Всем салют, дорогие друзья!

Хотелось бы выразить Вам благодарность за оказанное доверие и поздравить с поступлением в нашу академию!

Hacker Place Academy открывает Вам свои двери и мы надеемся, что знания полученные в её стенах кардинально изменят жизнь каждого из вас.

Погнали!

ПОГРАММА ОБУЧЕНИЯ "HACKER PLACE ACADEMY"

Безопасность и Анонимность
- Настройка полностью анонимной и безопасной системы
- Подмена своих IP и Mac адресов
- Секреты правильной настройки ПО
- Защита своих данных
- Как не оставить ни единой зацепки в сети Интернет
- Анонимность в реальной жизни
- Отмыв и обнал грязных денежных средств

Хакинг
- Взлом баз данных и последующая монетизация материала.
- Взлом серверов и их использование/продажа
- Взлом Wi-Fi точек доступа с помощью спец. версии ОС WifiSlax
- Освоение ОС Linux
- Проведение DDos атак
- Перехват трафика
- Нахождение и использование уязвимостей железа и ПО.
- Использование нашего авторского софта для взлома

Вирусознание
- Создание своих собственных вирусов и их использование
- Настройка и использование вирусов
- Заражение и контроль чужих машин
- Создание и управление ботнетом
- Обход антивирусов

4. Социальная инженерия
- Как втереться в доверие
- Как взломать человека
- Социальный хакинг
- СИ для распространения вирусов
- Ошибки и правильная стратегия в общении
- Создание убедительных аргументов
- Манипулирование сознанием
- Методы психологического воздействия на человека
- Манипулировать поведением

Обучение мы начнем с самого главного для любого хакера. Поскольку вы уже здесь, то догадались, что наш первый раздел:

«БЕЗОПАСНОСТЬ И АНОНИМНОСТЬ»

РАЗДЕЛ ВКЛЮЧАЕТ В СЕБЯ ТАКИЕ ТЕМЫ, КАК:

- *Настройка полностью анонимной и безопасной системы*
- *Подмена своих IP и Mac адресов*
- *Секреты правильной настройки ПО*
- *Защита своих данных*
- *Как не оставить ни единой зацепки в сети Интернет*
- *Анонимность в реальной жизни*
- *Отмыв и обнал грязных денежных средств*

Дебаты о анонимности и способов ее реализации никогда не утихают на формах даркнета. А все это из-за разных потребностей и разных моделей угроз. Представим, что ты хочешь оставить гневный коммент о правительстве в соц. сети и при этом не сесть. Что же для этого нужно? SSH-туннель? Может быть Tor или VPN? А может быть все сразу? НЕТ! Достаточно неприметно одеться, а может даже перестраховаться и нацепить очки или шарф, заботливо связанный бабулей. Далее мы отправляемся на крупный рынок вашего города и покупаем SIM-карту и Б/У смартфон, чем старше – тем лучше. Далее мы едем в самый дальний уголок вашего города, там включаем смартфон и делаем свои делишки, после благополучно там же его и уничтожаем. Можно спать спокойно. Анонимность с оценкой «отлично».

Но что если тебе нужно не просто оставить разовый комментарий, не просто скрыть свой IP-адрес от какого-то сайта? Что если необходим такой уровень анонимности,

который составит сложнейшую головоломку и практически не даст возможности для раскрытия на любом уровне? А также сможет скрыть и сам факт использования средств анонимизации. Именно об этом мы и поговорим.
Идеальная анонимность, как и все идеальное — это скорее утопия, но приблизиться к ней вплотную ты сможешь спокойно, потому что ты поступил в наш университет. Происходит это все за счет множества различных слоев защиты. Когда одна технология начинает дополнять и усиливать другую, и даже когда для твоей идентификации применяются отпечатки параметров системы и другие методы, ты по-прежнему остаешься неотличимым от общей массы пользователей сети. В данном разделе мы научим тебя, как этого добиться.

Для начала разделим анонимность на 4 уровня:

1. Базовый уровень защиты
2. Средний уровень защиты
3. Высокий уровень защиты
4. God' mode (Режим Бога)

Давайте разберем каждый из них подробнее.

Базовый уровень защиты

Базовый уровень безопасности и анонимности, выглядит так:
клиент → VPN/TOR/SSH-тунель → цель.

Схема базового уровня - это лишь продвинутая альтернатива прокси, позволяющая просто подменить **IP**. Один шаг, один клик и о анонимности тут говорить не придется. Уже не придется. Одна неверная или дефолтная настройка пресловутого **WebRTC** и ваш реальный **IP** уже известен. Данный тип защиты уязвим и перед **компрометацией узла**, и перед **fingerprints** и перед простым анализом **логов** у провайдера и в дата центре.

Часто на просторах Телеграмм встречаются статьи, воспевающие **частный VPN**, представляя его лучше чем **публичный**, т.к. человек уверен в своей настройке системы. Давайте на секунду представим, кому-то известен твой **внешний IP**, соответственно известен и **дата центр**, соответственно дата центру известно, какому серверу этот IP принадлежит. Сложно ли на месте, установить с какого реального IP к этому серверу подключались? Если ты там один клиент? Ответ очевиден. Когда клиентов, например 100, 1000 - тут уже все намного сложнее.

Это даже не касаясь аспектов, что редкий человек, заморочится на шифрованные диски и защиту от выемки, врятли бы даже заметил, если его сервер перезагрузят с

init level 1 и включат **логи** на **VPN**, описав это как «небольшие технические проблемы в дата центре». Да и разве это вообще нужно, если известны все входящие адреса на сервер и исходящие с него же?

Что же касается **Tor,** во-первых, его использование напрямую может вызывать подозрение, а во-вторых, выходные ноды, которых около 1000 штук известны и многие из них забанены, для многих сайтов это как красная тряпка. Например в **Cloudflare** есть возможность в **Firewall**'е разрешать или принимать подключения из сети Tor. В качестве страны следует использовать **T1**. Кроме того, использование Tor намного медленнее VPN (*Скорость в сети Tor на данный момент не превышает 10 мбит, а часто находится на уровне 1-3 мбит*).

Итог: Если вам нужно просто не носить по миру свой открытый паспорт и обходить простейшие запреты на сайты, иметь хорошую скорость соединения и возможность полностью пускать весь трафик через другой узел, то следует выбрать VPN. И на эту роль лучше подходит платный сервис, за те же деньги, что вы отдали бы за свой VPS, в 1-й стране, который еще нужно настроить и как-никак поддерживать, вы получите десятки стран и сотни или даже тысячи выходных IP.

В этом случае нет смысла использовать Tor, но в каких-то случаях и Tor является хорошим решением, особенно, если существует еще дополнительный слой безопасности, такой как VPN или SSH-туннель. Но об этом дальше.

Средний уровень защиты

Средний уровень безопасности и анонимности, выглядит так:
Клиент → VPN → Tor → цель

Это оптимальный и рабочий инструмент, для любого, не безразличного к подмене IP-адреса человека, это именно тот случай, когда сочетание технологий усилило каждую из них. Но не стоит питать иллюзий, да, узнать твой реальный адрес, будет затруднительно, но ты по-прежнему подвержен всем тем же атакам, что и выше. Твое слабое место — это твое физическое место работы, твой компьютер.

Высокий уровень защиты

Высокий уровень безопасности и анонимности, выглядит так:
Клиент → VPN → Удаленное рабочее место (через RDP/VNC) → VPN → цель

Рабочий компьютер должен быть не твой, а удаленный, например, на Windows 8, с Firefox, парой плагинов вроде Flash, парой кодеков, [ВНИМАНИЕ] никаких уникальных шрифтов и прочих плагинов. **Скучный и неотличимый от миллионов других** в сети. И

даже в случае какой-либо утечки или компрометации твоей системы, ты все равно остаешься прикрыт еще одним VPN'ом

Раньше считалось, что высокий уровень анонимности достигался путем использования Tor/VPN/SSH/Socks, но не сегодня. Поэтому обязательно добавляем еще и использование удаленного рабочего места в эту схему.

