Частное учреждение образования

Колледж бизнеса и права

|  |
| --- |
| УТВЕРЖДАЮ  Ведущий методист колледжа  \_\_\_\_\_\_\_\_\_\_\_Е.В. Паскал  «\_\_\_» 2023 |
| Специальность: 2-40 01 01 «Программное обеспечение информационных технологий» | Учебная дисциплина: «Защита компьютерной информации» | |

# Лабораторная работа №16

Инструкционно-технологическая карта

Тема: Защита программ от несанкционированной эксплуатации и копирования при помощи специальных ПС

Цель: научиться защищать программы от несанкционированной эксплуатации и копирования при помощи специальных ПС. Научиться шифровать флеш-накопитель.

Время выполнения: 2 часа.

СОДЕРЖАНИЕ РАБОТЫ

1. Теоретические сведения для выполнения работы
2. Практические задания
3. Контрольные вопросы
4. Литература
5. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

## Аппаратное и программного шифрование

В случае с флеш-накопителями (а также HDD и SSD) для осуществления аппаратного шифрования данных используется специальный чип, расположенный на печатной плате устройства. В него встроен генератор случайных чисел, который создает ключи шифрования. Данные шифруются автоматически и мгновенно дешифруются при вводе пользовательского пароля. В этом сценарии получить доступ к данным без пароля практически невозможно.

При использовании программного шифрования “блокировка” данных на накопителе обеспечивается внешним программным обеспечением, которое выступает в роли бюджетной альтернативы аппаратным методам шифрования. Недостатки такого ПО могут заключаться в банальном требовании регулярных обновлений, чтобы предлагать устойчивость к постоянно улучшающимся методикам взлома. К тому же для дешифровки данных используются мощности компьютерного процесса (а не отдельного аппаратного чипа), и, по сути, уровень защиты ПК определяет уровень защиты накопителя.

Главная же особенность накопителей с аппаратным шифрованием заключается в отдельном криптографическом процессоре, наличие которого говорит нам о том, что ключи шифрования никогда не покидают USB-накопитель, в отличие от программных ключей, которые могут временно храниться в оперативной памяти компьютера или на жестком диске. А поскольку программное шифрование использует память ПК для хранения количества попыток входа в систему, оно не может остановить атаки грубой силы на пароль или ключ. Счетчик попыток входа может постоянно сбрасываться злоумышленником до тех пор, пока программа автоматического взлома паролей не найдет нужную комбинацию.

Дело в том, что в этом случае программа шифрования хранится в памяти флеш-накопителя, и это делает ее более уязвимой для атак.

Как итог: программный подход не обеспечивает настолько же высокий уровень безопасности, как AES-шифрование. Это, скорее, базовая защита. С другой стороны – программное шифрование важных данных все же лучше, чем вообще отсутствие шифрования. И этот факт позволяет нам четко разграничить эти типы криптографии: аппаратное шифрование флеш-накопителей – необходимость, скорее, для корпоративного сектора (например, когда сотрудники компании пользуются накопителями, выданными на работе); а программное – больше подходит для пользовательских нужд.

Возьмем к примеру флешку Kingston:

Kingston использует 256-битное аппаратное шифрование AES-XTS (с использованием дополнительного полноразмерного ключа) для всех своих безопасных накопителей. Как мы уже отметили выше, флешки содержат в своей компонентной базе отдельный чип для шифровки и дешифровки данных, который выступает в роли постоянно активного генератора случайных чисел.

Когда вы подключаете устройство к USB-порту в первый раз, мастер настройки инициализации предлагает вам задать мастер-пароль для доступа к устройству. После активации накопителя алгоритмы шифрования автоматически начнут свою работу в соответствии с пользовательскими предпочтениями.

При этом для пользователя принцип работы флеш-накопителя останется неизменным – он по-прежнему сможет скачивать и размещать файлы в памяти устройства, как при работе с обычной USB-флешкой. Единственное отличие заключается в том, что при подключении флешки к новому компьютеру вам потребуется вводить установленный пароль для получения доступа к своей информации.

