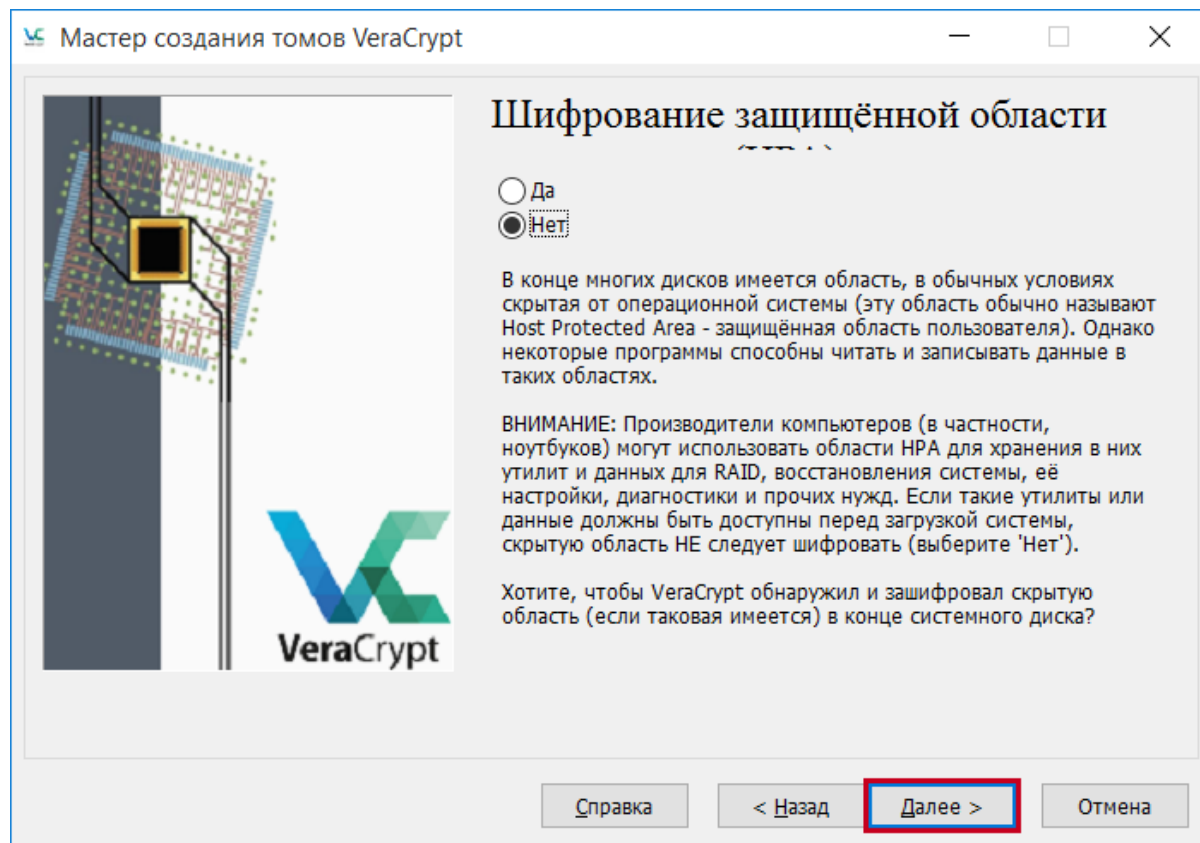


Полное шифрование диска

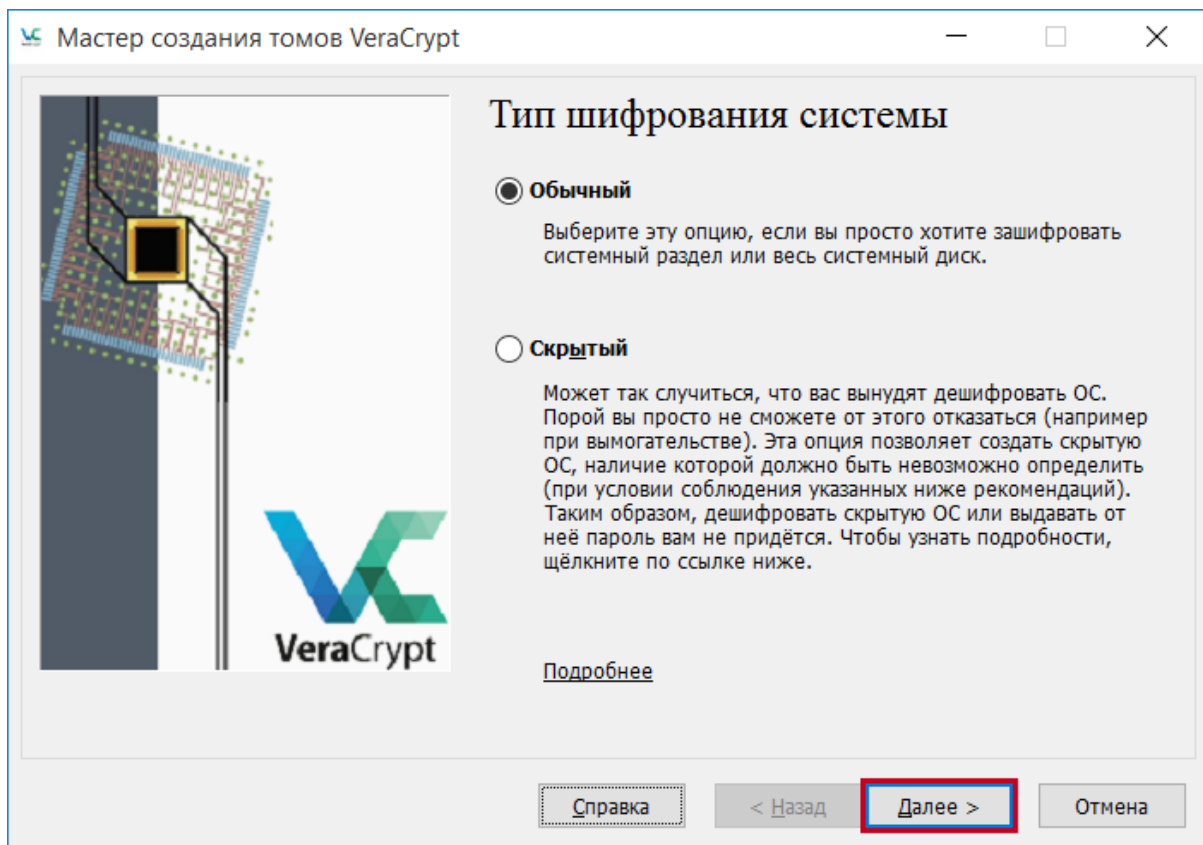
Сегодня нам понадобится утилита VeraCrypt. Если вы её ещё не скачали, скачайте её со страницы загрузки на [официальном сайте](#). Ставим обычную версию(не portable)

Запустите VeraCrypt, в главном окне программы перейдите на вкладку System (Система) и выберите первый пункт меню Encrypt system partition/drive (Зашифровать системный раздел/диск).