God' mode (Режим Бога)

Клиент → Double VPN (*в разных дата центрах, но рядом друг с другом*) → Удаленное рабочее место + Виртуальная машина → VPN → цель

Предлагаемая схема - это первичное подключение к **VPN** и вторичное подключение к **VPN** (*на случай, если 1-й VPN будет скомпрометирован, через какую либо утечку*), для скрытия трафика от провайдера и с целью не выдать свой реальный IP-адрес в дата центре с удаленным рабочим местом. Далее установленная **виртуальная машина** на этом сервере. *Зачем нужна виртуальная машина я думаю понятно?*
- Чтобы каждую загрузку делать откат к самой стандартной и банальной системе, со стандартным набором плагинов. Именно на машине с удаленным рабочим местом, а не локально. Люди, которые использовали виртуальную машину локально, а из под нее **TripleVPN** на эллиптических кривых, однажды зайдя на whoer.net, очень удивились увидеть в графе **WebRTC** свой реальный и настоящий **IP-адрес**. Какую ловушку реализуют завтра, обновя тебе браузер, не знает никто, главное **не держи ничего локально**. *Кевин Митник это 30 лет назад уже знал*.

Данная схема неоднократно использовалась в наших делах. Тормоза — приличные, даже если географически вся схема составлена правильно. Но терпимые. В данном случае, подразумевается, что человек не разносит сервера на пути по разным континентам.
Допустим ты физически находишься в Москве, так и строй схему так, чтобы *первый* **VPN** *тоже был в Москве*, второй, например, в Милане, а удаленное рабочее место, например, в Италии и конечный VPN, например, в Беларуси. Логика построения должна быть такой, что не стоит использовать все сервера внутри, например, еврозоны. Все дело в том, что там хорошо налажено сотрудничество и взаимодействие различных структур, но при этом не стоит их разносить далеко друг от друга. ***Соседние государства, ненавидящие друг-друга — вот залог успеха твоей цепочки!***

Что бы быть ультра-неуязвимым - можно еще добавить автоматическое посещение веб-сайтов в фоновом режиме, с твоей реальной машины как имитацию серфинга, чтобы не было подозрения, что ты используешь какое-то **средство анонимизации**. Так

как трафик идет лишь к одному IP-адресу и через один порт. Можно добавить использование ОС **Whonix/Tails**, получать доступ в интернет через **публичный Wi-Fi** в кафе *(практически все пароли есть в приложении **Wi-Fi Map**)*, при этом **обязательно** поменяв данные сетевого адаптера, которые тоже могут привести к **деанонимизации**. Если дело очень серьезное, то есть необходимость сменить внешность (вспоминаем про очки, бабушкин шарф и даже накладные усы и парики), чтобы не быть идентифицированы по лицу в том же самом кафе. Уже внедрены технологии, позволяющие делать. *К сожалению, это будущее и оно уже здесь.* Ты можешь быть определен, как по наличию координат местонахождения, в файле фотографии, сделанной твоим телефоном до диагностики определенного стиля письма. Просто помни об этом.

Fingerprints, как и попытки определения использования **VPN**, по средствам замера времени отправления пакета от пользователя к вебсайту и от вебсайта к IP-адресу пользователя (не берем в расчет такой «костыль» как блокировка только входящих запросов определенного вида) обойти не так просто. Обмануть кое-что можно, одну-другую проверку, но нет гарантий, что завтра не появится очередное «зло». Именно поэтому тебе необходимо удаленное рабочее место, именно поэтому нужна чистая виртуалка, именно поэтому это лучший совет, который можно дать, на данный момент. Стоимость такого решения может начинаться всего лишь от 40$ в месяц. Но учти, что для оплаты, следует использовать исключительно крипту.

Самая важная часть и самый главный залог успеха в защите анонимности — разделение работы с персональными данными и с данными секретными, представляющими какую-то ценность. Все эти туннели и выстроенные схемы, будут абсолютно бесполезны, если ты с нее зайдешь, например, в свой почтовый ящик или ВК.

Поговорим о подмене MAC-адреса своего сетевого адаптера. Это понадобится, например, если ты будешь использовать свой ПК для подключения к публичному Wi-Fi, для целей указанных в разделе «God' mode (Режим Бога)»

Каждый сетевой интерфейс, подключенный к сети — будь то маршрутизатор, беспроводное устройство или сетевая карта, — имеет уникальный **MAC-адрес**. Эти адреса, иногда называемые **физическими** или **аппаратными адресами**, устанавливаются заводом-изготовителем, но обычно можно их изменять при помощи программного обеспечения.

— Для чего вообще нужны MAC-адреса?
—На самом низком уровне сети сетевые интерфейсы, подключенные к сети, используют MAC-адреса для связи друг с другом. Когда браузеру на Вашем компьютере необходимо загрузить веб-страницу с сервера в Интернете, этот запрос проходит через несколько уровней протокола TCP/IP. Введенный веб-адрес преобразуется в IP-адрес сервера. Компьютер отправляет запрос маршрутизатору, который затем отправляет его в Интернет. Однако на уровне «железа» сетевая карта ищет только другие MAC-адреса для интерфейсов в той же сети. Она знает только как отправлять запрос на MAC-адрес сетевого интерфейса маршрутизатора.

В дополнение к основному сетевому использованию MAC-адреса часто используются в других целях:

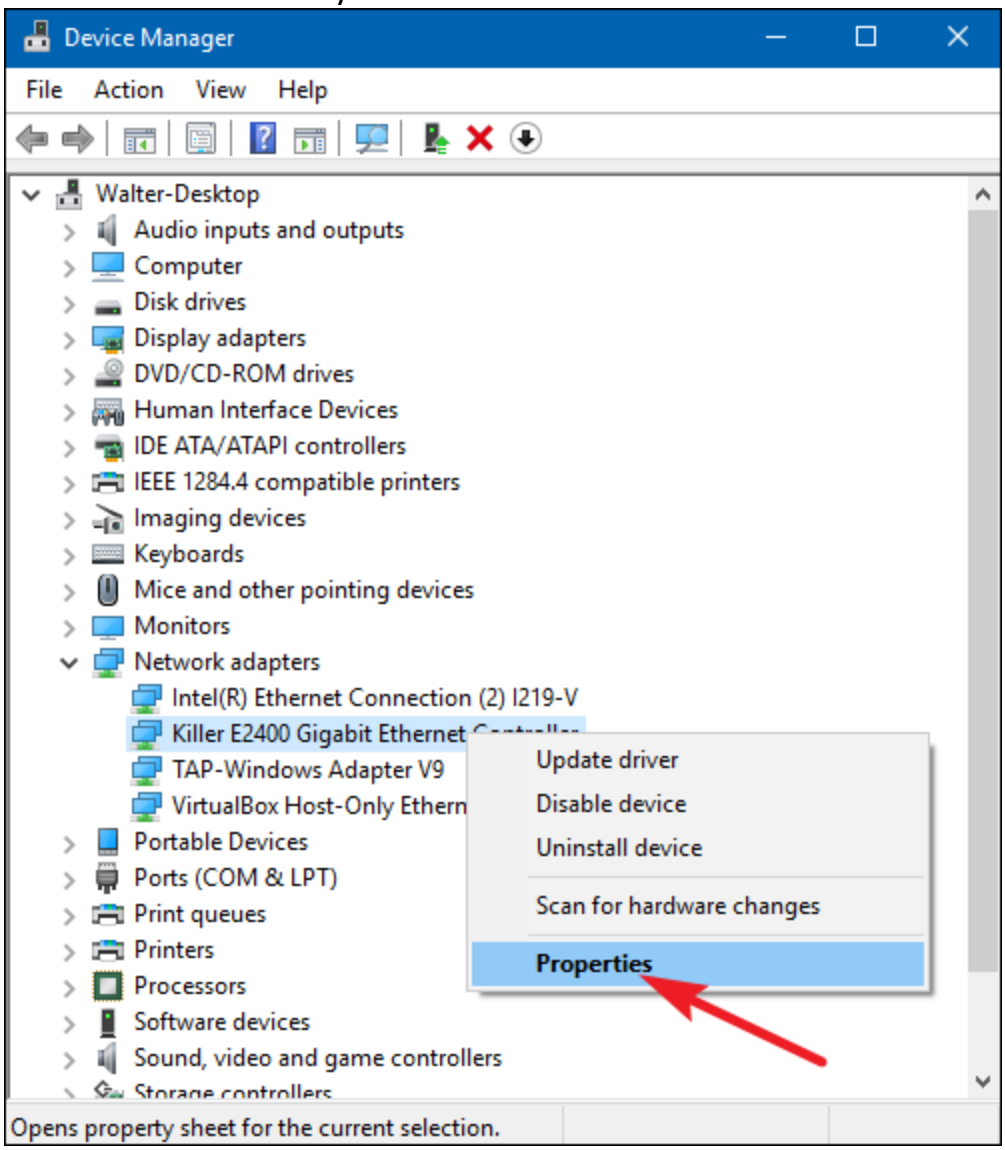
- **Статический IP:** маршрутизаторы позволяют назначать компьютерам статические IP-адреса. При подключении устройства он всегда получает определенный IP-адрес, если он имеет соответствующий MAC-адрес
- **Фильтрация MAC-адресов:** сети могут использовать фильтрацию MAC-адресов, разрешая подключение к сети только устройствам с определенными MAC-адресами. Это не очень хороший инструмент безопасности, потому что люди могут подменить свои MAC-адреса.
- **MAC-аутентификация:** некоторые поставщики услуг Интернета могут требовать проверки подлинности с помощью MAC-адреса и разрешить подключение к Интернету только устройству с этим MAC-адресом. Для подключения может потребоваться изменить MAC-адрес маршрутизатора или компьютера.
- **Идентификация устройства:** многие сети Wi-Fi в аэропорту и другие общественные сети Wi-Fi используют MAC-адрес устройства для его идентификации. Например, сеть Wi-Fi аэропорта может предоставить бесплатные 30 минут, а затем запретить определенному MAC-адресу от доступ к Wi-Fi. Для получения дальнейшего доступа к Wi-Fi нужно просто изменить свой MAC-адрес.
- **Отслеживание устройств:** поскольку они уникальны, MAC-адреса можно использовать для отслеживания. Когда вы ходите по улице, смартфон сканирует близлежащие сети Wi-Fi и передает свой MAC-адрес. Компания «Renew London» использовала мусорные корзины в городе Лондон для отслеживания движения людей в городе на основе их MAC-адресов. Apple iOS 8 будет использовать случайный Mac-адрес каждый раз при сканировании близлежащих сетей Wi-Fi, чтобы предотвратить такое отслеживание.

*Следует иметь в виду, что **каждый сетевой интерфейс имеет собственный MAC-адрес**. Таким образом, на обычном ноутбуке, оснащенном Wi-Fi-портом и проводным Ethernet-портом, каждый интерфейс беспроводной и проводной сети имеет свой уникальный MAC-адрес.*

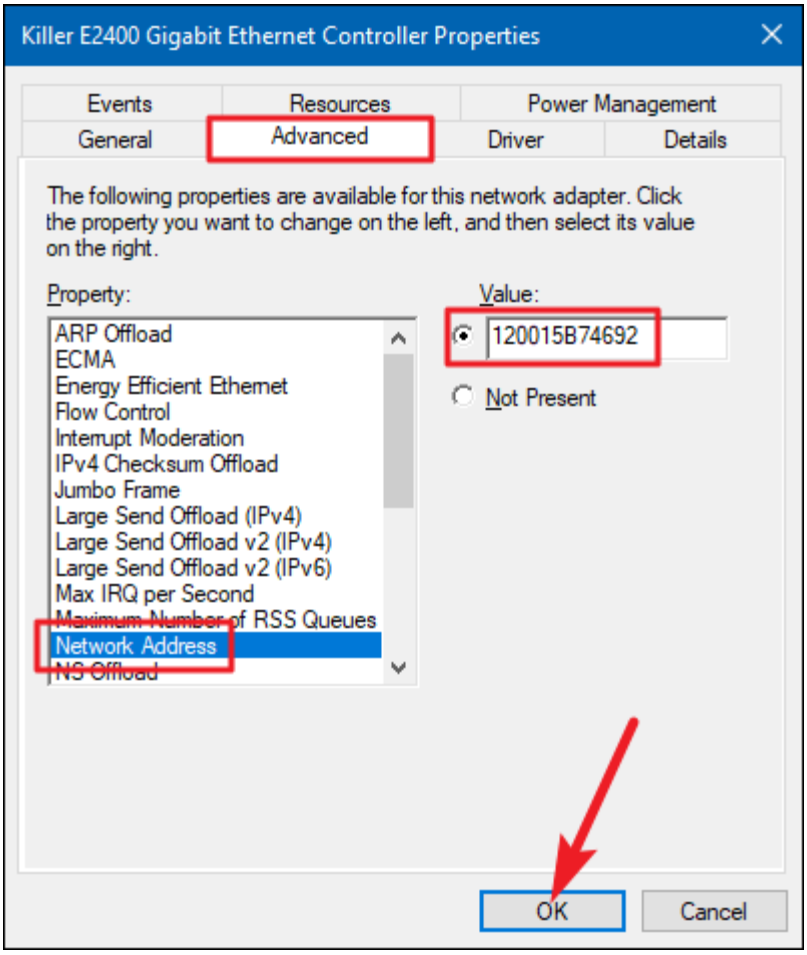
Изменение MAC-адреса в Windows

Большинство сетевых карт позволяют устанавливать свой MAC-адрес из панели конфигурации диспетчера устройств, хотя некоторые сетевые драйверы могут не поддерживать эту функцию.

1. Сначала открой Диспетчер устройств. В Windows 8 и 10 нажми Win+X, а затем выбери пункт «Диспетчер устройств» в меню Power User. В Windows 7 нажми клавишу Windows, введи «Диспетчер устройств», чтобы найти его, а затем выбери «Диспетчер устройств». Приложение диспетчера устройств будет выглядеть одинаково независимо от используемой версии Windows.
2. В диспетчере устройств в разделе «Сетевые адаптеры» щелкни правой кнопкой мыши по сетевому интерфейсу, который хочешь изменить, и выбери в контекстном меню пункт «Свойства».



3. В окне «Свойства» на вкладке «Дополнительно» выбери «Сетевой Адрес» в списке свойств. *Если этот параметр не отображается, сетевой драйвер не поддерживает эту функцию.*
4. Включи параметр «Значение» и введи требуемый MAC-адрес без разделителей — не используй дефисы или двоеточия. Нажми кнопку «OK».



Так же MAC-адрес легко изменить, используя программу Technitium MAC Address Changer

Прямая ссылка на скачивание: https://ivstar.net/download/TMAC_Setup.exe

Как сменить MAC-адрес с помощью программы:

1. Запусти программу и в списке выбери адаптер у которого ты хочешь изменить MAC-адрес.

