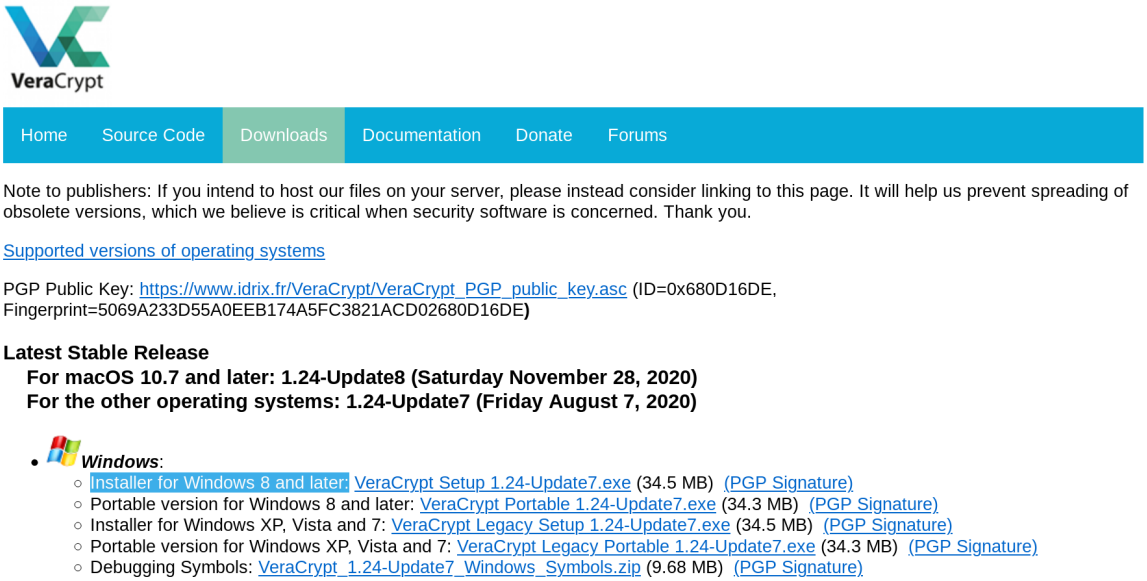
VeraCrypt. Как зашифровать чертёж

(подробнее на сайте https://urbanplanmarket.com)

Чтобы зашифровать чертёж, нужно выполнить **3 шага**:
I. **Установить** программу VeraCrypt;
II. **Создать** зашифрованный контейнер;
III. **Поместить** чертёж в зашифрованный контейнер.

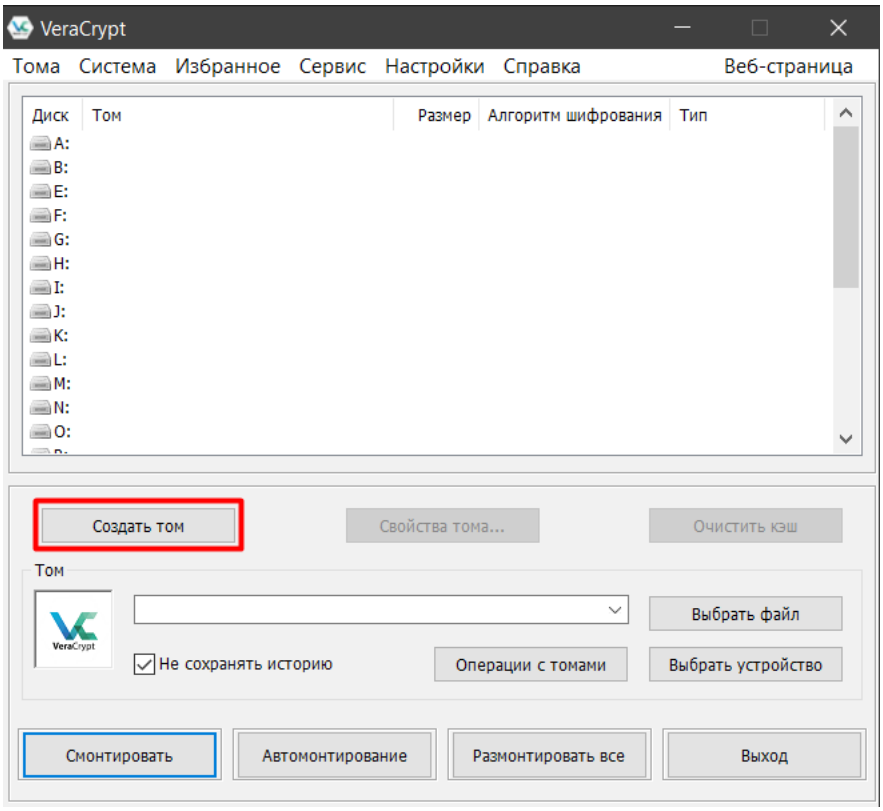
I. Как установить VeraCrypt?

1. Зайти на сайт VeraCrypt: https://veracrypt.fr/en/Downloads.html
2. Скачать и установить программу.
Например, для Windows - «*Installer for Windows 8 and later*»:

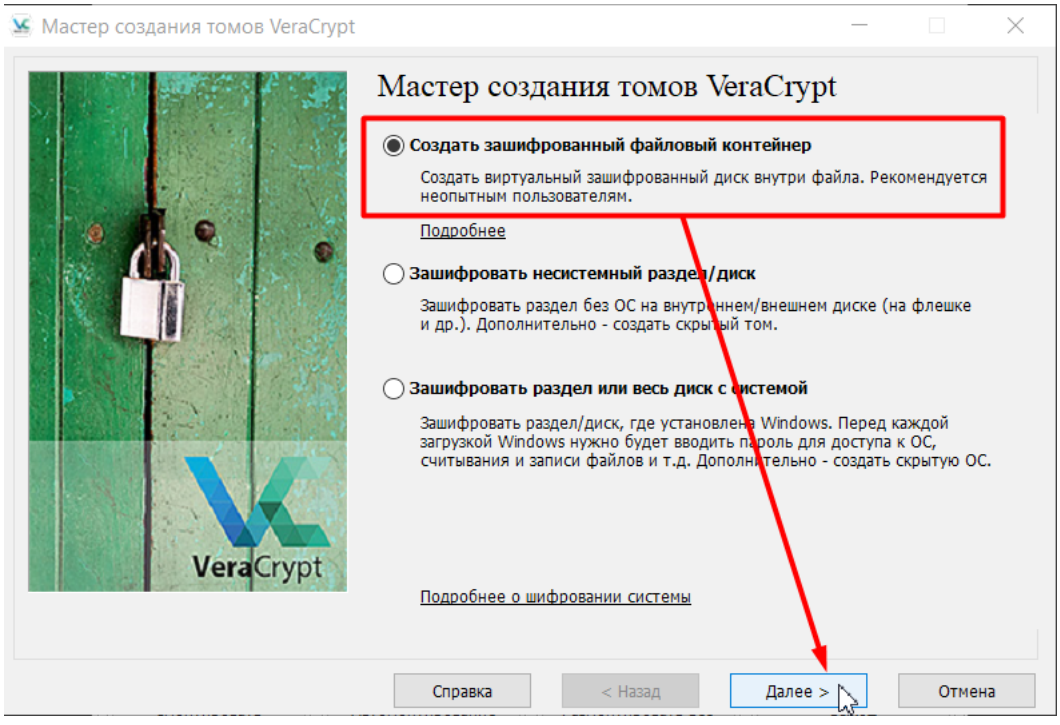


II. Как создать зашифрованный контейнер?

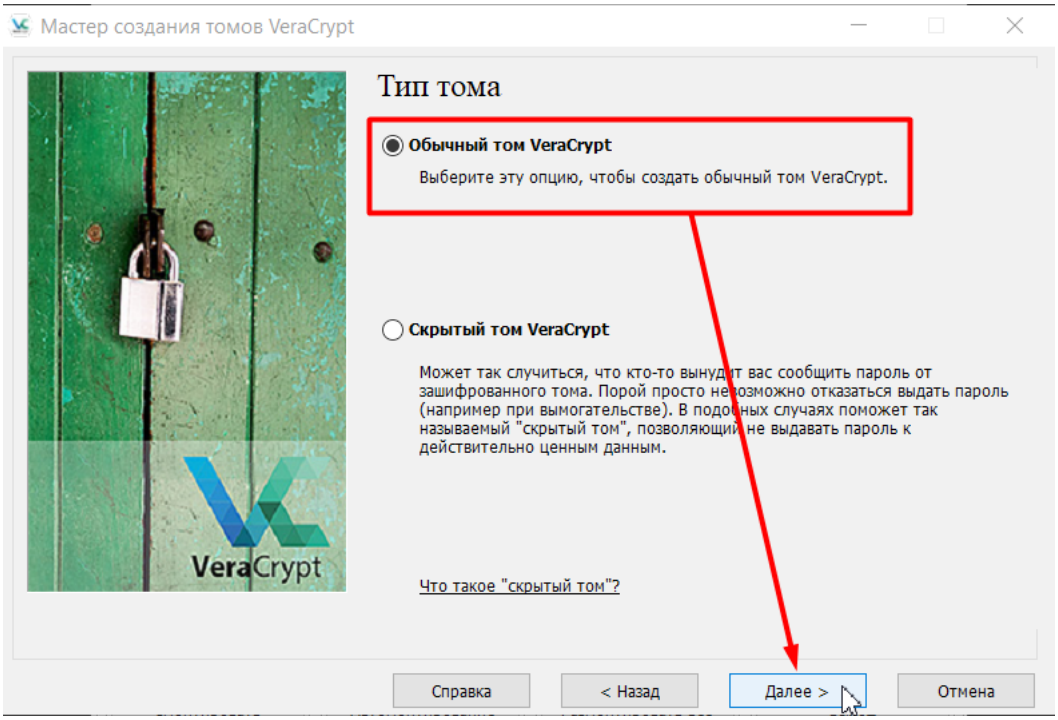
1. Запускаем VeraCrypt и нажимаем кнопку «Создать том»:



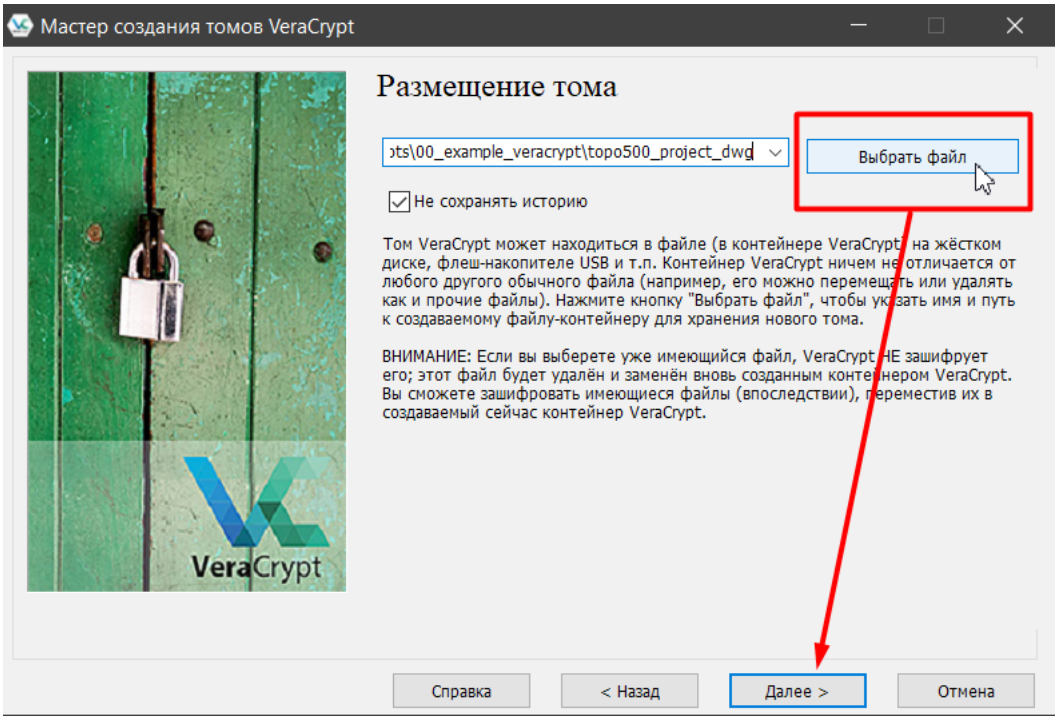
2. Выбираем «Создать зашифрованный файловый контейнер»:



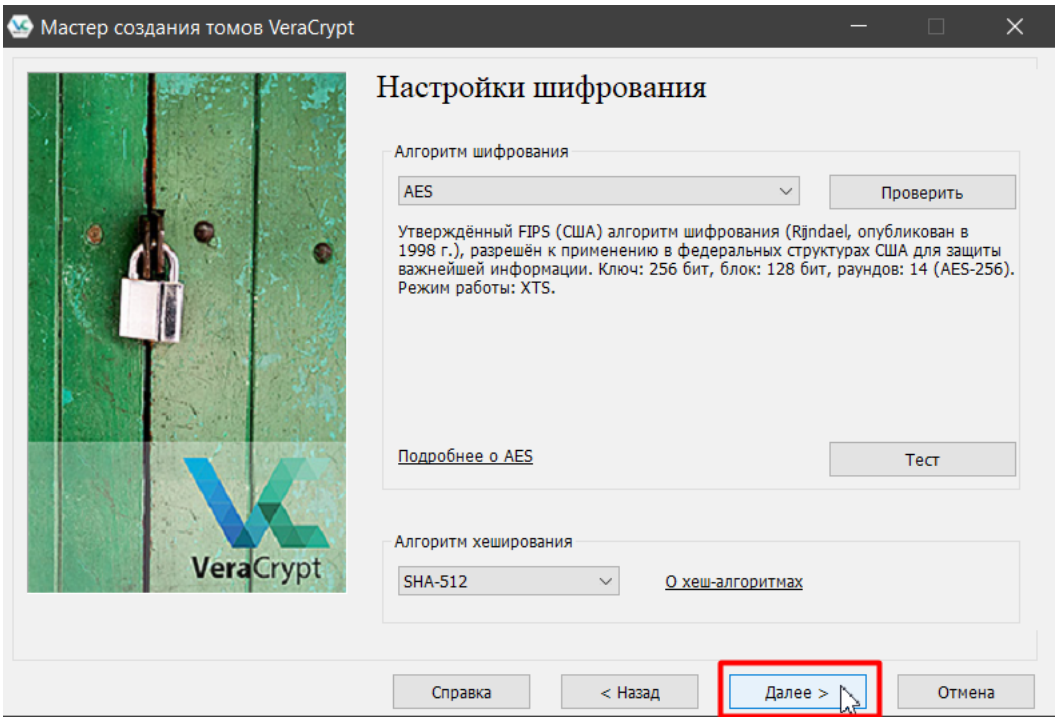
3. Тип контейнера «Обычный том VeraCrypt»:



4. Выбрать папку, в которой будет создан файловый контейнер и задать ему название:

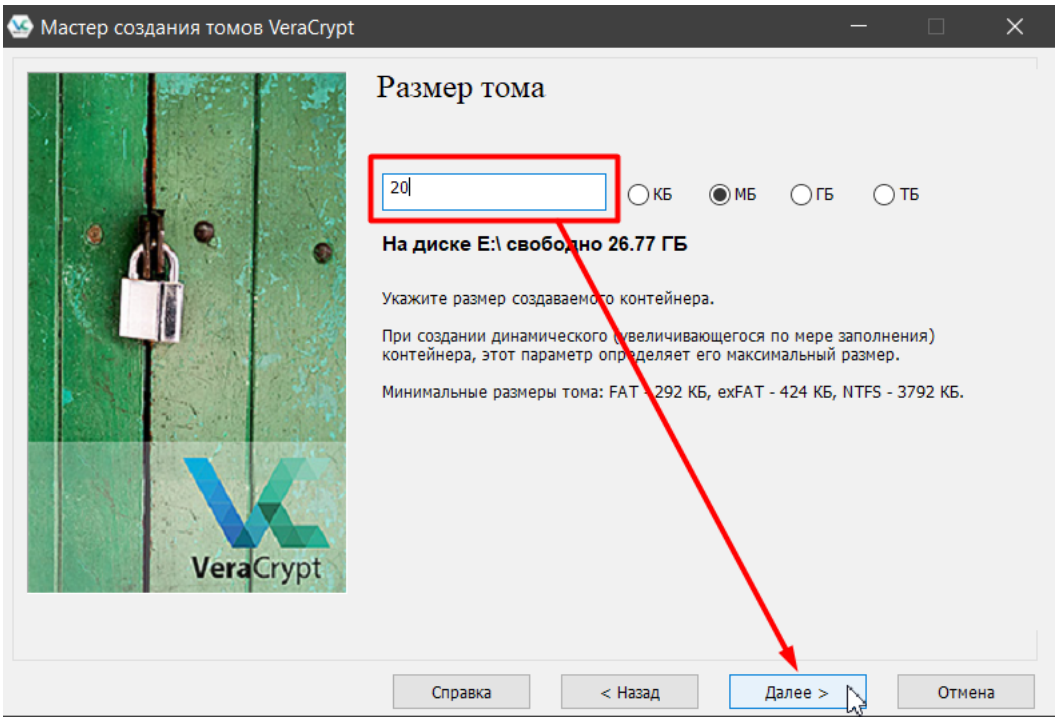


5. В настройках шифрования можно ничего не менять:



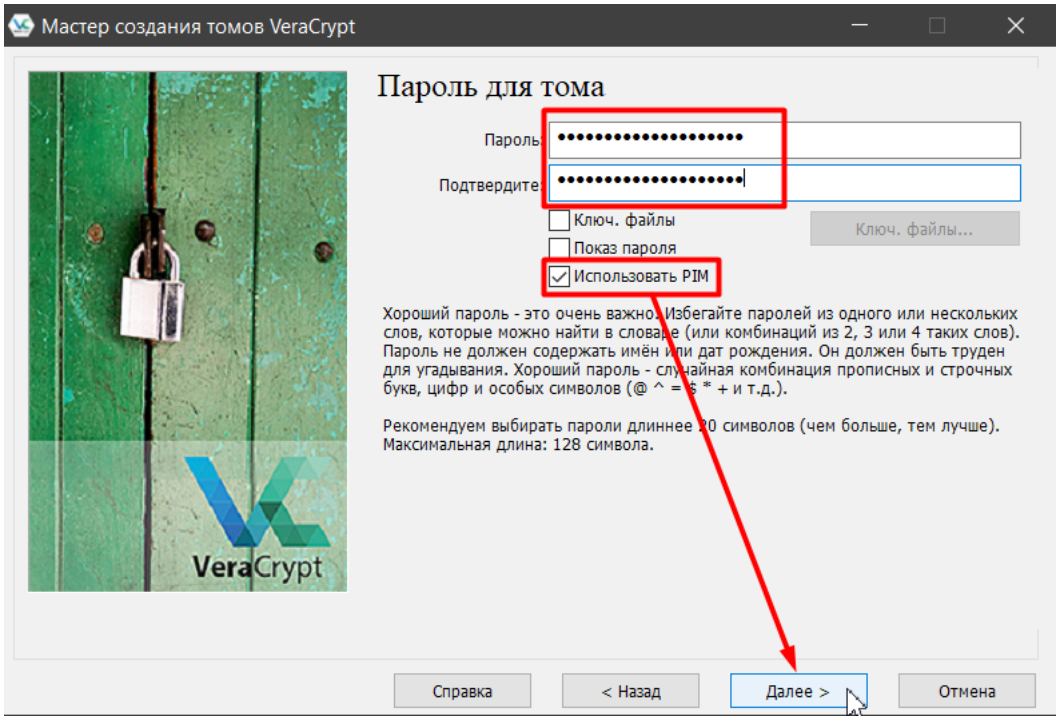
6. Задаём размер будущего контейнера.

Размер контейнера лучше делать на 3-5% больше от размера файлов, которые будут в него помещены. В данном примере создаётся контейнер на 20 Мб.



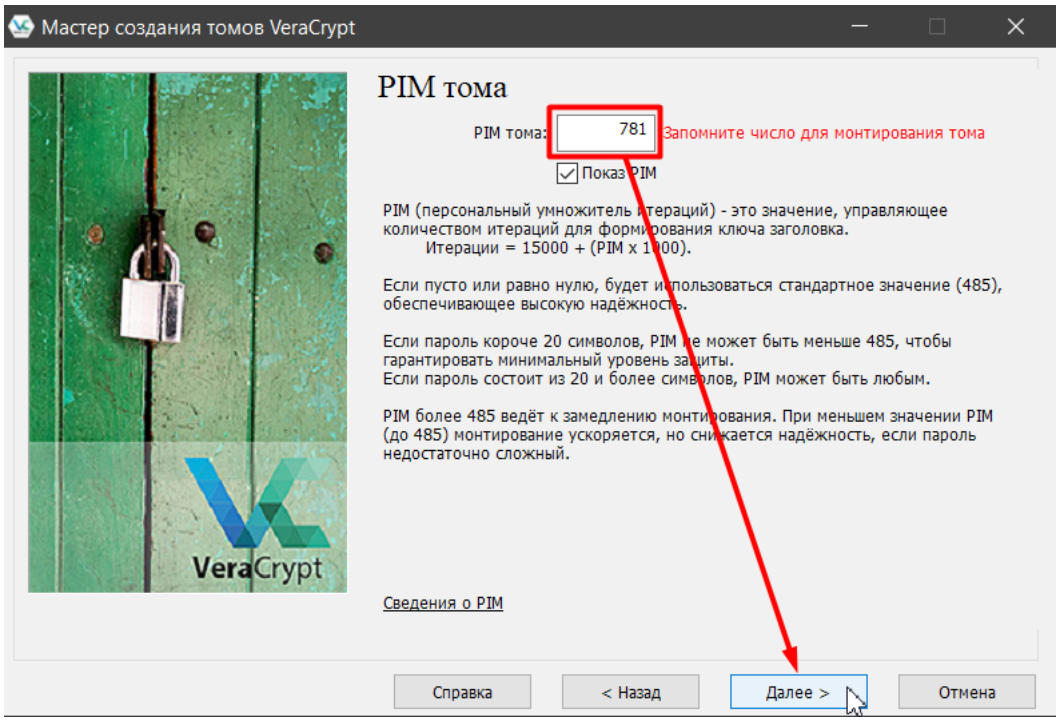
7. Задаём пароль для контейнера.

Минимальная длина пароля должна быть 20 символов. Для лучшей надёжности: пароль должен быть 26 символов и более. Также нажимаем галочку «Использовать PIM»!



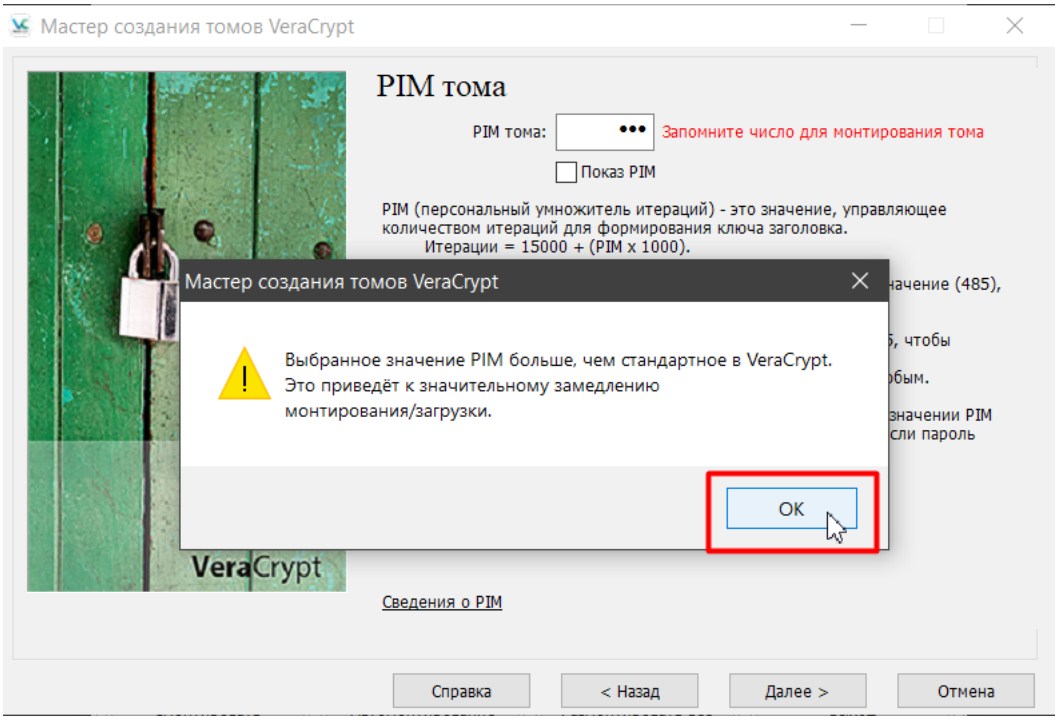
8. Задаём число PIM.