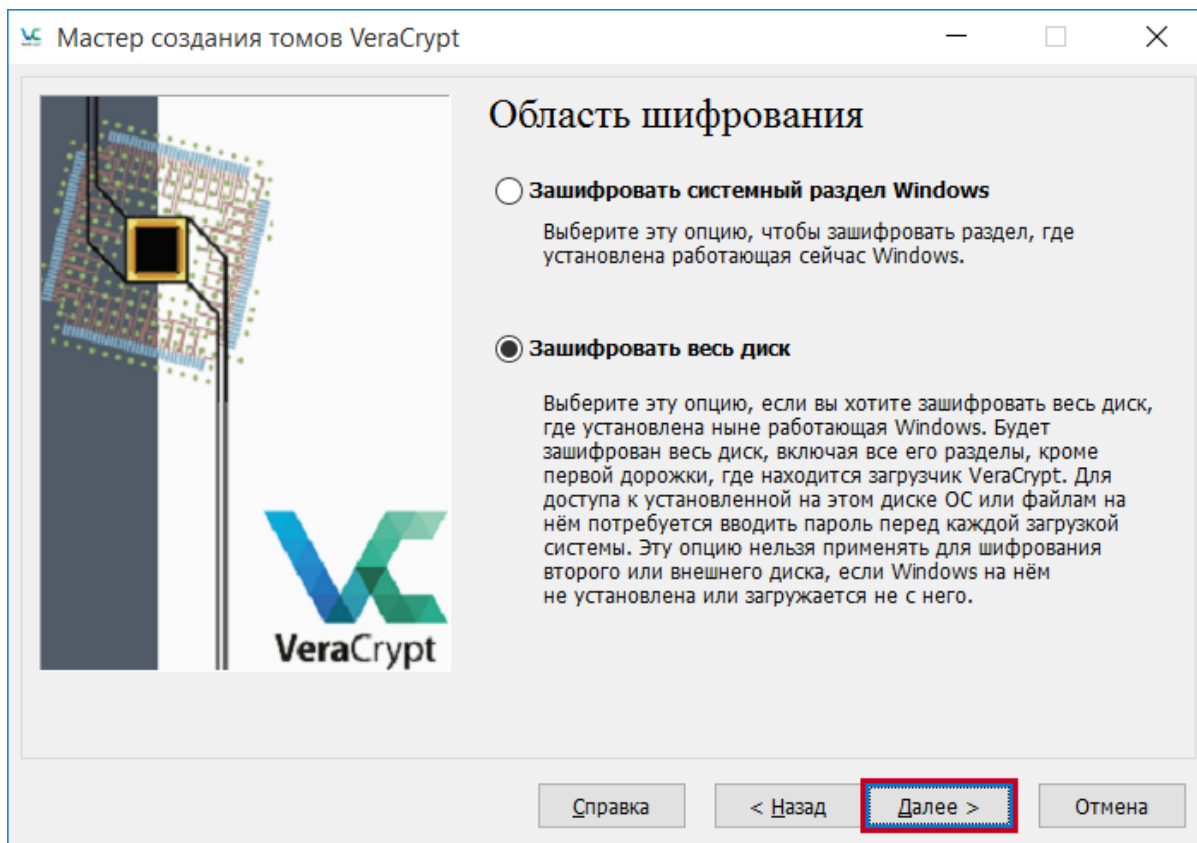
Выбор типа шифрования

Оставьте установленный по умолчанию тип Normal (Обычный). Нажмите Next (Далее)



Область шифрования

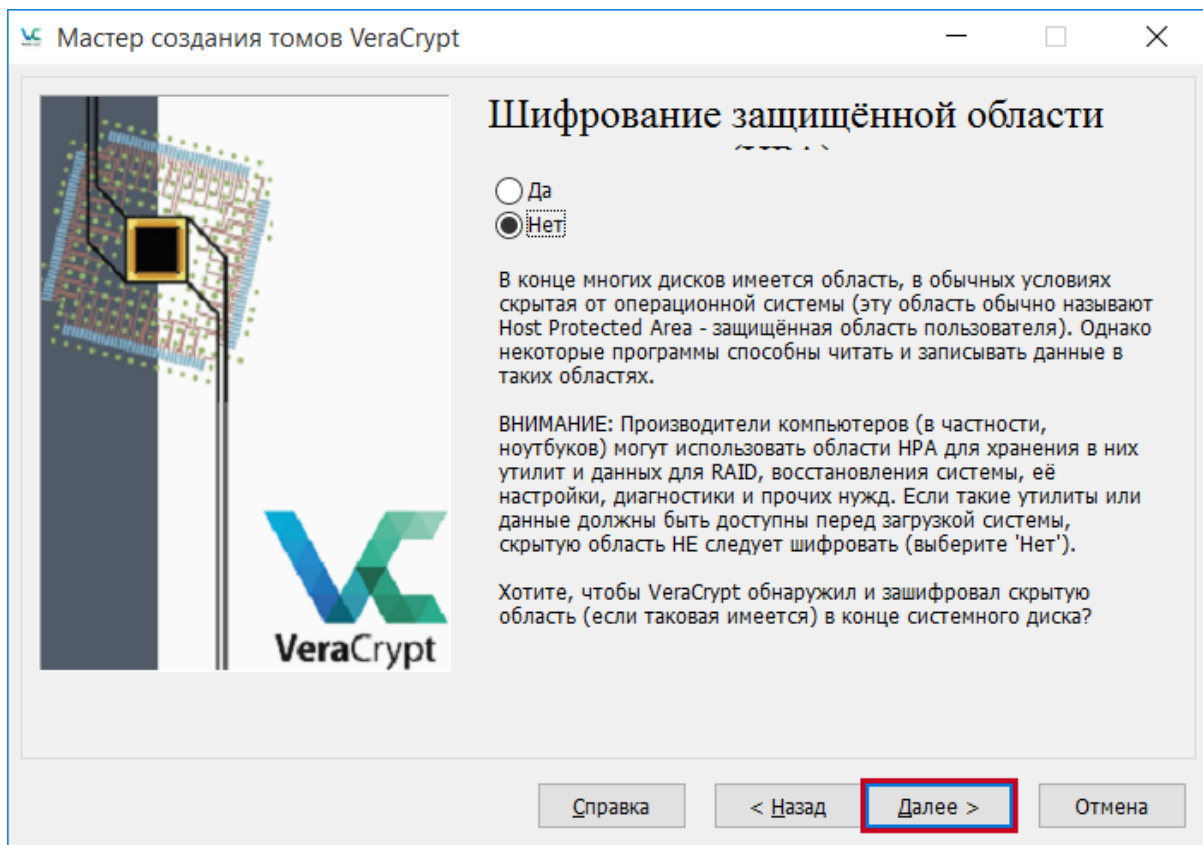
Если существует только один диск и он системный(обычно это диск C:\), то можно ограничиться пунктом с шифрованием системного раздела. Вполне возможно, что ваш физический диск разбит на несколько разделов, например C:\ и D:\. Если это так, то выбирать надо только Encrypt the whole drive (Зашифровать весь диск).