Флешки с аппаратным шифрованием

Для организаций, в которых конфиденциальные данные являются частью бизнеса, (будь то финансовые, медицинские или государственные учреждения), шифрование является наиболее надежным средством защиты. В этом плане флеш-накопители с поддержкой 256-битного аппаратного шифрования AES – масштабируемое решение, которое может использоваться любыми компаниями: от частных лиц и малых предприятий до крупных корпораций, а также военных и правительственных организаций. Если рассматривать этот вопрос немного конкретнее, использование зашифрованных USB-накопителей необходимо:

* для обеспечения безопасности конфиденциальных данных компании
* для защиты информации о клиентах
* для защиты компаний от потери прибыли и лояльности клиентов

Текущий стандарт FIPS 140-2 определяет четыре различных уровня безопасности, которым могут соответствовать флеш-накопители. Первый уровень обеспечивает умеренный набор функций безопасности. Четвертый уровень – подразумевает строгие требованиями к самозащите устройств. Уровни два и три обеспечивают градацию этих требований и образуют некую золотую середину.

Первый уровень безопасности: для USB-накопителей, сертифицированных на первом уровне, предполагается использование хотя бы одного алгоритма шифрования или же иной функции обеспечения безопасности.

Второй уровень безопасности: здесь от накопителя требуется не только обеспечение криптографической защиты, но и фиксация несанкционированных вторжений на микропрограммном уровне, если кто-то попытается открыть накопитель.

Третий уровень безопасности: предусматривает предотвращение взломов посредством уничтожения «ключей» шифрования. То есть требуется наличие ответной реакции на попытки проникновения. Также третий уровень гарантирует более высокий уровень защиты от электромагнитных помех: то есть считать данные с флешки, используя беспроводные устройства взлома не получится.

Четвертый уровень безопасности: самый высокий уровень, который предполагает полную защиту криптографического модуля, которая обеспечивает максимальную вероятность обнаружения и противодействия на любые попытки несанкционированного доступа со стороны постороннего пользователя. Флешки, получившие сертификат четвертого уровня включают в себя в том числе и такие опции защиты, которые не позволяют произвести хакинг посредством изменения напряжения и температуры окружающей среды.

Как зашифровать флешку в VeraCrypt

ВераКрипт — это бесплатный инструмент шифрования с открытым исходным кодом. Это форк легендарной утилиты TruCrypt, в которой были обнаружены уязвимости, позволяющие взломать шифрование. Для устранения этих уязвимостей и была создана ВераКрипт.

**Для шифрования флешки с помощью VeraCrypt потребуется:**

ПК с оперативной памятью не менее 4 ГБ.

Файл установки VeraCrypt.

USB-накопитель.

Это короткая инструкция, в которой я не буду объяснить все пункты, а лишь покажу на что нажать. Разбор всех настроек ВераКрипт вы найдете в статье «[Правильное использование VeraCrypt](https://spy-soft.net/veracrypt-security/)». Рекомендуется прочитать статью, если собираетесь хранить на зашифрованном носителе важную, конфиденциальную информацию.

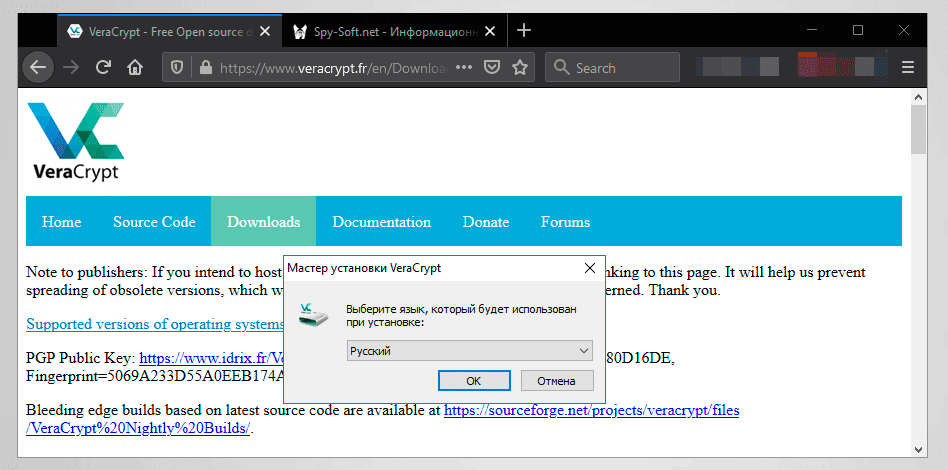
Итак, приступим к установке и шифрованию флешки с помощью ВераКрипт.