2. Ниже выбранного адаптера появится подробная информация о нем. Там же в закладке Информация в поле с чёрточками введи свой MAC-адрес, либо нажми на кнопку Random MAC для случайной генерации. Либо под строкой ввода адреса выбери мак из диапазона конкретных производителей

3. Нажмите кнопку Change now!

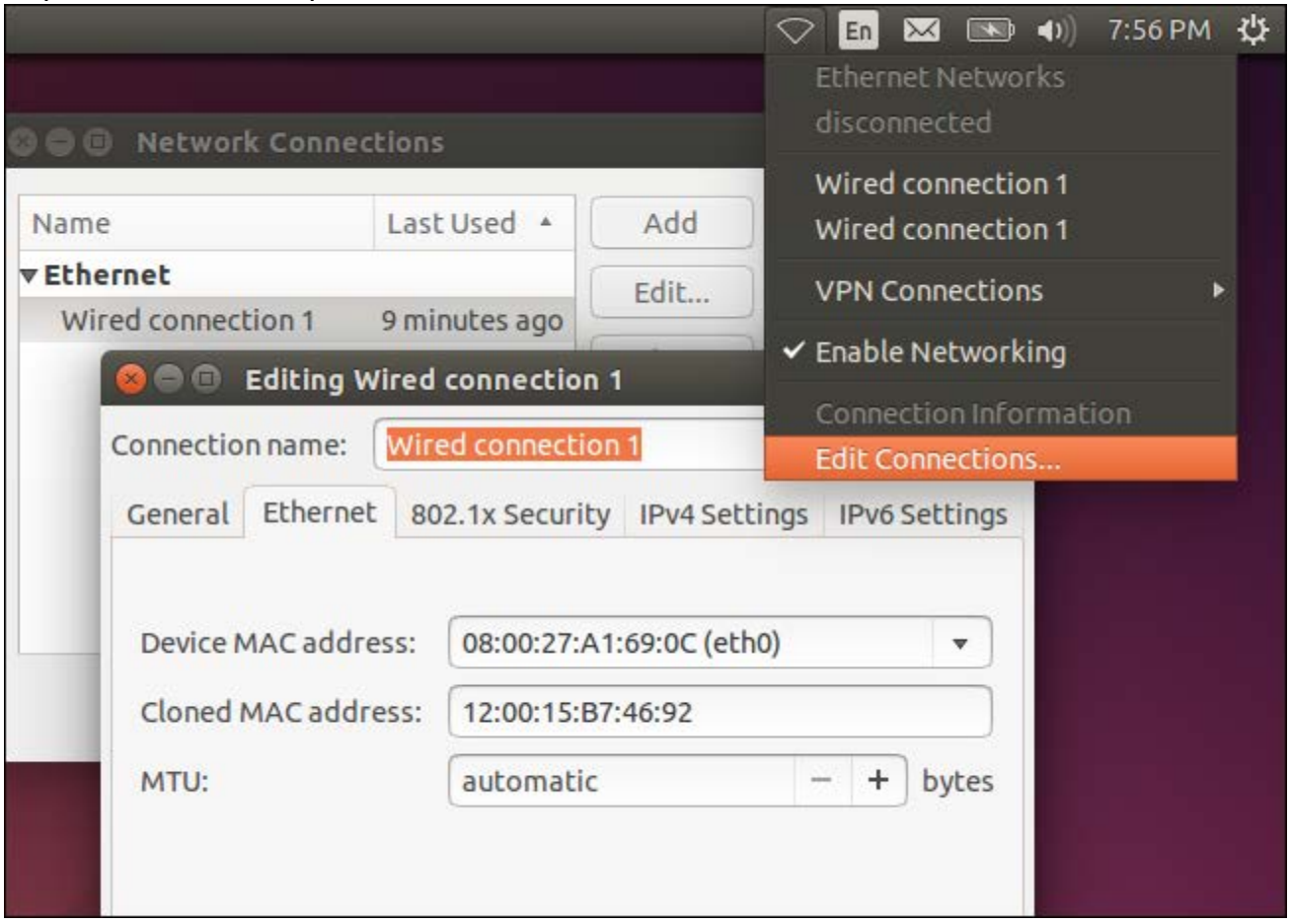
*Чтобы восстановить исходный MAC- адрес
сетевого адаптера, выбери снова нужный адаптер и нажми внизу окна кнопку Restore original

Изменение MAC-адреса в Linux

Современные дистрибутивы Linux обычно используют **Диспетчер Сети**, который предоставляет графический интерфейс для подмены MAC-адреса.

Например, в Ubuntu:

- щелкни по значку сети на верхней панели;
- выбери «Изменить соединения…»;
- выбери сетевое подключение, которое требуется изменить;
- нажми кнопку «Изменить»;
- на вкладке Ethernet введи новый MAC-адрес в поле «клонированный Mac-адрес», а затем сохрани изменения.



Ты можешь проверить, что изменение вступили в силу, выполнив команду, отображающую сведения о сетевом подключении, и проверив, какие MAC-адреса

*будут показаны сетевым интерфейсом после этого. В Windows запусти команду «**ipconfig /all**» в окне командной строки. В Linux запусти команду «**ifconfig**». Если необходимо изменить MAC-адрес маршрутизатора, этот параметр будет найден в веб-интерфейсе маршрутизатора.*

Защита своих данных

Попробуем выделить два основных подхода к защите информации. Данные можно зашифровать так, что их не сможет прочесть посторонний человек. Или их можно спрятать, чтобы злоумышленник даже не подозревал о том, что данные существуют. Замечательная программа **Veracrypt** решает обе задачи сразу.

Зашифровать информацию — примерно то же, что и положить в хороший сейф, только надежнее. Профессионал-"медвежатник" способен взломать запоры. Сейф можно попытаться взорвать. Обладая терпением и знаниями, можно попробовать подобрать код. Компьютерные программы (многие из которых бесплатны и доступны широкому кругу людей) умеют создавать такие электронные "сейфы", на вскрытие которых даже у крупных корпораций или спецслужб с их мощными компьютерами, деньгами и специалистами уйдут не часы и даже не дни, а годы. **Veracrypt** — одна из таких программ.

Veracrypt создает на диске компьютера защищенный (зашифрованный) том. Физически это файл, который может называться как угодно (по выбору пользователя). Операционная система Windows "видит" этот файл как отдельный диск. При записи на этот "диск" данные автоматически шифруются. При чтении — расшифровываются. Все происходит "на лету", пользователь работает так, как работал бы с обычным диском

Общее правило: *не храните такую информацию по принципу "а пусть будет". Если без нее можно обойтись — удалите.*

Как не вызвать подозрений

Бывает, однако, что сам факт использования шифрования способен вызвать нездоровый интерес злоумышленников *("если зашифровано, значит, что-то важное")*. Для некоторых людей это является решающим аргументом против шифрования. Давайте не будем ничего менять, говорят они. Меньше подозрений — меньше риска.

*Напоминаем, **данные можно не только зашифровать, но и спрятать***

Можно использовать **стеганографию**: скрывать важную информацию в безобидных файлах, например, в картинках. Есть программы, которые умеют это делать. Но стеганография подразумевает ручную работу. Этот метод в большей степени подходит для единовременной передачи какой-то краткой информации по электронной почте.

Для начала можно просто переименовать файл **Veracrypt**. Например, сделать его с расширением .avi. Он будет выглядеть как видео, скажем, кинофильм, и не вызовет подозрений

Неплохо, но мало. Файл-то все равно существует. Представь, что ты устроил свой сейф в стене и закрыл его картиной. Большинство людей увидит картину. Но если к нам нагрянут следователи с обыском, они перевернут все и, конечно, найдут за картиной сейф.