Шифрование скрытых разделов

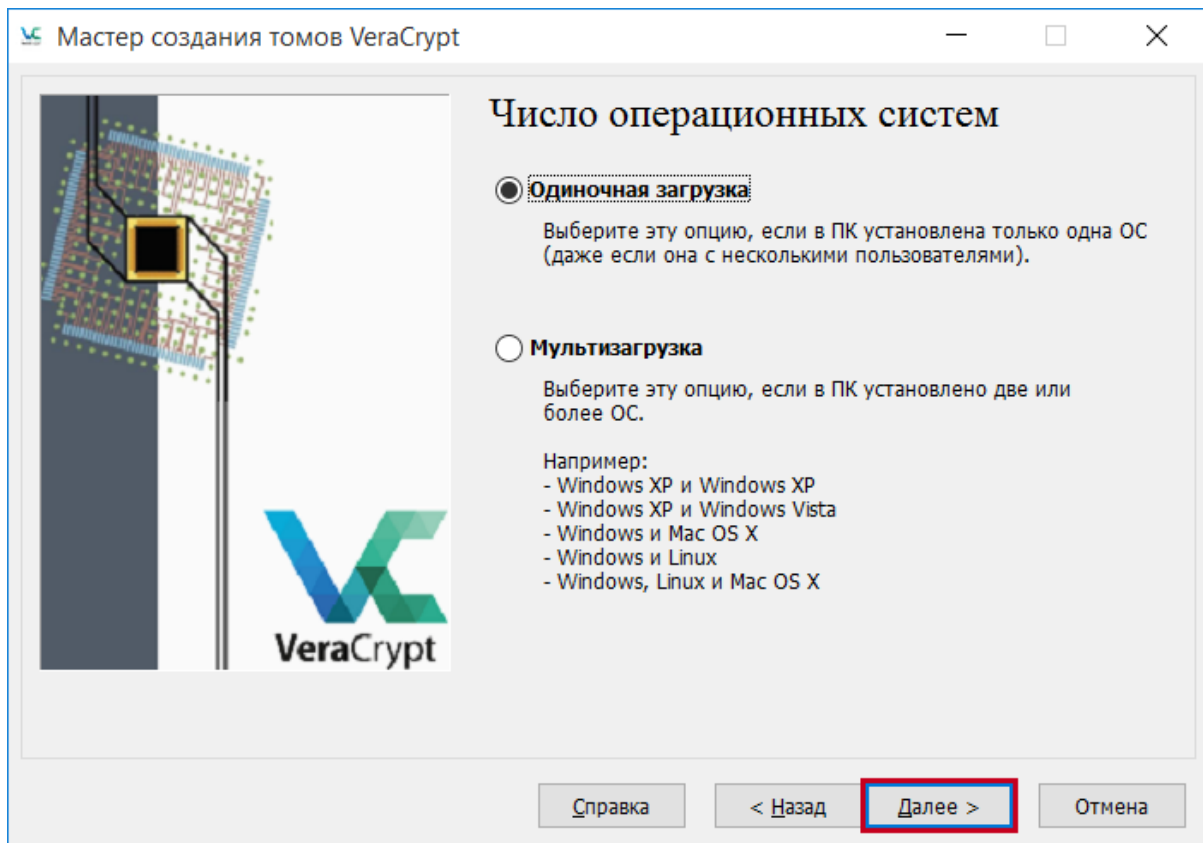
Выберите Yes (Да) если на вашем устройстве есть скрытые разделы с утилитами производителя компьютера, и Вы хотите зашифровать их, обычно в этом нет необходимости.

Нажмите кнопку Next (Далее).



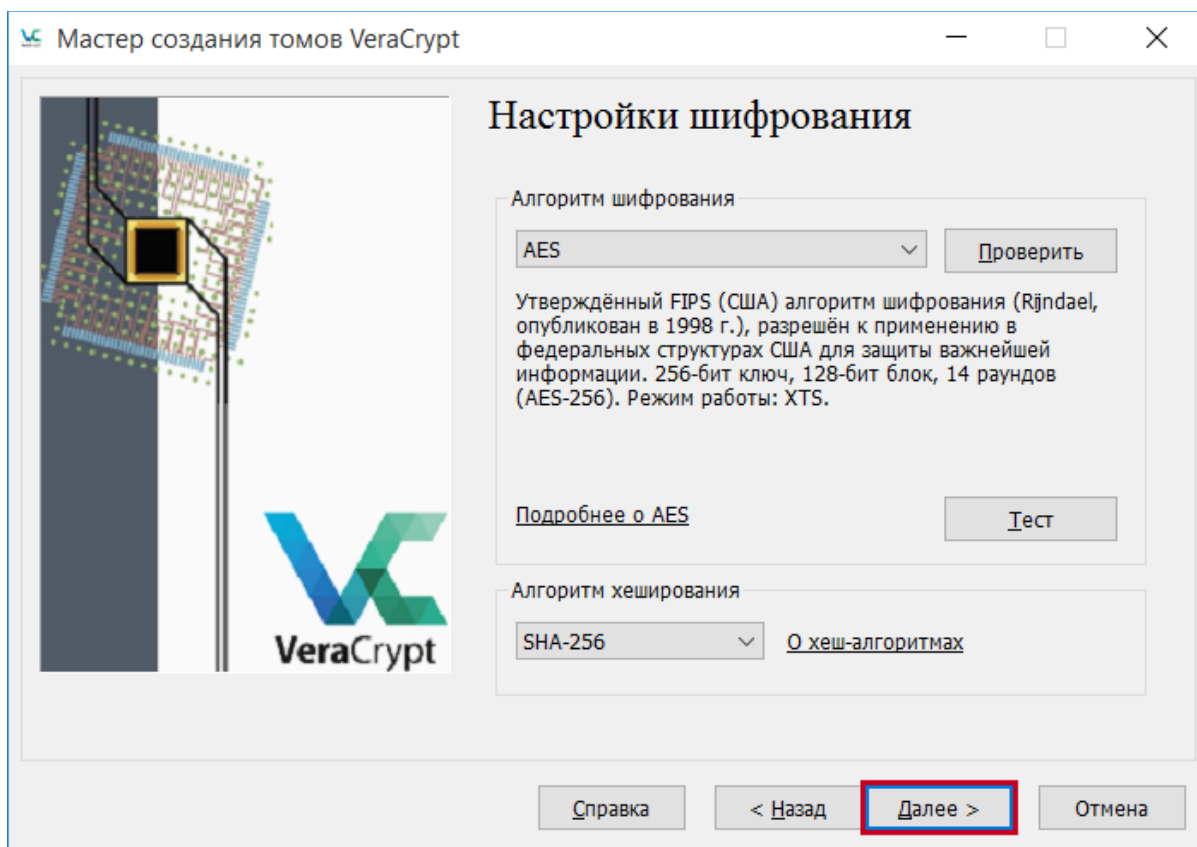
Число операционных систем

Выберите Single boot (Одиночная загрузка) и нажмите кнопку Next (Далее).



Настройки шифрования

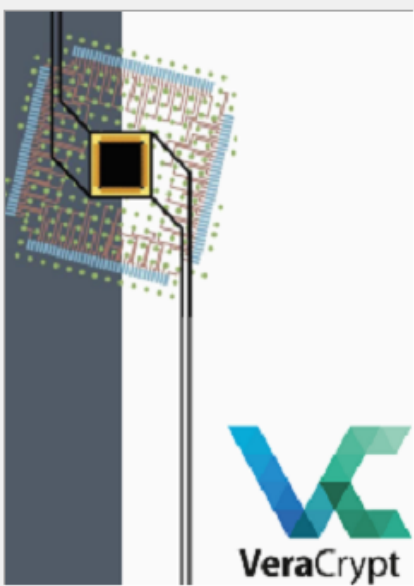
Выбор алгоритмов шифрования и хеширования. Тут смело можно оставить значения AES и SHA-256 по умолчанию как наиболее сильный вариант.



Пароль

При выборе пароля лучше придумать его из головы. Он должен быть длиннее 12 символов и обязательно не содержать легко подбираемых элементов. Пароль 000000000000, очевидно, будет подобран очень быстро, однако и что-то типа ZZZZZZZZZZZZ будет подобрано за короткое время. При взломе используют не перебор напрямую - для длинных паролей это невозможно, а сложные алгоритмы на основании словарей. Поэтому надо избежать явных закономерностей в пароле.