Скачивание VeraCrypt

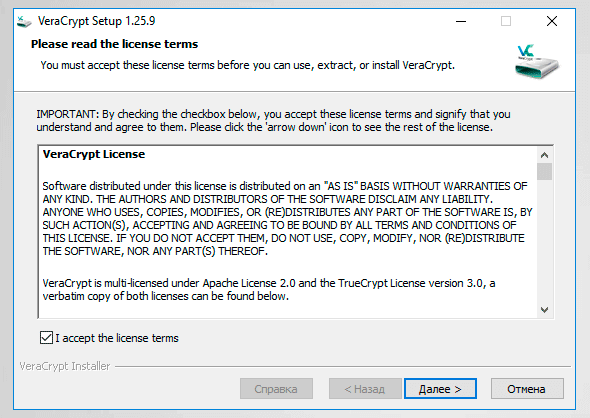
Перейдите на [официальный сайт](официальный%20сайт) (<https://veracrypt.ru/skachat-veracrypt>) VeraCrypt и скачайте файл установки соответствующий вашей операционной системе.

Установка VeraCrypt

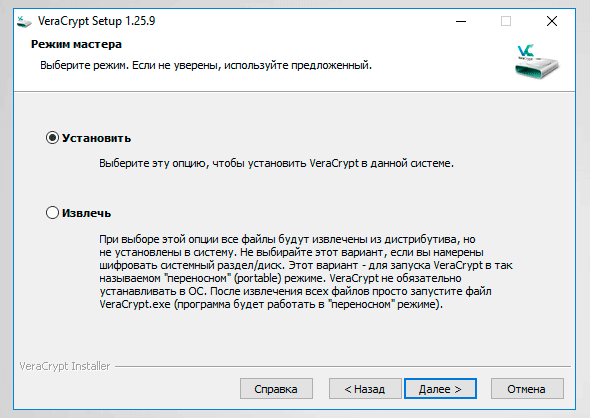
Выберите язык



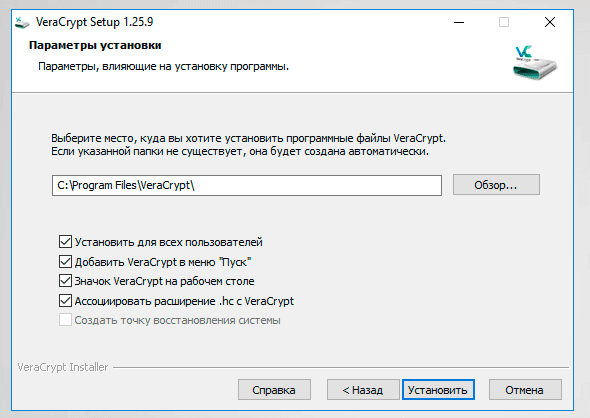
Согласитесь с условиями использования и нажмите «Далее».



Выберите режим установки. Первый вариант установит VeraCrypt в систему. Второй вариант — позволяет использовать VeraCrypt в режиме портеэйбл (запуск программы без установки). Отметьте первое.



Следующие настройки можете изменить на свое усмотрение. В конце нажмите «Установить».

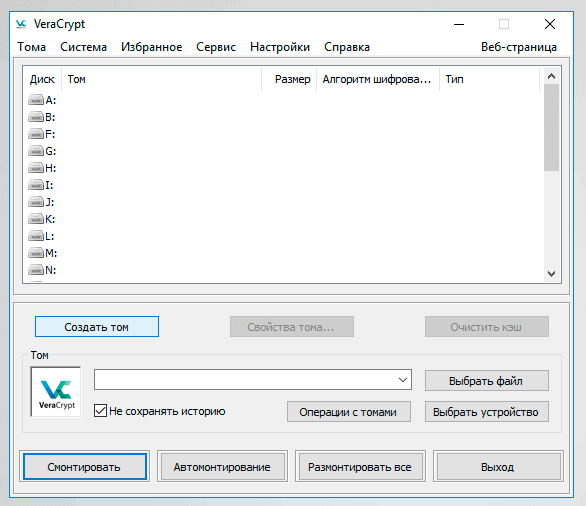


Вы установили VeraCrypt. Давайте перейдем к созданию зашифрованной флешки.

