифрование может занять некоторое время. Обязательно дождитесь окончания этого процесса (рисунок 56).

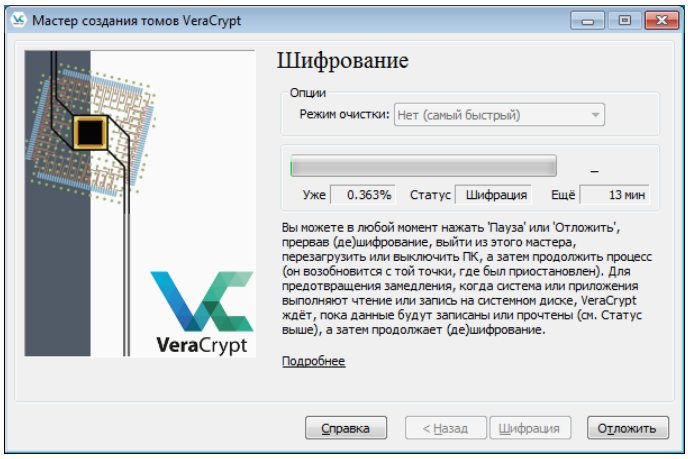

Рисунок 56 – Процесс шифрования системного диска

После успешного шифрования будет выдано соответствующее сообщение (рисунок 57).

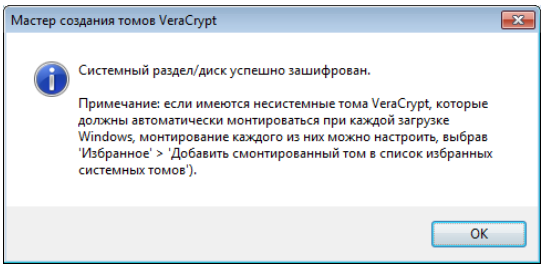

Рисунок 57 – Успешное шифрование системного диска

Перезагрузитесь, введите пароль и PIM (рисунок 58).

Рисунок 58 – Введенный пароль и PIM

Откройте программу VeraCrypt и посмотрите, как отображается в ней диск C (рисунок 59).

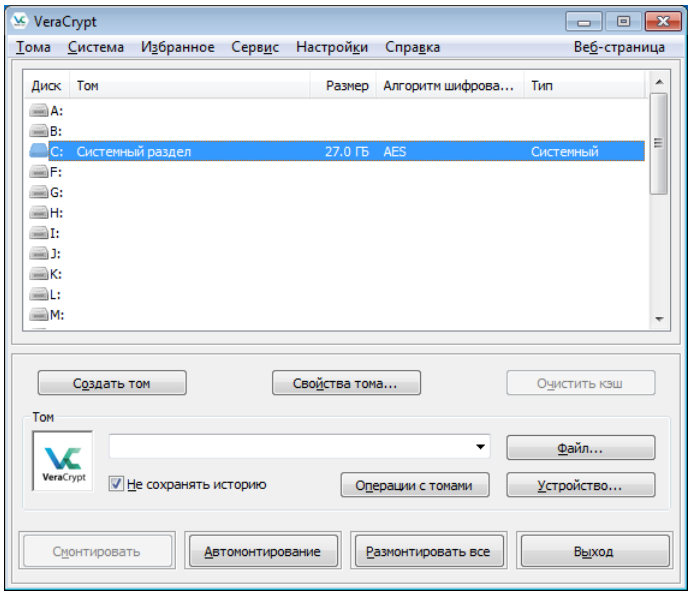

Рисунок 59 – Отображение диска C в программе

3 Варианты

Вариант	Файловый контейнер	Шифрование диска
1	AES	AES(Twofish)
2	Serpent	AES(Whofish(Serpent))
3	Twofish	Camellia
4	Camellia	Kuznyechik
5	Kuznyechik	Serpent
6	AES(Twofish)	Twofish
7	AES(Whofish(Serpent))	AES
8	Serpent(AES)	Kuznyechik(Serpent(Camellia))
9	Twofish(Serpent)	Camellia(Serpent)
10	Camellia(Kuznyechik)	Kuznyechik(AES)
11	Kuznyechik(Twofish)	Camellia(Kuznyechik)
12	Camellia(Serpent)	Kuznyechik(Twofish)
13	Kuznyechik(AES)	Serpent(AES)
14	Kuznyechik(Serpent(Camellia))	Twofish(Serpent)

Контрольные вопросы

1. Что такое файловый контейнер?
2. Чем отличается скрытый том от обычного?
3. Какой алгоритм шифрования, на ваш взгляд, предпочтительнее?
4. Для чего необходима очистка диска при шифровании системного диска?
5. Как подключить зашифрованный диск (системный, локальный том, файловый контейнер)?
6. Что такое PIM?
7. Какие плюсы и минусы использования ключевых файлов?
8. Что такое скрытая ОС?
9. Что будет, если в обычный записать сильно много информации и в скрытый? Как это на них отразится?