Мастер создания томов VeraCrypt



Пароль

Пароль:

Подтвердите:

☐ Ключ. файлы

☐ Показ пароля

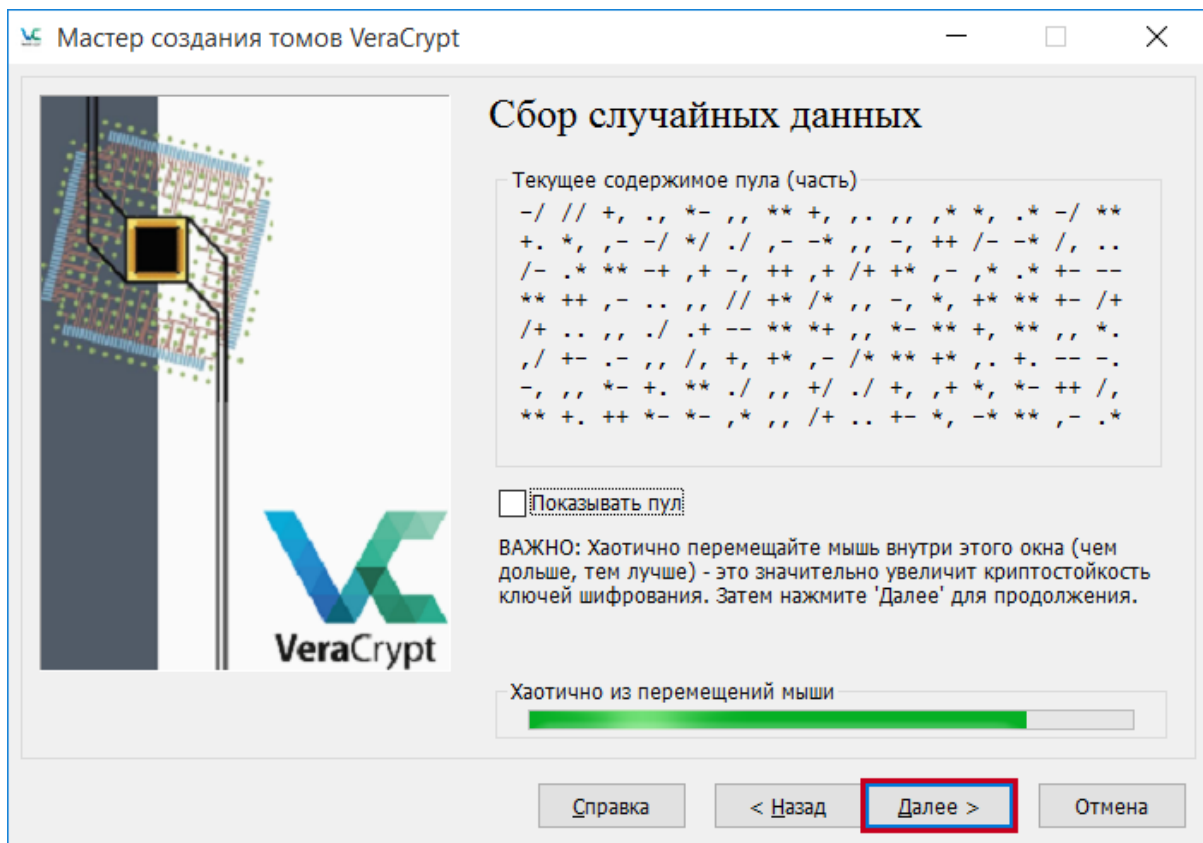
☐ Использовать PIM

Очень важно выбрать хороший пароль. Избегайте указывать пароли из одного или нескольких слов, которые можно найти в словаре (или комбинаций из 2, 3 или 4 таких слов). Пароль не должен содержать имён или дат рождения. Он должен быть труден для угадывания. Хороший пароль - случайная комбинация прописных и строчных букв, цифр и особых символов (@ ^ = \$ * + и т.д.).

Рекомендуем выбирать пароли длиннее 20 символов (чем больше, тем лучше). Макс. длина: 64 символа.

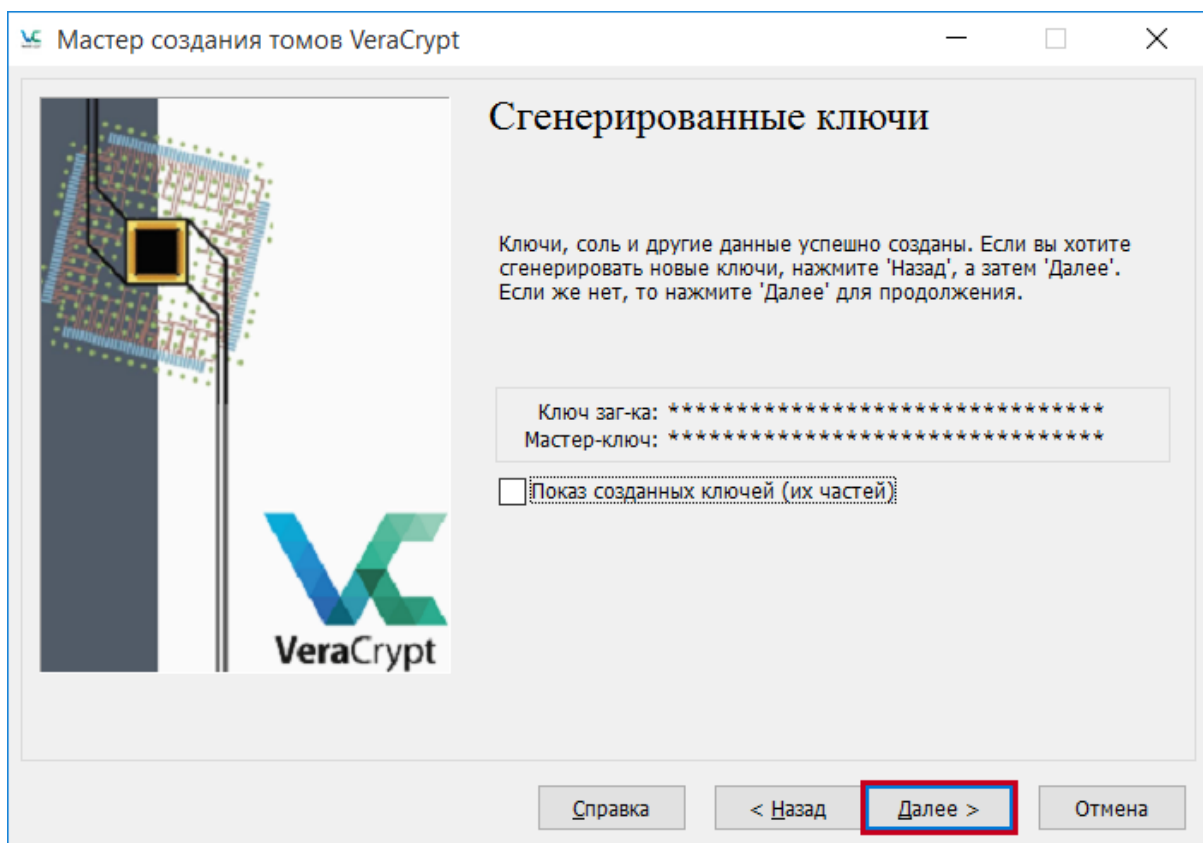
Сбор случайных данных

Этот шаг необходим для формирования ключа шифрования на основе пароля, введённого ранее, чем дольше Вы будете двигать мышью, тем надежнее будут полученные ключи. Хаотично двигайте мышью как минимум до тех пор, пока индикатор не станет зеленым, затем нажмите Next (Далее).