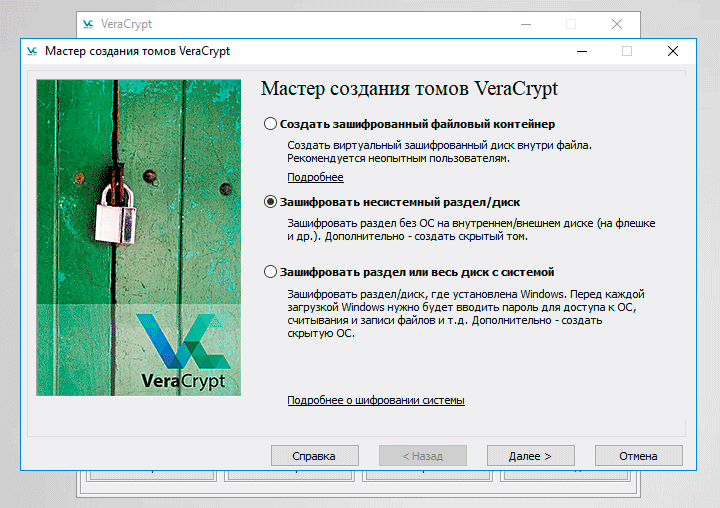
**Перед шифрованием флешки рекомендую еще раз убедится, что на флешке нет важных для вас файлов.**

Создание зашифрованной флешки в VeraCrypt

Нажмите на кнопку «Создать том».

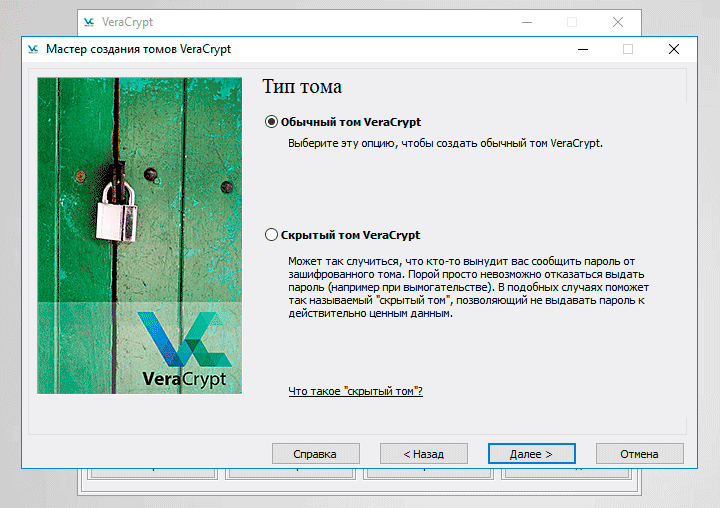


Для создания зашифрованной флешки, выберите пункт «Зашифровать несистемный раздел / диск»

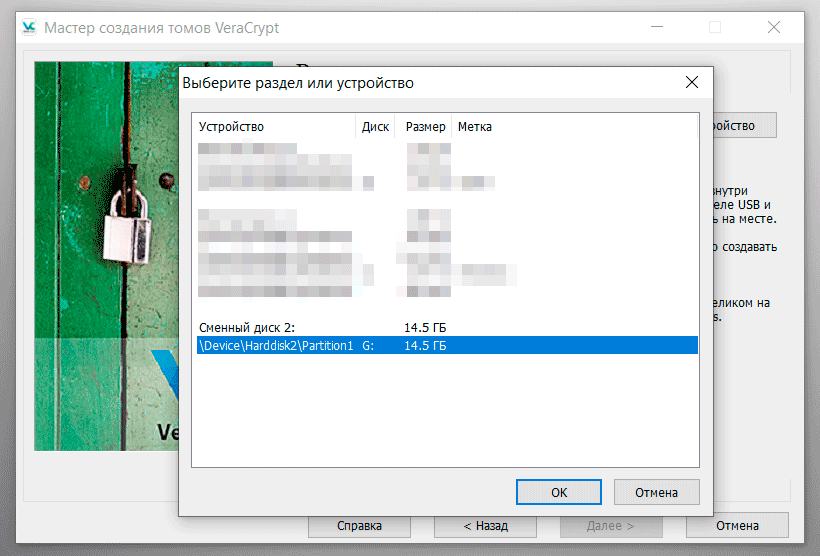


Нажмите «Далее» и разрешите установку драйвера ВераКрипт.