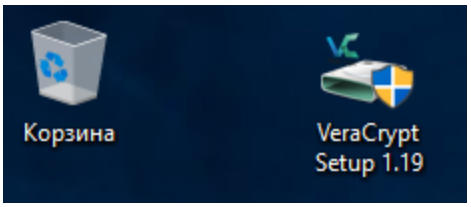
Обязательно найдут. Поэтому ***нужно убедить их, что они нашли именно то, что искали***. Хотя на самом деле вся важная информация будет храниться в другом месте.

Veracrypt позволяет создавать "спрятанный" том внутри обычного тома. Никто, кроме тебя, не знает, что "спрятанный" том вообще существует. Его невозможно увидеть и даже заподозрить. Поэтому даже если злоумышленникам в руки попадет защищенная Veracrypt информация, даже если они раздобудут пароль, они ни за что не догадаются, что внутри сейфа есть еще одно, маленькое, тайное отделение, где хранится то, что действительно важно.

Установка VeraCrypt

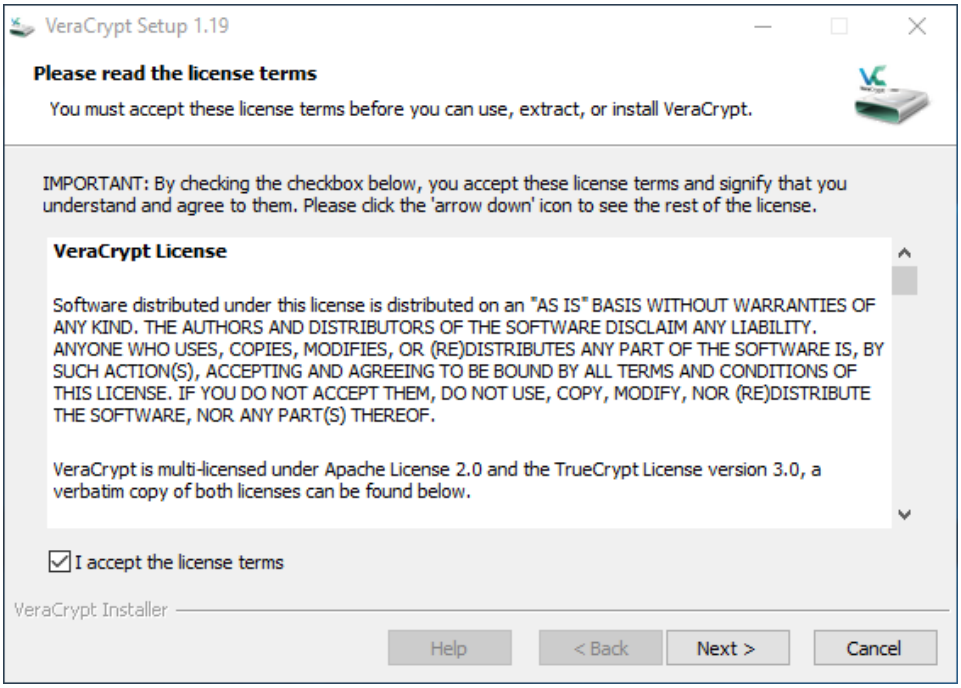
Чтобы у тебя не возникло вопросов, мы разберем установку VeraCrypt во всех подробностях.

Шаг 1. Дважды нажми на файл-установщик "VeraCrypt Setup.exe".

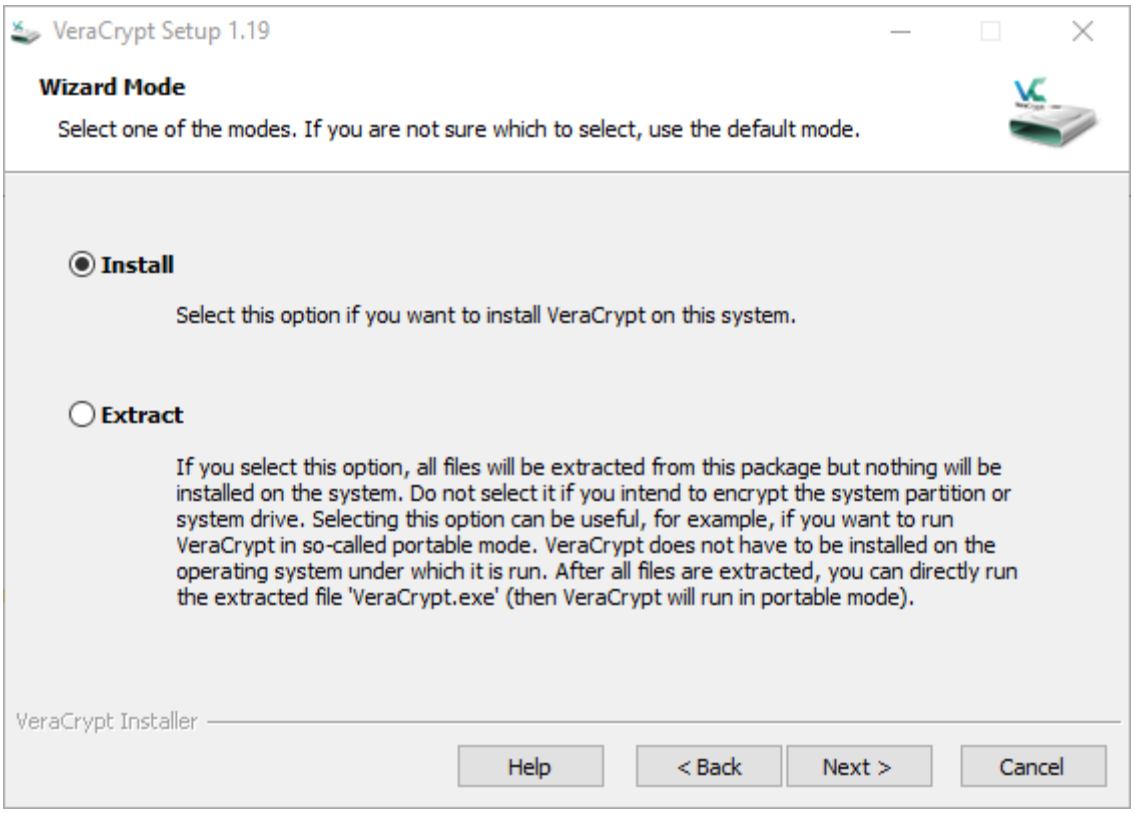


Ты увидишь запрос на разрешение изменений.

Шаг 2. Нажми кнопку **Да**, чтобы начать установку **VeraCrypt**. Появится окно с *лицензией*.



Шаг 3. Поставь галочку в поле *I accept the license terms (Я принимаю условия лицензии)* и **нажми** кнопку **[Next].** Далее тебе предстоит сделать выбор: *установить* VeraCrypt или *распаковать* его в виде *портативной версии*.



Режим *Установки*: подходит тем, для кого сам факт использования **VeraCrypt** не означает дополнительных рисков. Если доступ к **VeraCrypt** понадобится на *другом* компьютере, программу следует установить и там.