Сгенерированные ключи

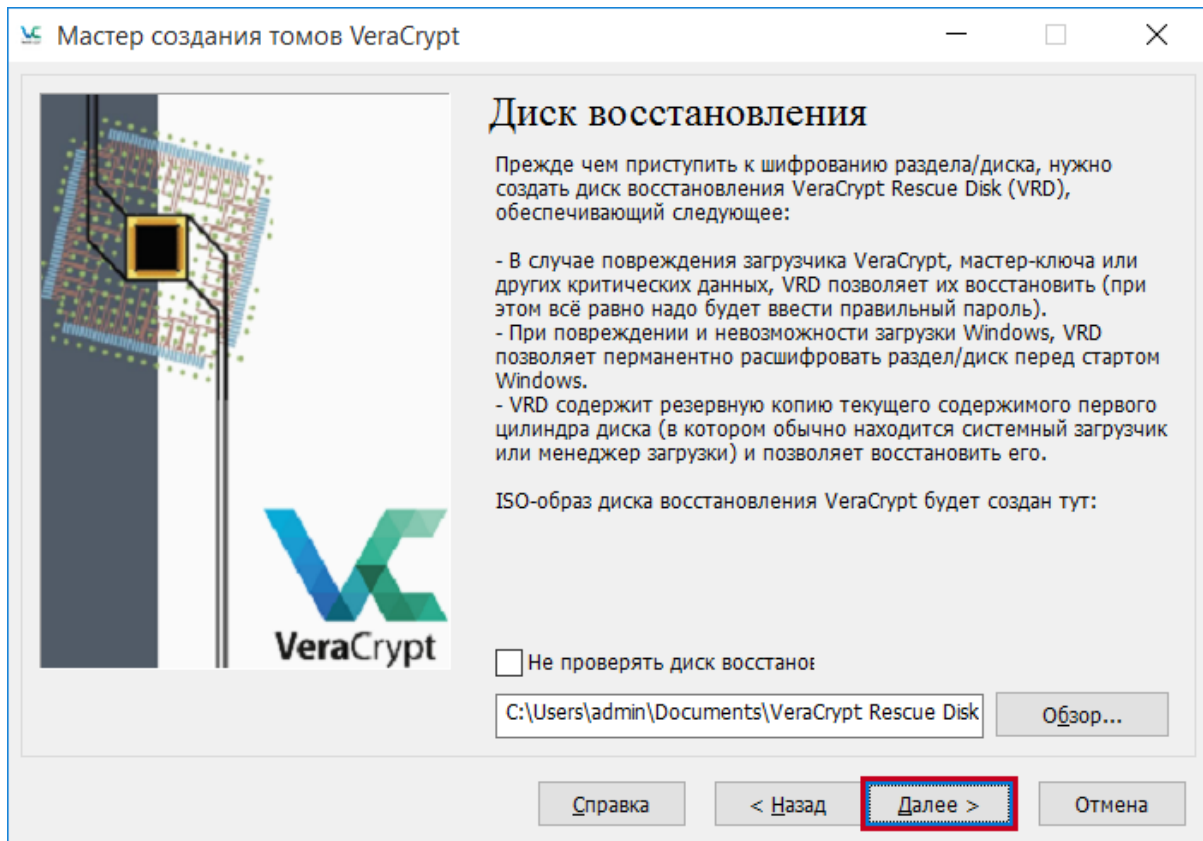
Этот шаг информирует о том, что ключи шифрования, привязка (соль) и другие параметры успешно созданы. Это информационный шаг, нажмите Next (Далее).



Диск восстановления

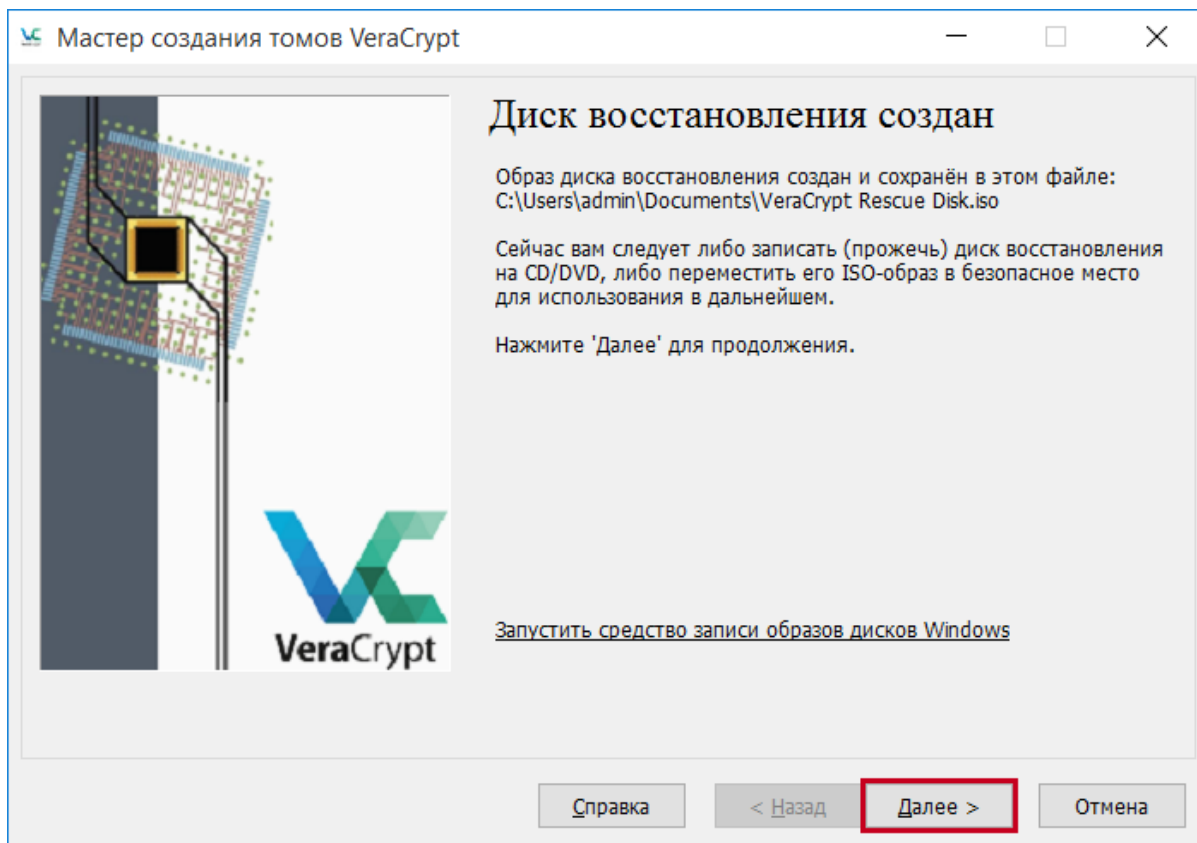
Укажите путь где будет сохранен ISO образ диска восстановления (rescue disk) этот образ может вам понадобится в случае повреждения загрузчика VeraCrypt, при этом Вам все равно понадобится ввести верный пароль. Сохраните образ диска восстановления на съёмный носитель (например флешку) или запишите его на оптический диск и нажмите Next (Далее).