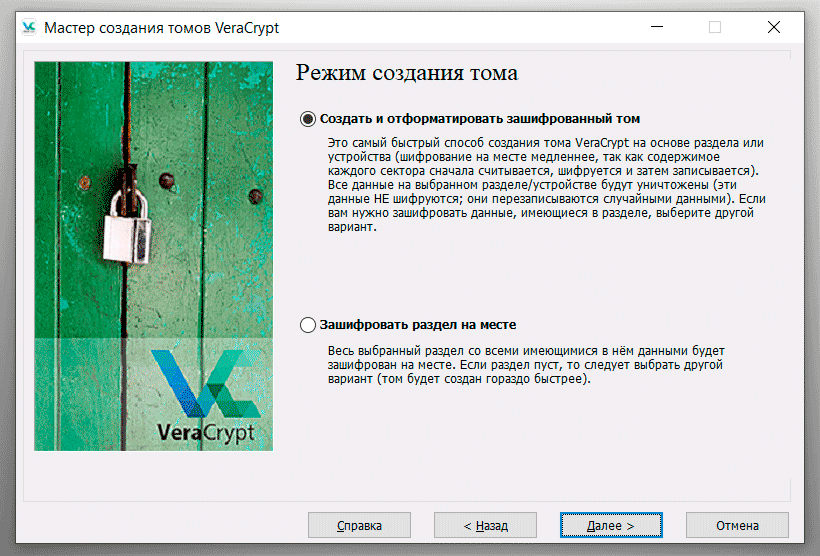
Выберите «Обычный том VeraCrypt» и нажмите «Далее».



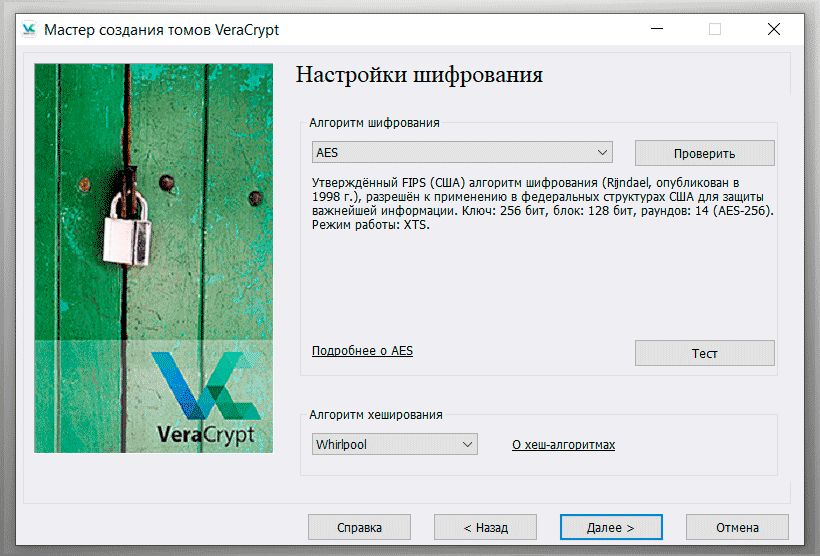
Теперь нужно выбрать расположение тома. Отметьте флешку, которую следует зашифровать и нажмите «ОК».



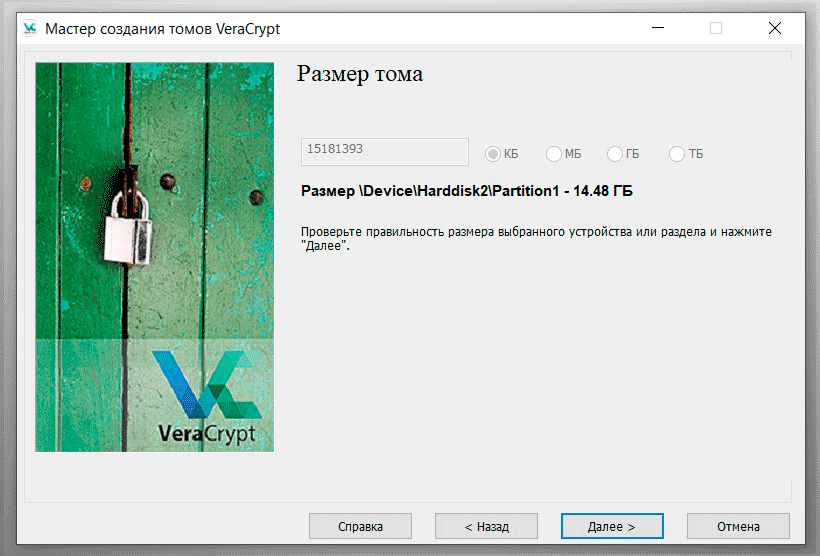
Отметьте первый пункт «Создать и отформатировать зашифрованный том» и нажмите «Далее».