Рекомендуемое число PIM — от 700 до 990. Можно и больше.



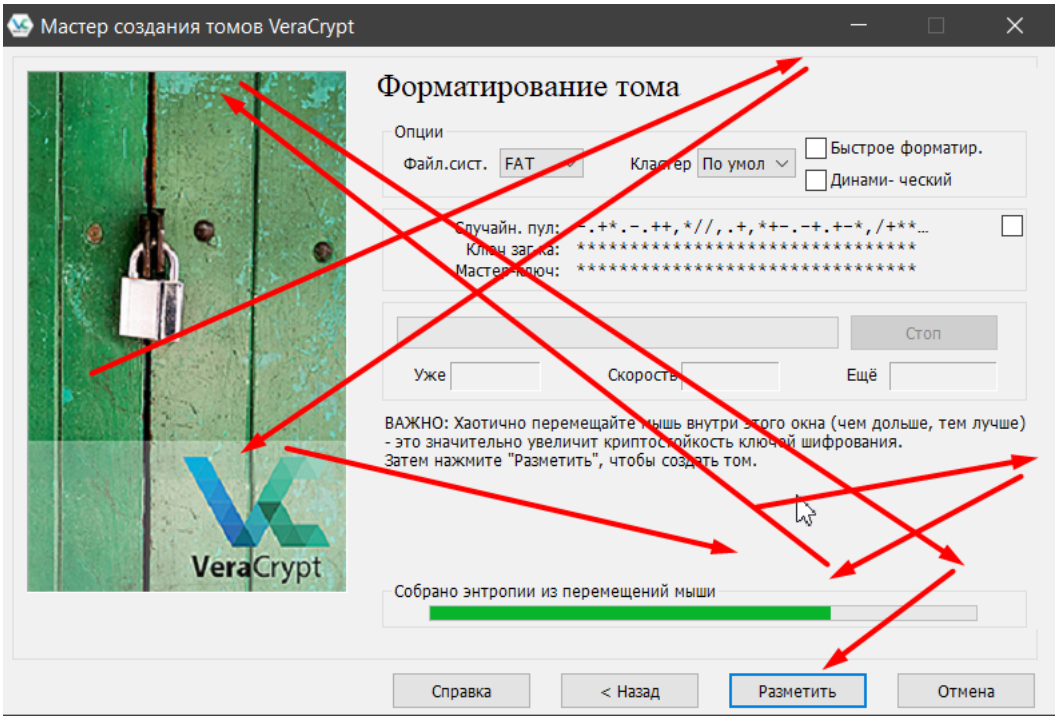
PIM — это множитель, улучшающий защиту шифрования. Например, если даже кто-то узнает пароль от зашифрованного контейнера, то ему всё-равно не удастся расшифровать файлы, не зная число PIM.

9. Нажимаем кнопку «ОК», если PIM выбрано более 485:

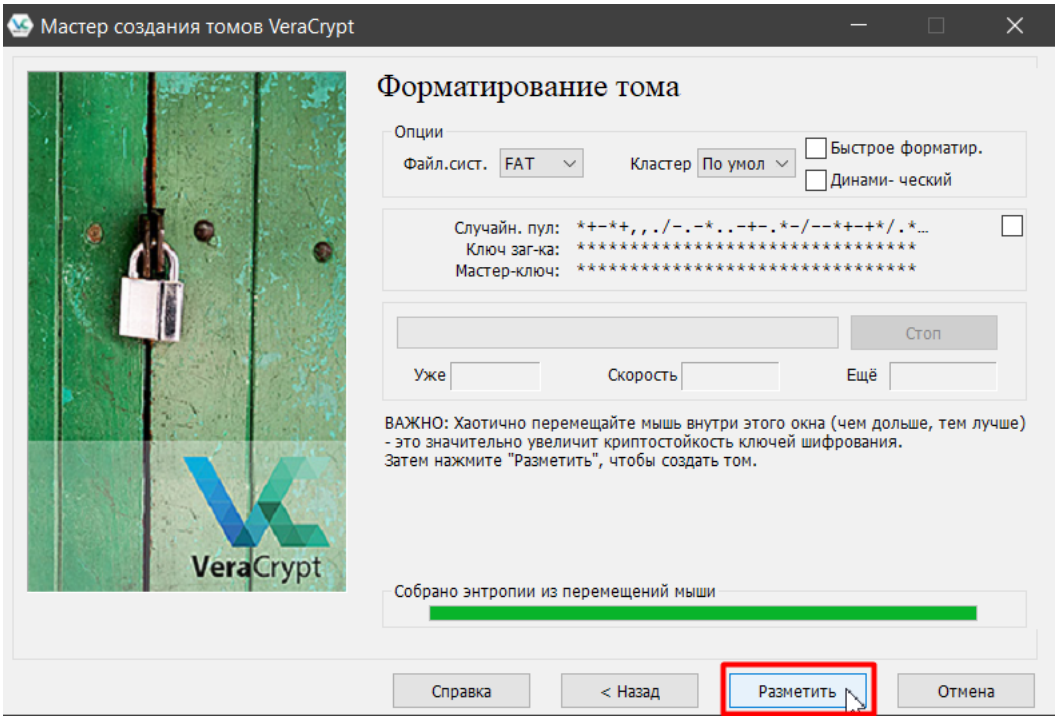


10. В следующем окне нужно двигать указатель мышки в случайных направлениях. Это нужно для увеличения стойкости ключей шифрования.

Также в этом окне можно выбрать файловую систему создаваемого контейнера:
- **FAT** (по умолчанию);
- **NTFS** (если размер зашифрованного файла будет более 4 Гб);
- **EXT4** (для GNU/Linux).