Для сохранения на флешку на этом шаге надо поставить галочку "Не проверять диск восстановления" и на следующем шаге выбрать, что пишущего накопителя нет



Диск восстановления создан

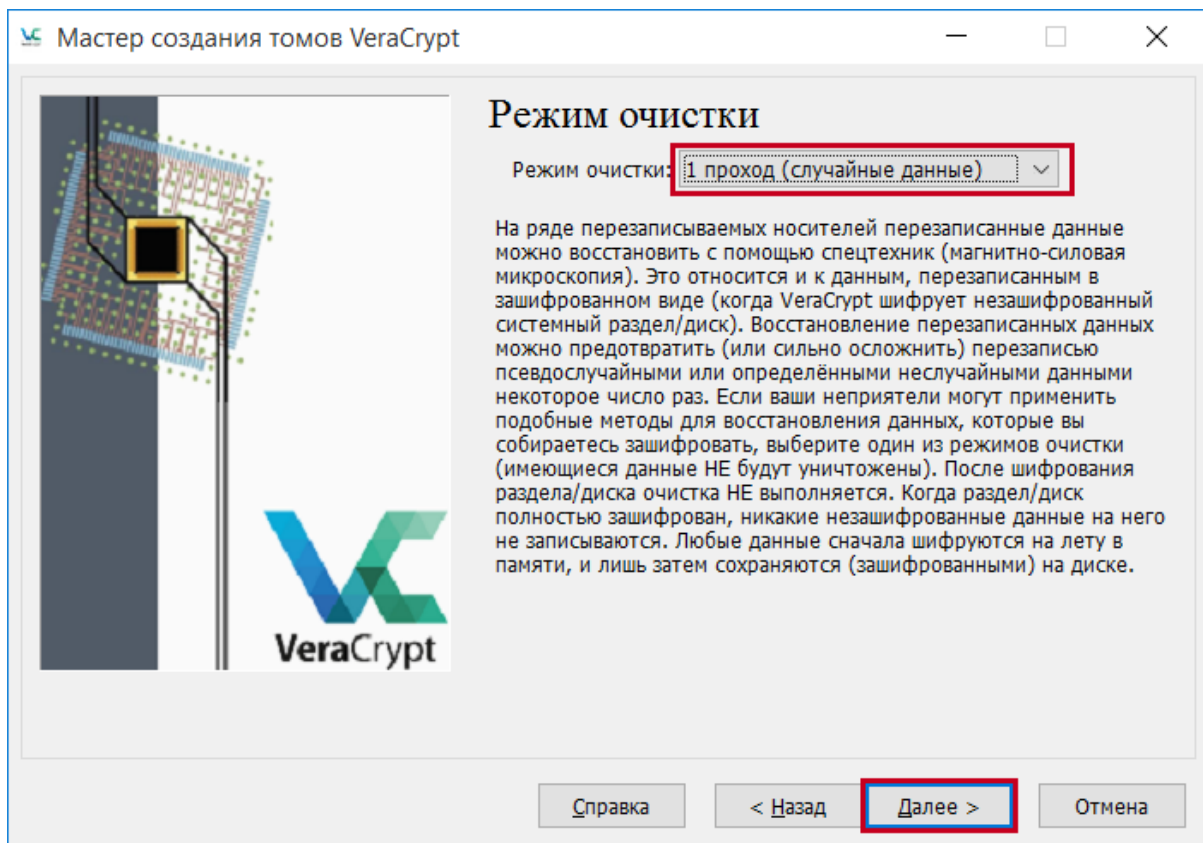
Обратите внимание! Для каждого зашифрованного системного раздела необходим свой диск восстановления. Обязательно создайте его и храните на съёмном носителе. Не храните диск восстановления на этом же зашифрованном системном диске. Только диск восстановления может помочь вам расшифровать данные в случае технических сбоев и аппаратных проблем.



Очистка свободного места

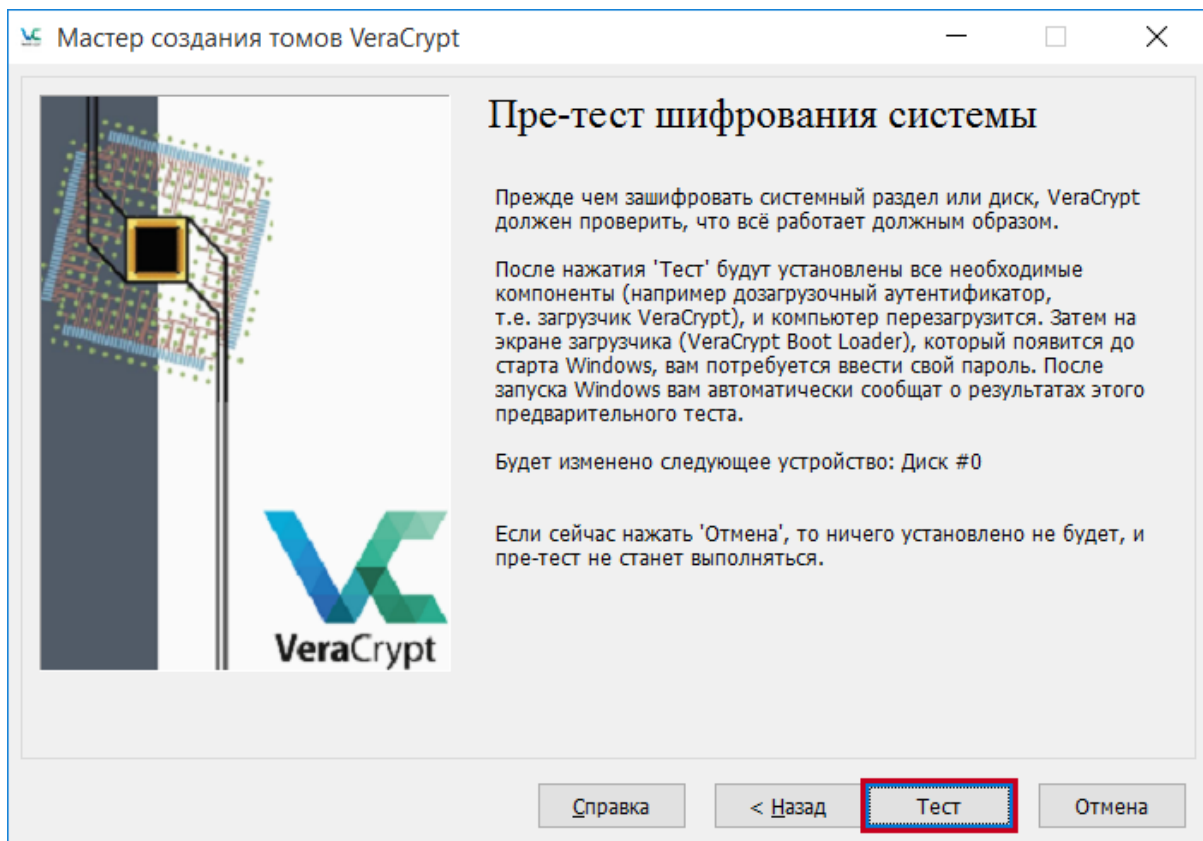
Очистка свободного места позволяет безвозвратно удалить ранее удаленные данные с диска, которые возможно восстановить с помощью специальных техник (особенно актуально для традиционных магнитных жестких дисков). Если Вы шифруете SSD накопитель, выберите 1 или 3 прохода, для магнитных дисков рекомендуем 7 или 35 проходов. Учтите, что эта операция отразится на общем времени шифрования диска, по этой причине откажитесь от неё в случае если ваш диск не содержал важные удаленные данные раньше. Не выбирайте 7 или 35 проходов для SSD накопителей, магнитно-силовая микроскопия не работает в случае с SSD, вполне достаточно 1 прохода.

Если на диске не хранилось информации, которую надо скрыть от посторонних глаз, не надо ставить слишком большое количество проходов. Это очень сильно увеличит время, требуемое на очистку.