Теперь необходимо выбрать алгоритм шифрования и алгоритм хеширования. Я рекомендую выбрать алгоритм шифрования AES и алгоритм хеширования Whirlpool.

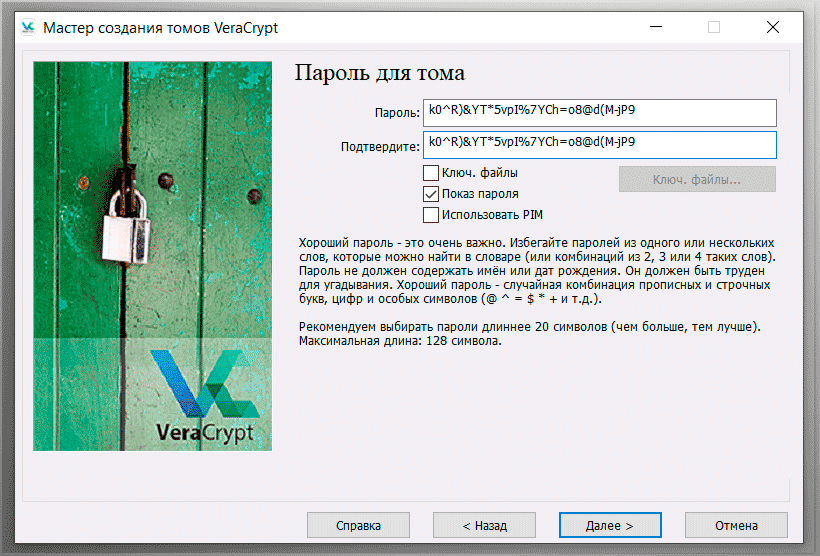


Подтвердите размер зашифрованного тома нажав на кнопку «Далее».