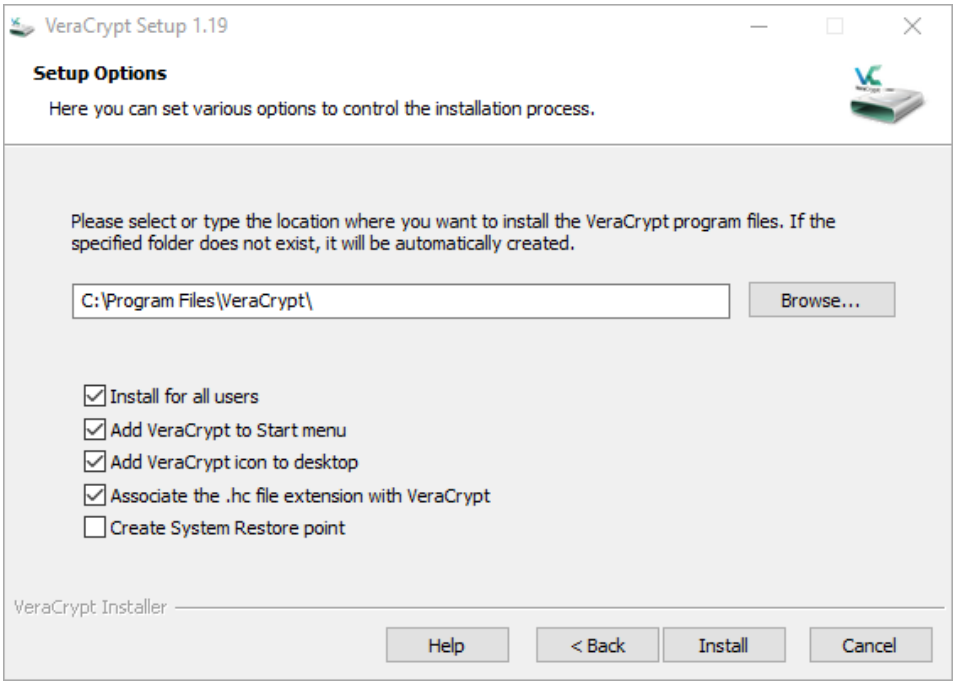
Режим *Распаковки*: для тех, кто предпочитает не устанавливать программу, а записать портативную версию **VeraCrypt** на USB-устройство. Это устройство можно брать с

собой и пользоваться **VeraCrypt** на любом компьютере с Windows (при наличии прав *администратора*).

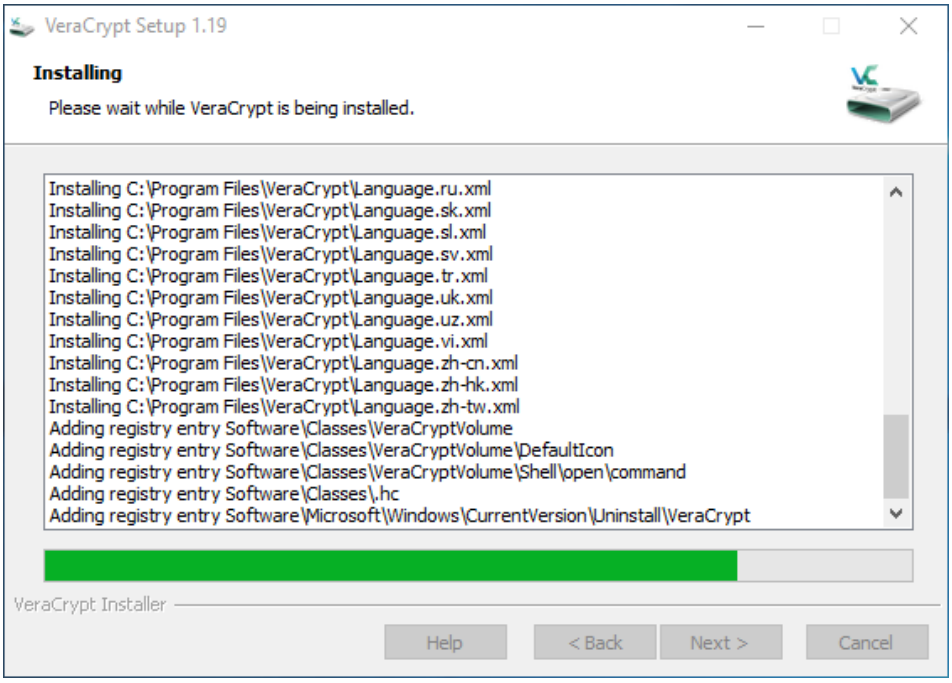
Важно. Даже в портативном режиме **VeraCrypt** оставляет некоторые следы на компьютере, где его запускают. Эти следы не раскроют содержимое зашифрованных файлов, но могут выдать присутствие **VeraCrypt** на компьютере.

Примечание. В нашем случае мы будем *устанавливать* **VeraCrypt**.

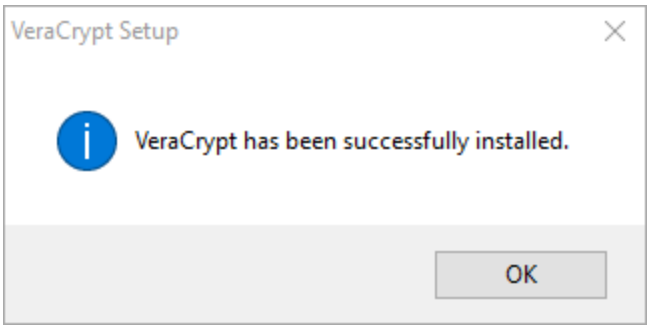
Шаг 4. Нажмикнопку **[Next]** и выбери, куда установить **VeraCrypt**.



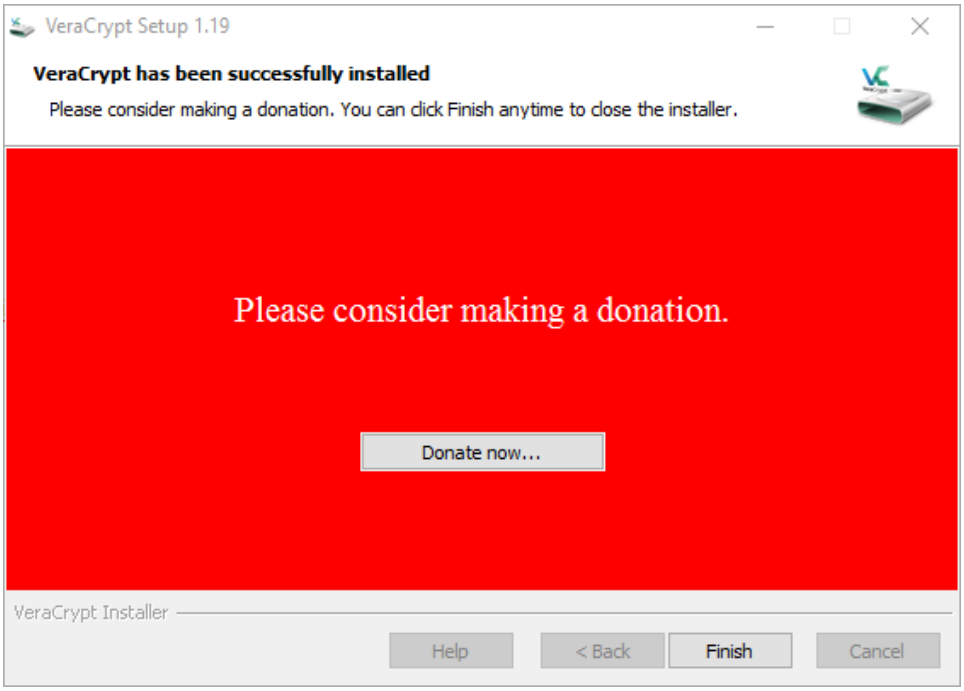
Шаг 5. Нажми кнопку **[Install]** для начала установки **VeraCrypt** в выбранную папку, как показано ниже.