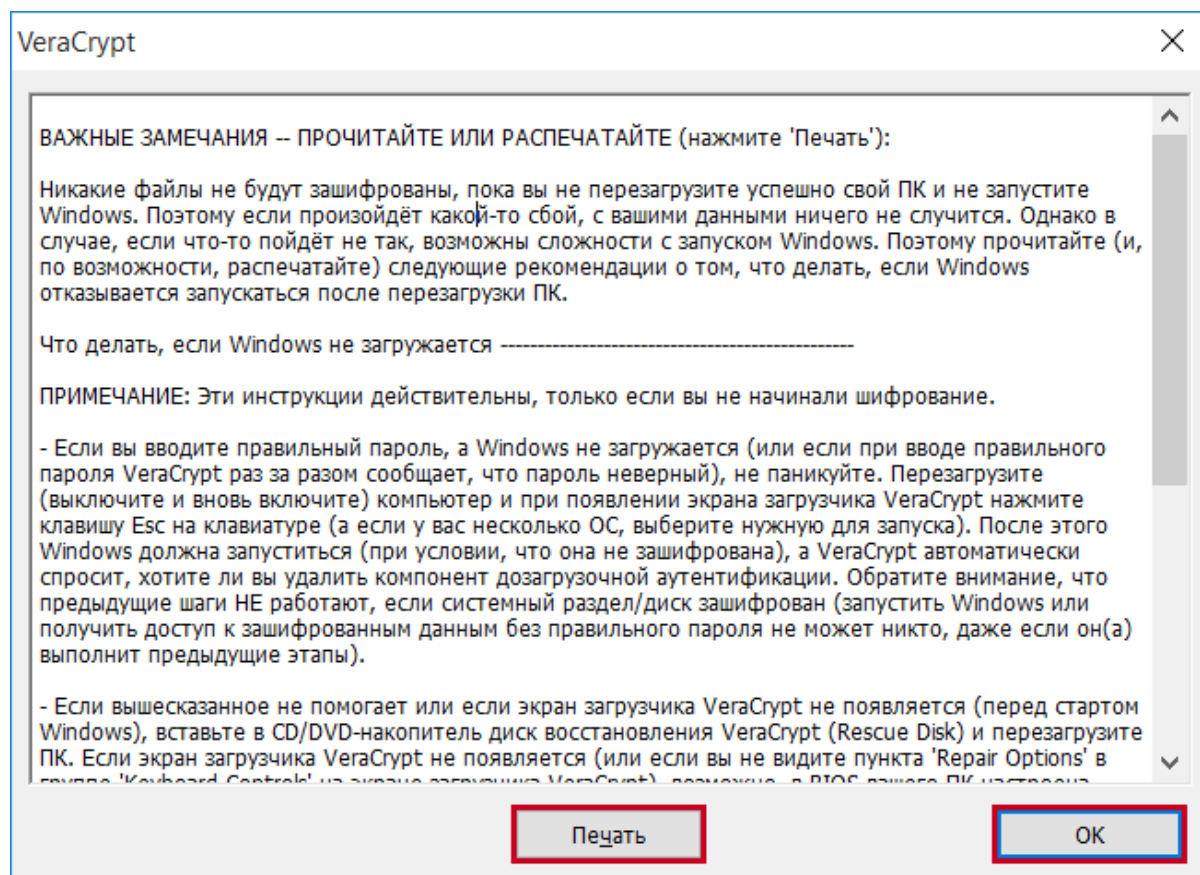
Тест шифрования системы

Этот шаг - проверка перед шифрованием. Он относительно безопасный и на нём редко что-то ломается, но на всякий случай прочитайте текст тут и на следующей странице



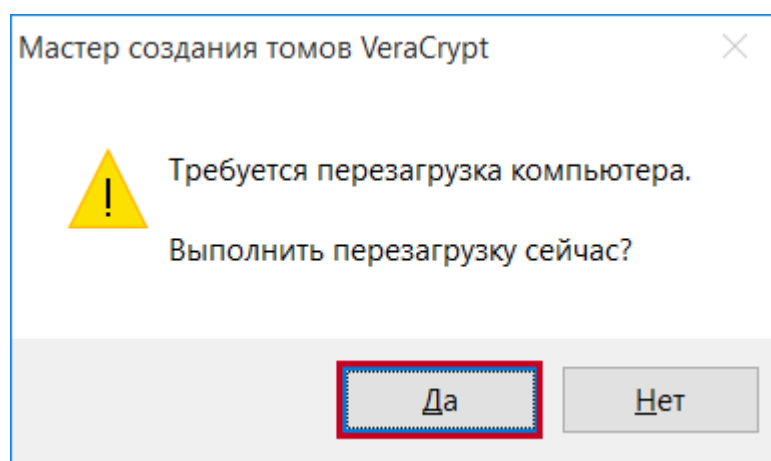
Что делать если Windows не загружается

Ознакомьтесь, а лучше распечатайте рекомендации на случай, что делать если Windows не загрузится после перезагрузки (такое случается). Нажмите ОК если прочитали и поняли сообщение.



Перезагрузка

Перезагрузите компьютер



Ввод пароля при загрузке

После перезагрузки и перед началом загрузки операционной системы Вы увидите интерфейс загрузчика VeraCrypt и запрос на ввод пароля. Укажите пароль который

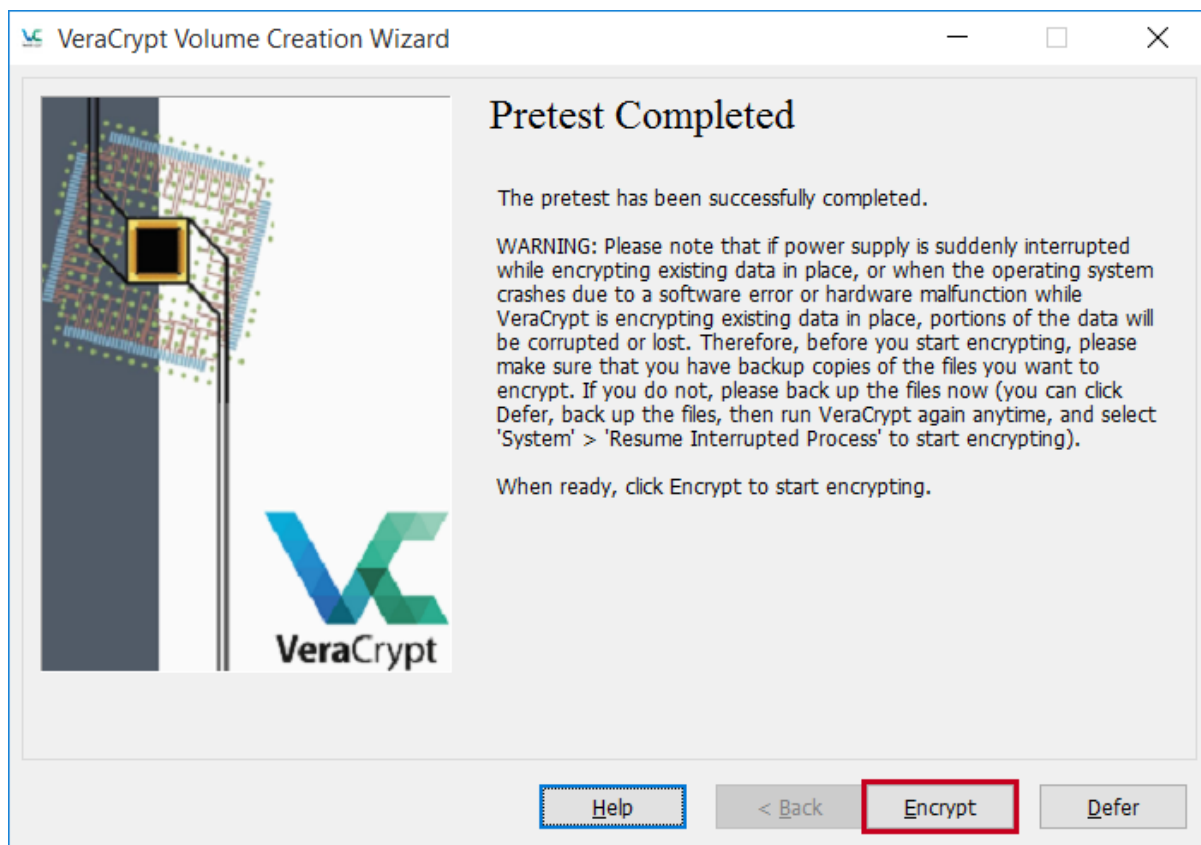
вводили на Шаг Если после пароля запросит PIM, то просто нажмите enter. Это параметр алгоритма шифрования, который может быть настроен автоматически.