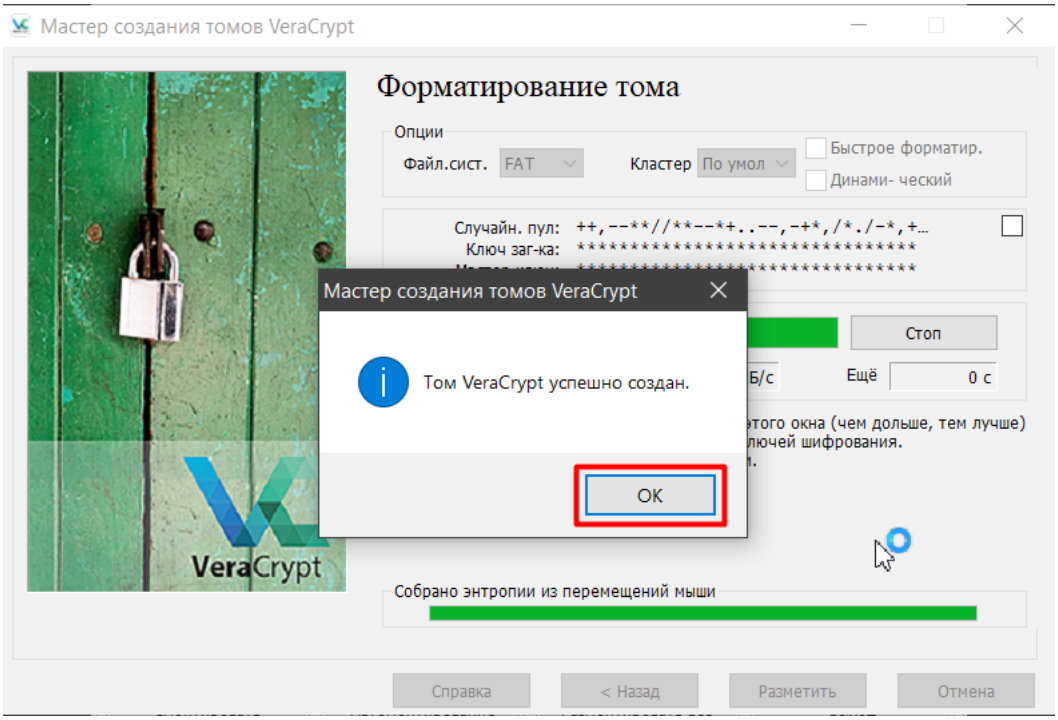


Двигать мышкой нужно до тех пор, пока зелёная полоска не заполнится полностью. Потом нажимаем кнопку «Разметить»:



11. Через некоторое время контейнер будет создан.

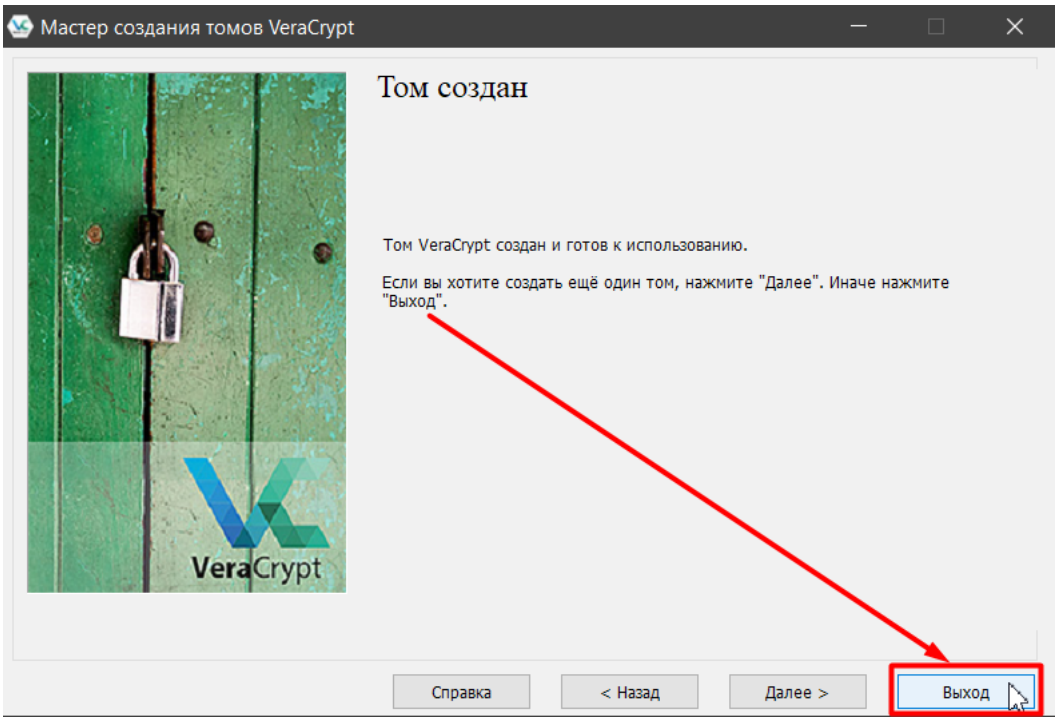
Появится сообщение «Том VeraCrypt успешно создан»:



12. Зашифрованный контейнер VeraCrypt создан.

Теперь нажимаем кнопку «Выход».

