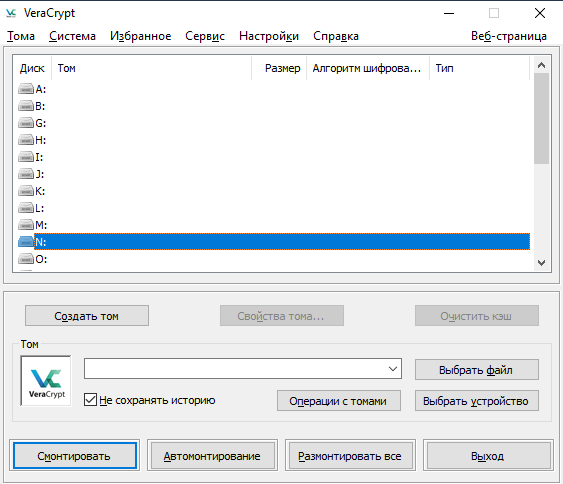
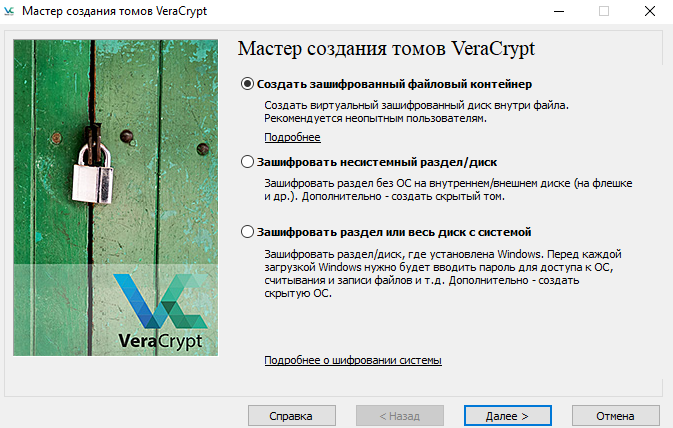
Шифрование жёсткого диска

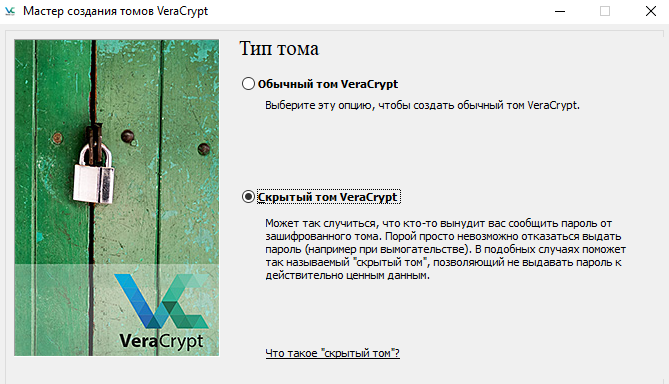
Скачайте программу VeraCrypt - <https://www.veracrypt.fr/en/Downloads.html> и установите её.

Откройте и нажмите на кнопку “Создать том”. Откроется дополнительное окно шифрования раздела. Здесь вы сперва сможете выбрать тип тома для шифрования - файловый контейнер, несистемный раздел/диск, раздел/диск с системой.





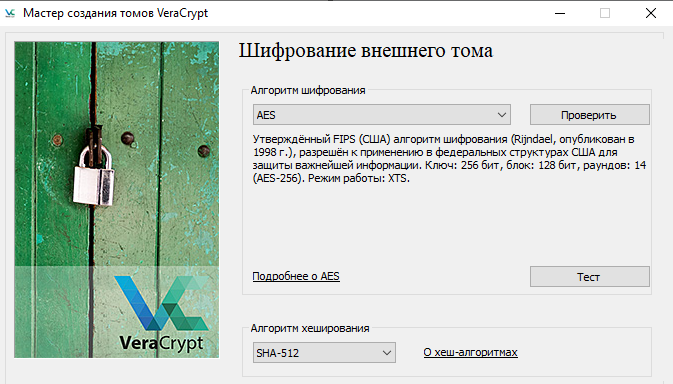
В нашем случае мы будем создавать файловый контейнер со скрытым томом.