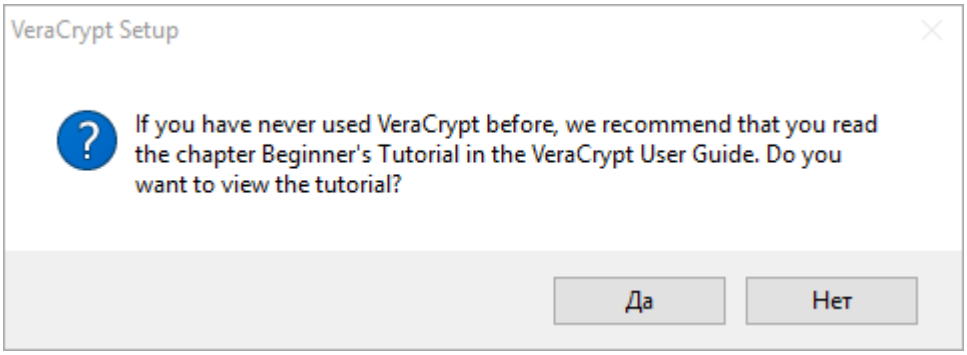
Когда установка завершится, ты увидишь сообщение.



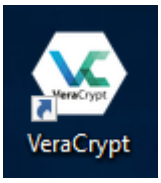
Шаг 6. Нажми кнопку **[OK]**, чтобы завершить установку. Программа предложит тебе сделать пожертвование для поддержки разработчиков **VeraCrypt**.



Шаг 7. Нажми кнопку **[Finish]**. Вам предложат руководство по **VeraCrypt**.



Шаг 8. Нажми любую кнопку, чтобы завершить установку **VeraCrypt**. Если ты не менял установки по умолчанию, на рабочем столе появится ярлык **VeraCrypt**.



Важно. *Если вы не хотите обнаруживать присутствие шифровального средства на своем компьютере, разумно удалить этот ярлык. Если использование шифровального средства может привлечь на вашу голову* серьезные *неприятности, лучше вовсе удалить* ***VeraCrypt*** *и выбрать* портативную версию *для USB-устройства.*

Создание обычного тома

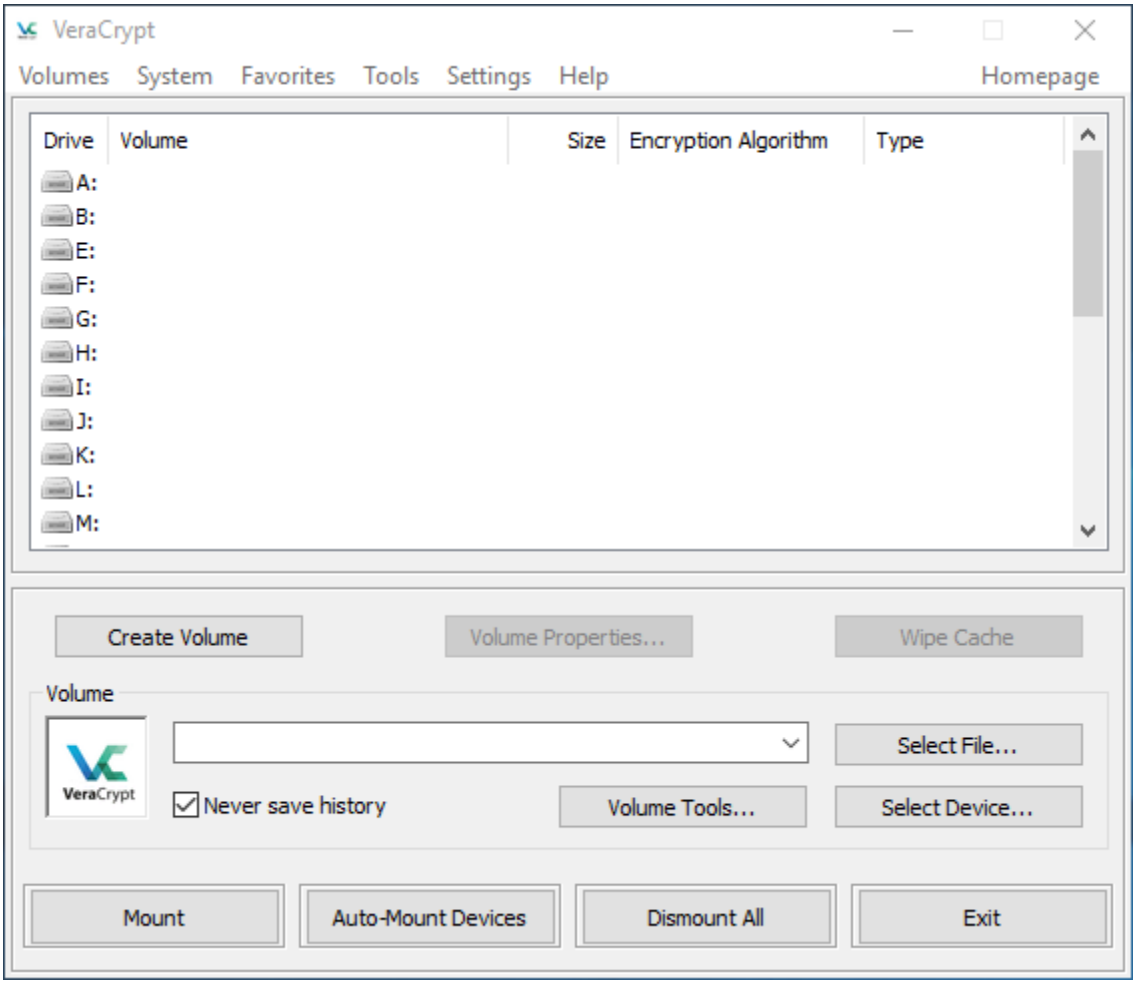
VeraCrypt позволяет создавать тома двух типов: **скрытый** и **обычный**.

Обычный том защищает ваши файлы паролем. Этот пароль нужно вводить всякий раз при начале работы с зашифрованным томом VeraCrypt.

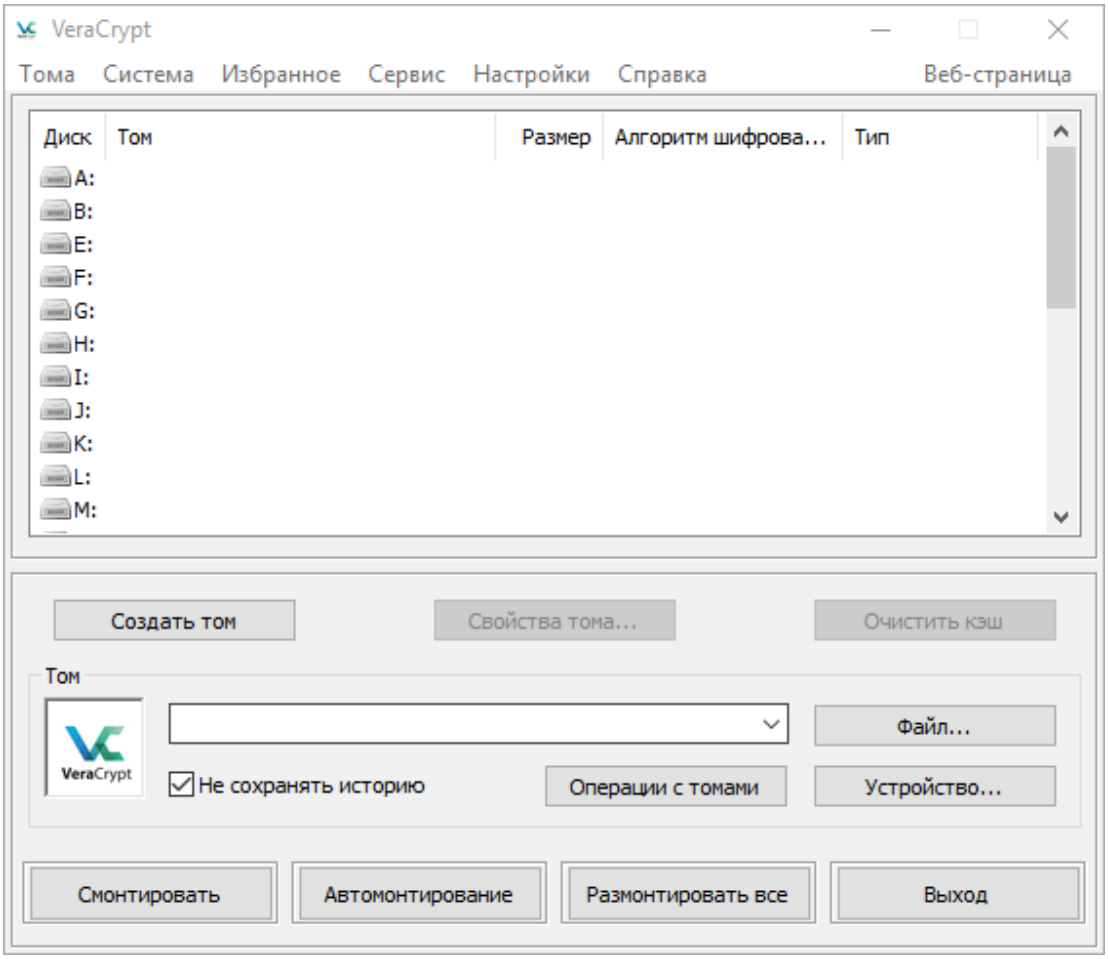
Скрытый том имеет *два* пароля. Ты можешь использовать один из них, чтобы открыть *маскирующий* обычный том, где хранятся не столь важные данные. Этой информацией не страшно рискнуть при крайней необходимости. Второй пароль дает доступ к скрытому тому, где хранится самое важное.