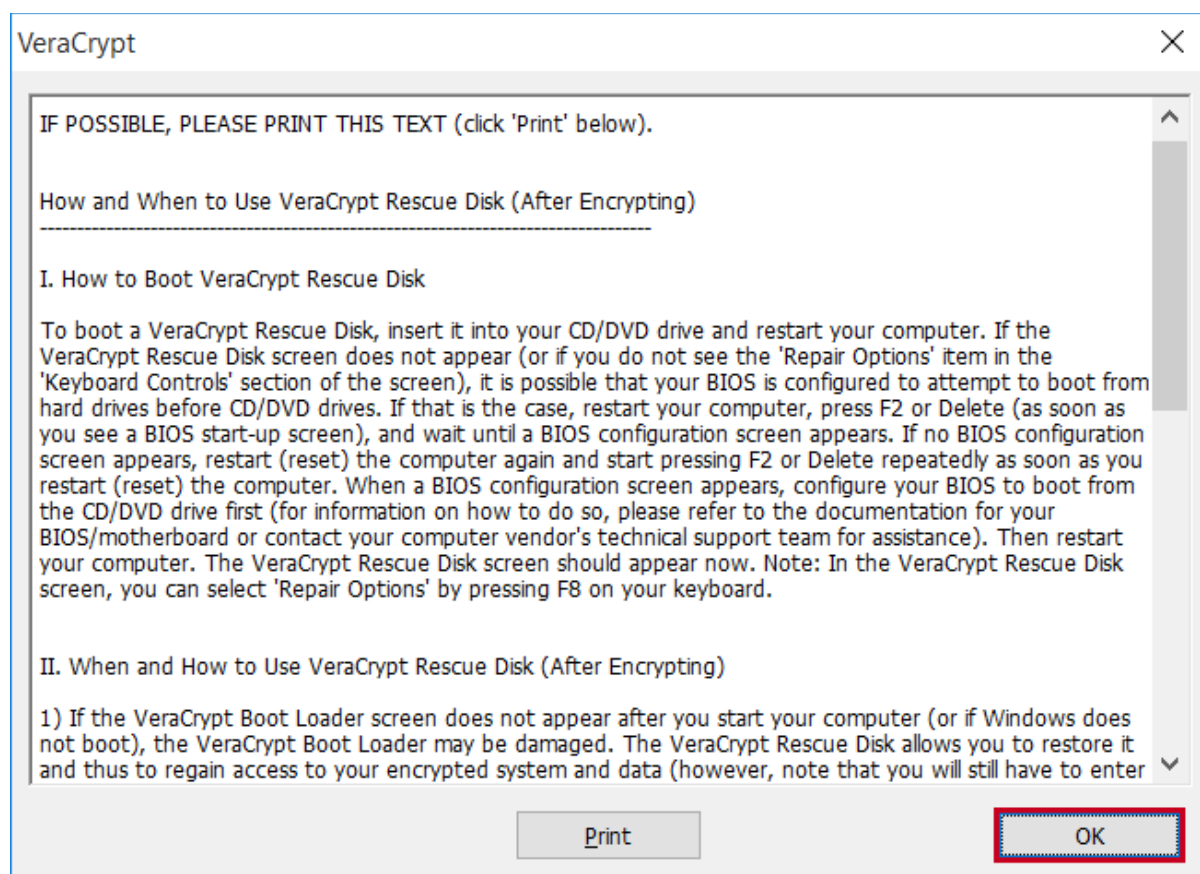
Тест завершен

Сделайте скриншот окна об успешном прохождении претеста и приложите его к практике(надо упаковать в zip архив). Это подтвердит, что система готова к шифрованию и можно двигаться дальше. Вместо него можно приложить скриншот с окном после шифрования.

Если Ваш Windows загрузился, и Вы увидели данное окно значит Тест успешно завершен, нажмите Encrypt для начала шифрования.

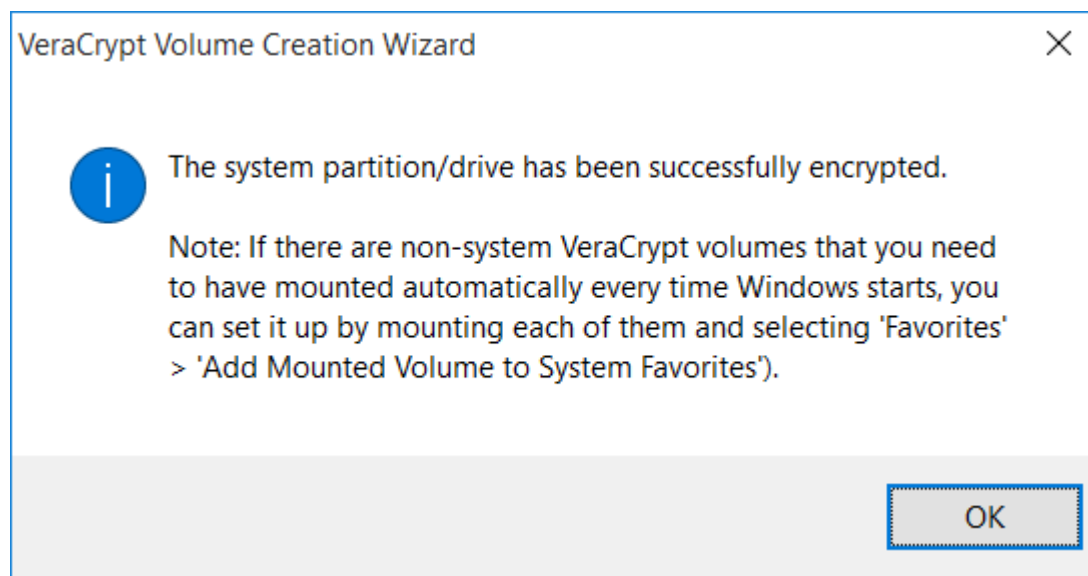


Ознакомьтесь с инструкцией как загрузить диск восстановления.



Шифрование

После окончания процесса шифрования Вы получите сообщение, нажмите OK.



Нажмите Finish.

Поздравляем, все ваши файлы и файлы операционной системы теперь зашифрованы и будут расшифровываться на лету при обращении к ним. Все расшифрованные данные

хранятся в оперативной памяти. VeraCrypt никогда не записывает их на диск в расшифрованном виде.