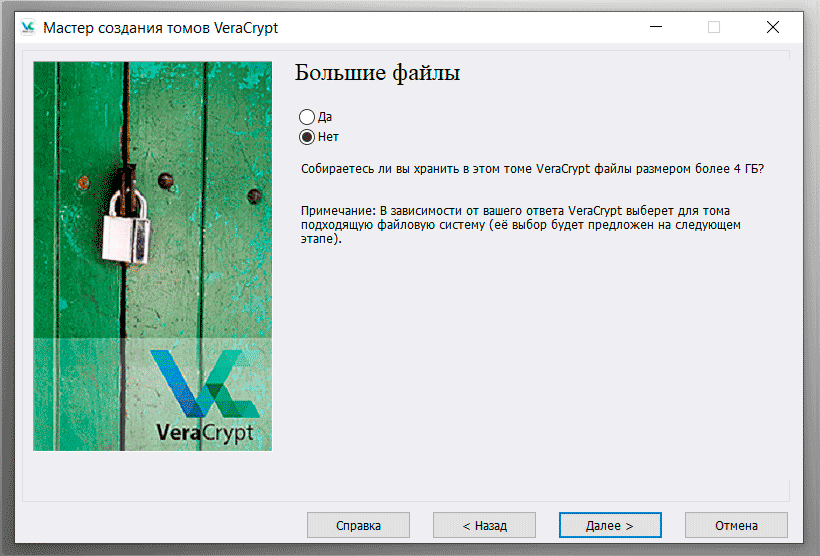


**Установка пароля тома**

Это важный шаг в шифровании флешки. Вы должны использовать надежный пароль

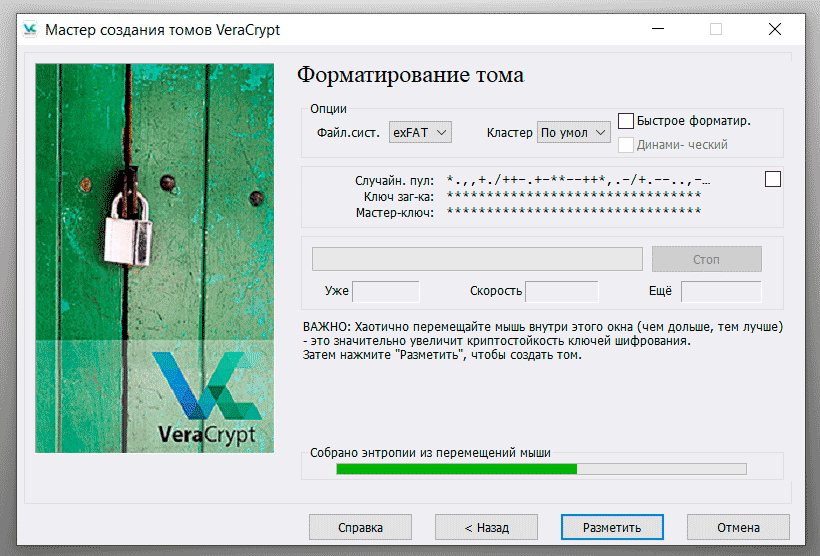


Если вы собираетесь использовать том для хранения файлов размером более 4 ГБ, тогда отметьте первый.



**Форматирование тома**

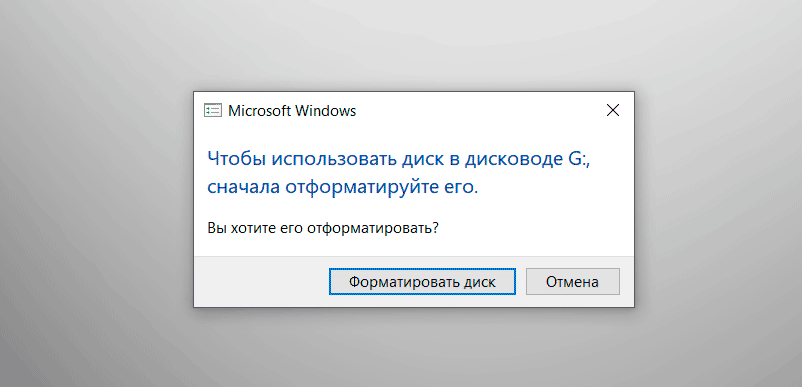
Начните хаотично перемещать курсор мышки внутри окна. В выпадающем меню выберите пункт «exFAT» и нажмите «Разметить», чтобы начать шифрование флешки.



Если на флешке находятся файлы, вы увидите предупреждение.

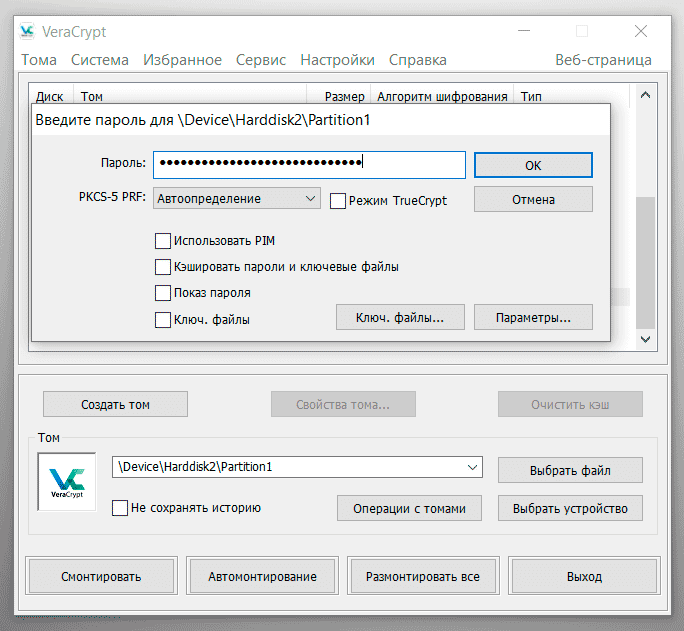
**Монтирование зашифрованной флешки**

Вы зашифровали флешку. Теперь при попытке использования флешки, вы увидите сообщение об ошибке, с предложением отформатировать флешку. Форматировать конечно нельзя.