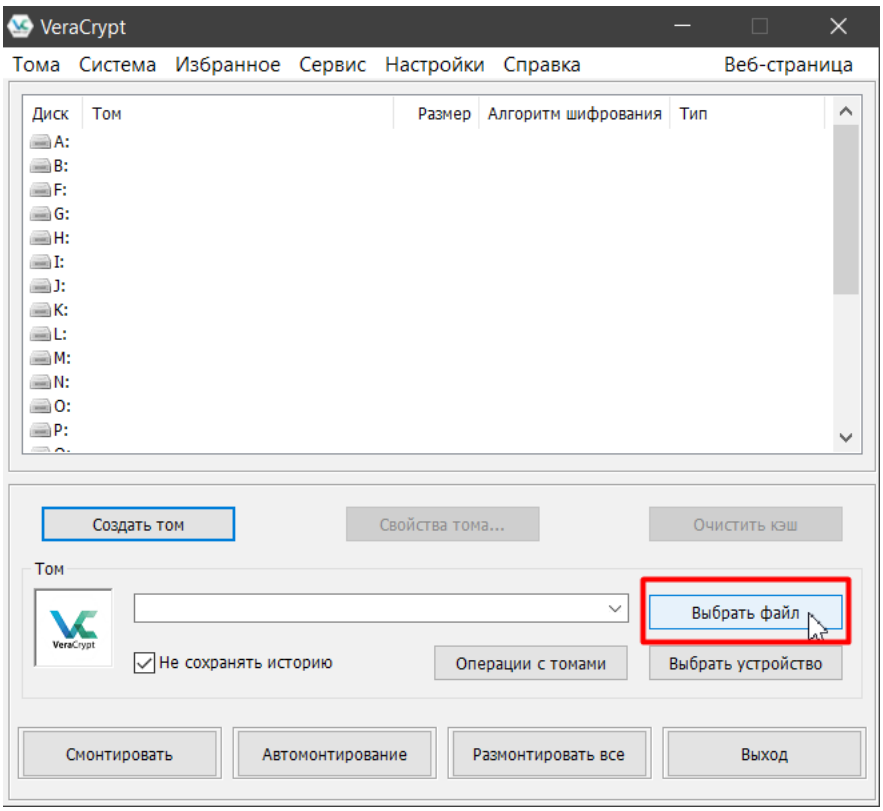
И теперь в той папке, которой была указана при создании контейнера, появится файл с заданным названием.



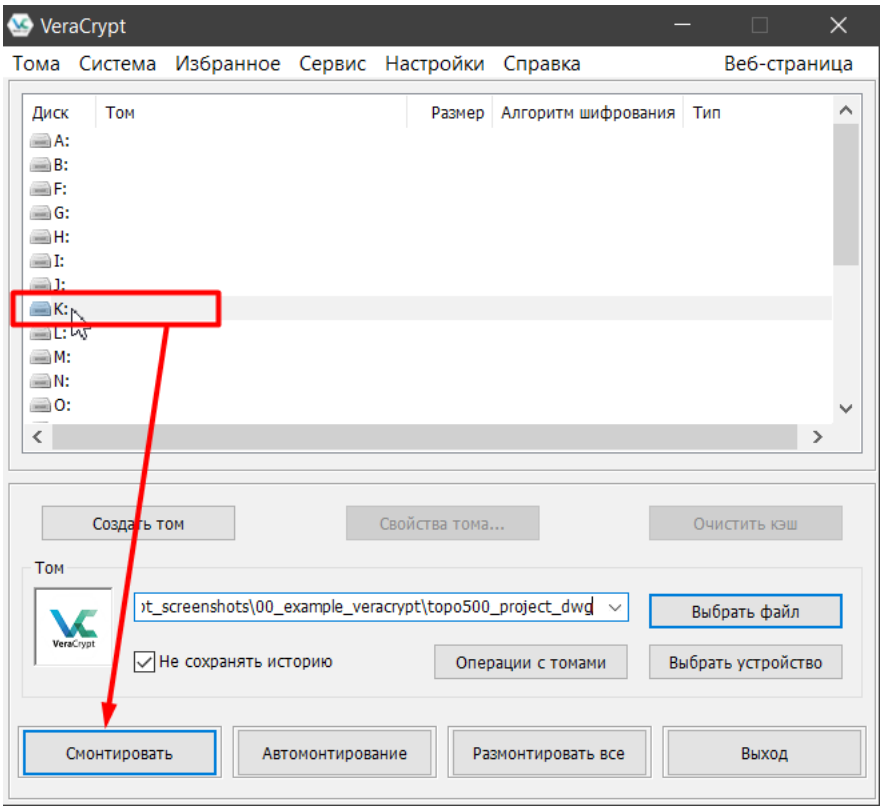
III. Как поместить чертёж в контейнер?

Теперь остался последний шаг: нужно поместить чертёж в только что созданный зашифрованный контейнер.

1. Выбираем в той же папке контейнер VeraCrypt, созданный на предыдущем этапе.
Это будет файл с заданным прежде названием, но без указания на его расширение, которое обычно идёт после точки (например, *.pdf). Так и должно быть:

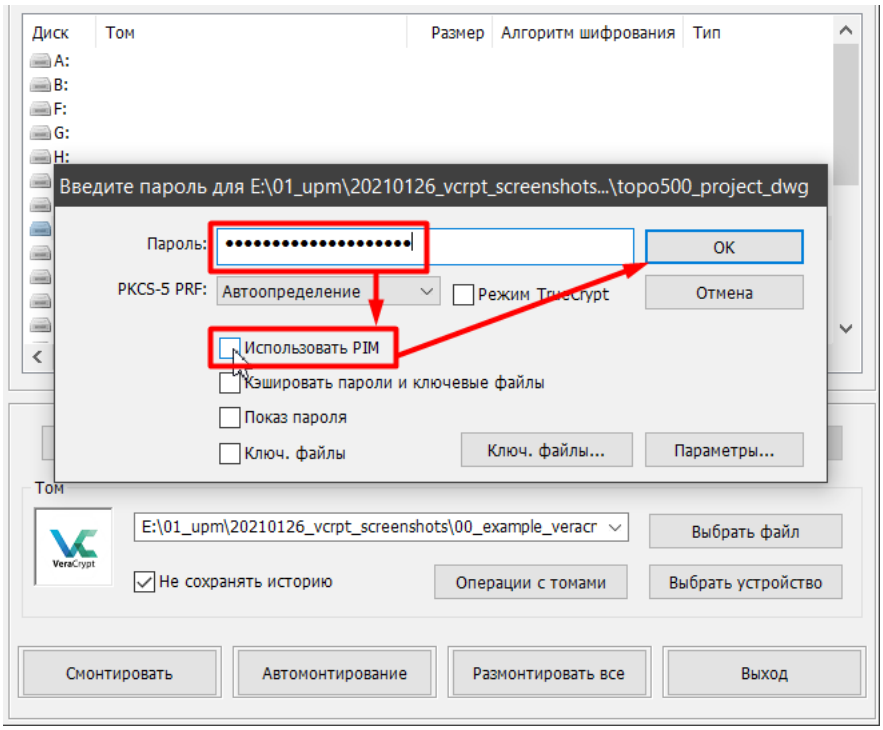


2. Указываем букву диска, под которой будем монтировать контейнер VeraCrypt к компьютеру.
Нужно указывать только ещё не занятую на компьютере букву диска. Например, в операционной системе Windows диски под буквами C: и D: уже заняты системным диском и диском с файлами соответственно.
Далее нажимаем кнопку «Смонтировать»:

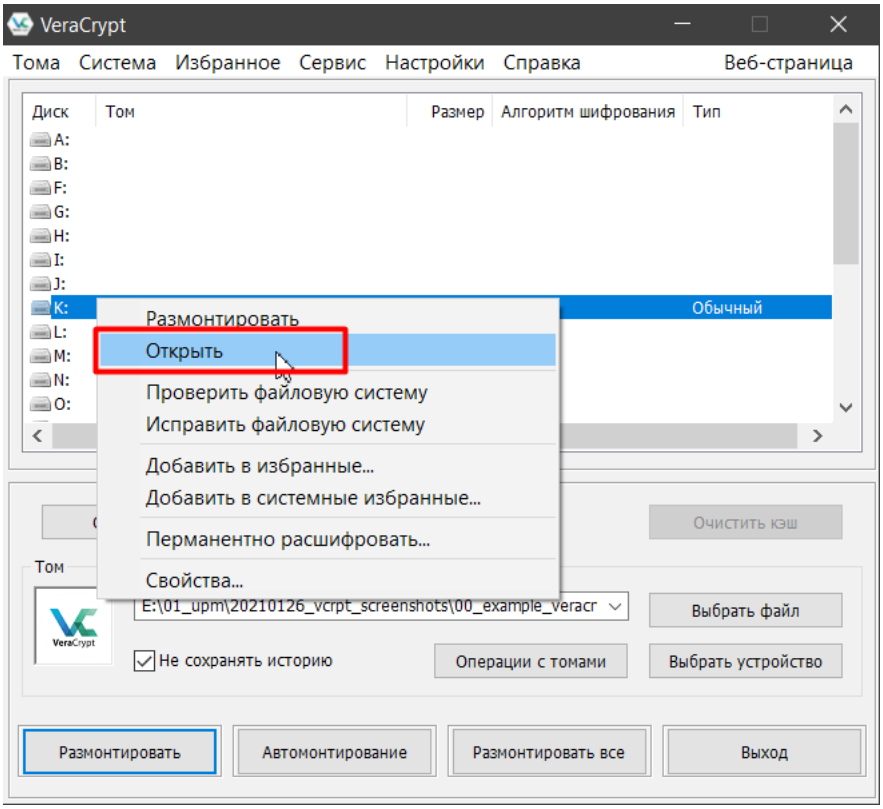


3. Вводим пароль и число PIM.

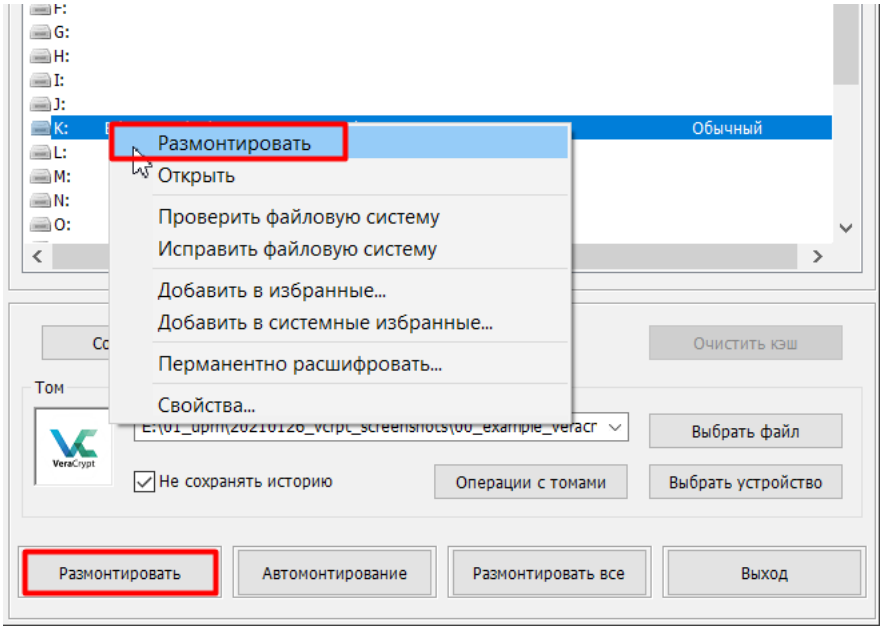
Вводим тот пароль, который был указан при создании зашифрованного контейнера. Чтобы ввести число PIM, нужно сперва нажать на галочку «Использовать PIM»:



4. Теперь контейнер VeraCrypt смонтирован и чтобы открыть его, нужно нажать правой кнопкой на строке с именем диска:



5. Откроется контейнер в виде обычной пустой папки. Теперь нужно скопировать в эту папку чертёж, который планируется зашифровать. И после нажать кнопку «Размонтировать». Всё, чертёж зашифрован!



Примечания:

1) Теперь этот зашифрованный контейнер VeraCrypt можно отправлять по интернету.

2) Для того, чтобы открыть уже зашифрованный контейнер, нужно выполнить только **шаг 3**.

3) Контейнер, пароль и число PIM лучше передавать получателю по разным каналам.
Например, **контейнер** — по e-mail, **пароль** — через смс, а **PIM** — через мессенджер (Jabber и т.п.). Конечно, самый надёжный способ — передать пароль и PIM лично в руки на листке бумаги.

4) Пароль должен состоять из букв и разных символов. Буквы не должны повторяться, даже если они в разных регистрах (т. е. одна и та же буква заглавная и строчная — это уже повтор символа). Пример надёжного пароля: ~FS41#_Tg7$Qw23~?y[R*}Ai

5) Важно, понимать, что контейнер, смонтированный на компьютер, ничем не отличается от обычного диска. Файлы в контейнере зашифрованы только когда контейнер размонтирован, т. е. не подключен к компьютеру. Поэтому, после монтирования контейнера, любой, имеющий доступ к ПК, может прочитать находящиеся там файлы.

6) Более безопасно, когда для получения контейнера по интернету и для его монтирования используются разные компьютеры. К примеру, один компьютер использовать только для выхода в интернет, а на втором компьютере, отключенном от интернета, контейнеры монтировать.

7) GNU/Linux — рекомендуемая операционная система для работы с зашифрованными контейнерами.