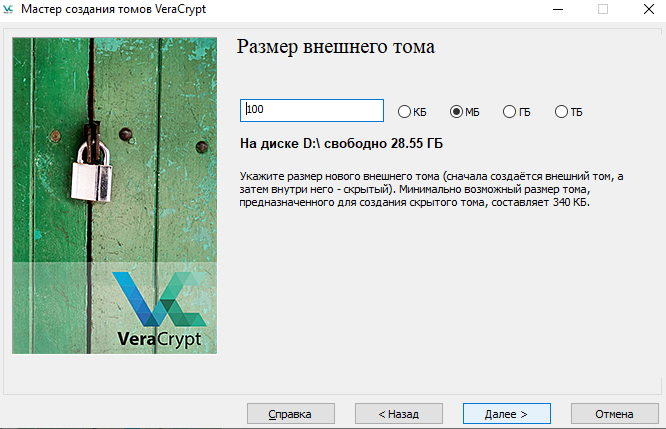


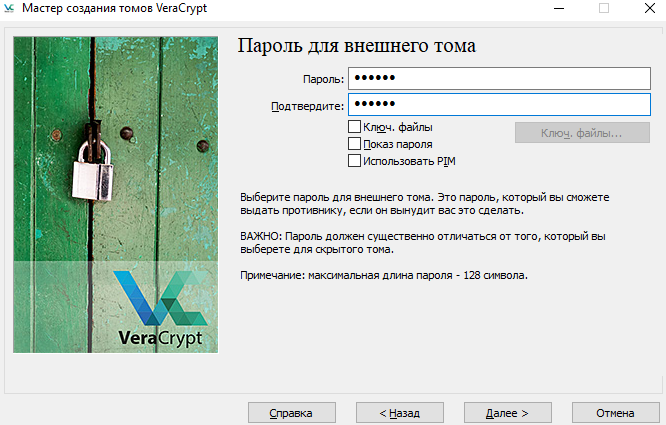
Дальше выбирайте обычный режим создания тома и файл, который будет служить хранилищем, либо же можем сами создать этот файл.



Сперва будет создан внешний том - он будет доступен по обычному паролю. Вы увидите меню, в котором сможете выбрать алгоритм хэширования и шифрования, затем количество места для этого файлового контейнера и пароль.

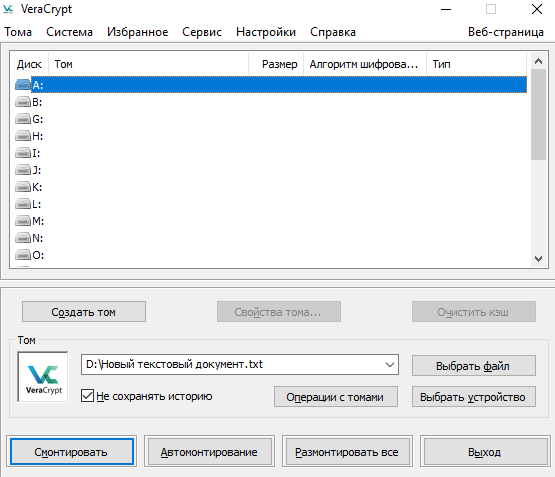


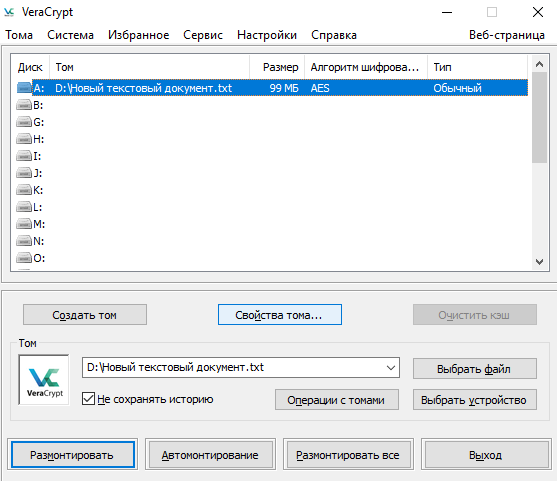




После начнётся шифрование и вам предложат создать энтропию движением мыши. После заполнения шкалы, нажмите “разметить”. После непродолжительного ожидания вам предложат создать секретный том внутри внешнего. Процесс его создания аналогичен созданию внешнего.

Чтобы расшифровать файловый контейнер необходимо выбрать немонтированный диск из списка VeraCrypt, найти необходимый файловый контейнер и нажать кнопку “Смонтировать”. Вам предложат ввести пароль. Введите пароль от необходимого тома (внешний или скрытый) и получите смонтированный том в списке VeraCrypt.





Шифрование несистемного диска/раздела почти полностью идентично, за исключением того факта, что нужно будет указать, намерены ли вы хранить в этом разделе файлы свыше 4ГБ.