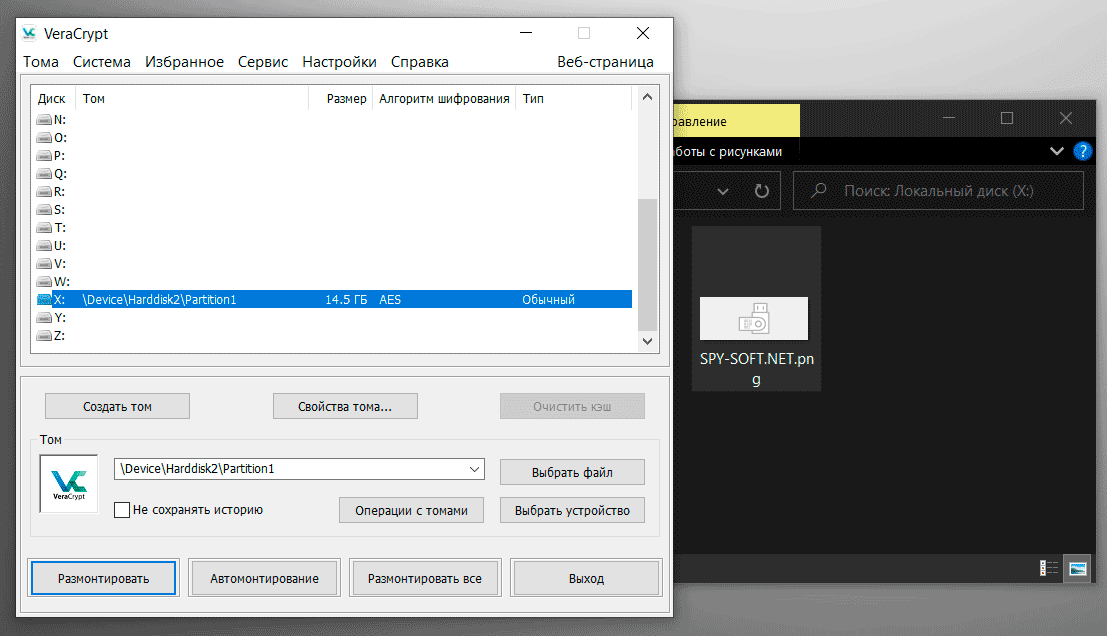


Попробуем смонтировать (сделать доступной для использования т.е. расшифровать) зашифрованную флешку.

Откройте VeraCrypt и нажмите на «Выбрать устройство». В появившемся окне введите пароль, который был использован ранее.



При использовании верного пароля, после нескольких секунд появится содержимое флешки.



Теперь вы можете работать с файлами, а после завершения нажав на кнопку «Размонтировать» заблокировать доступ к файлам на носителе.

1. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

С помощью реализованного приложения выполнить задания, описанные выше.

1. КОНТРОЛЬНЫЕ ВОПРОСЫ:
2. Какие преимущества имеют флеш-накопители с аппаратным шифрованием данных перед программным шифрованием?
3. Какие недостатки программного шифрования данных на флеш-накопителях и почему аппаратное шифрование считается более безопасным?
4. Зачем нужны флешки с аппаратным шифрованием?
5. Чем аппаратное шифрование отличается от программного?
6. Назовите четыре уровня безопасности флеш-накопители.

4. ЛИТЕРАТУРА

1. Андресс Д. Защита данных. От авторизации до аудита – Питер, 2021.
2. Козлов С. Защита информации, устройства несанкционированного съема информации и борьба с ними - Академический проект, 2019.
3. М.В. Баранова и В.В. Кучеренко. Шифрование данных в информационных системах
4. Р.Х. Адам "Шифрование в информационных системах. Теория и практика"
5. А.А. Данилов, С.А. Копылова, И.В. Михайлов. Защита информации в компьютерных системах и сетях"
6. У. Столлингс. Шифрование и криптография.

Преподаватель Д.А. Бунькевич

Рассмотрено на заседании цикловой комиссии

программного обеспечения информационных технологий

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_ К.О.Якимович