Давай разберем, как создать **обычный том**, а после перейдем к созданию **скрытого тома**.

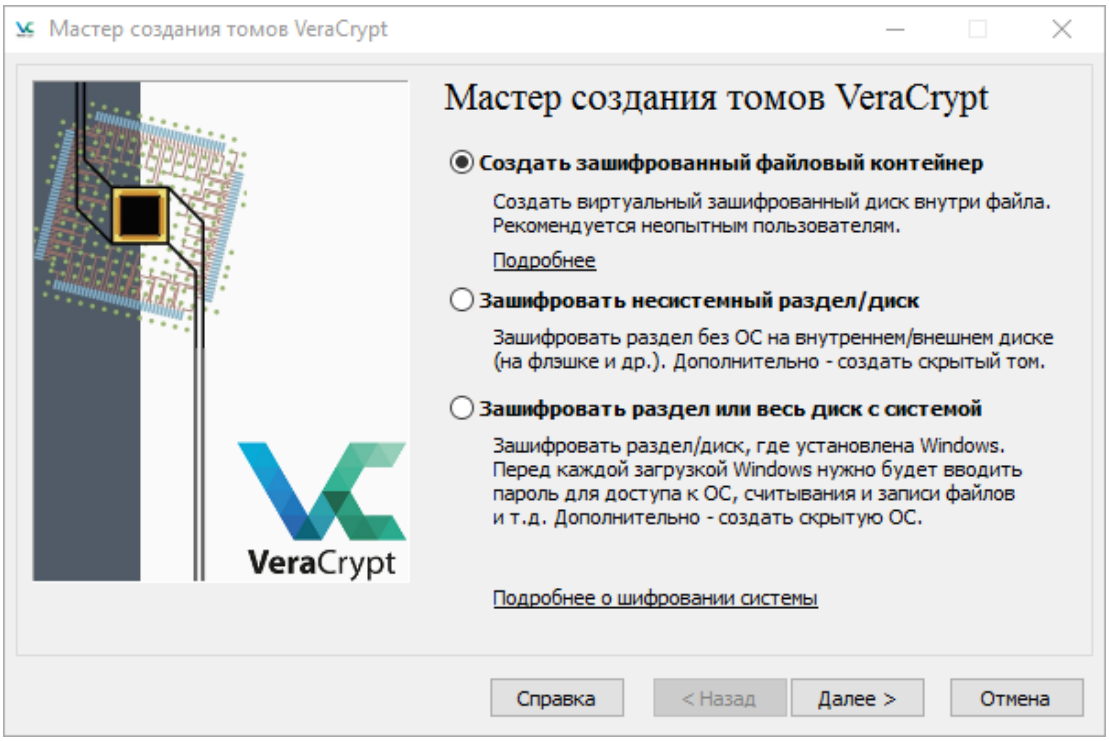
Шаг 1. **Запусти** VeraCrypt. Откроется главное окно программы.



Шаг 2. *(Переключи на русский язык, потребуется сделать один раз)* **Выбери** в меню **Settings > Language > Русский** и нажми кнопку **ОК**. Ты увидишь главное окно программы на русском языке.

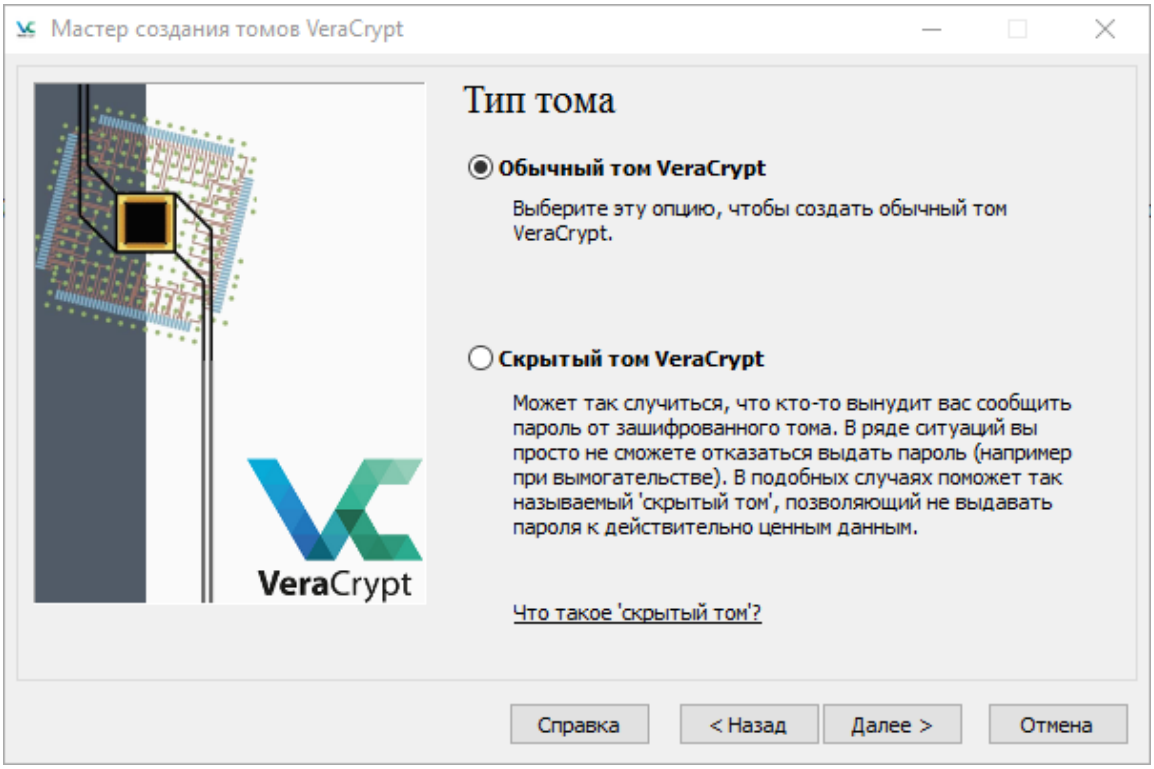


Шаг 3. Нажмите кнопку **[Создать том]**, чтобы запустить мастер создания томов.



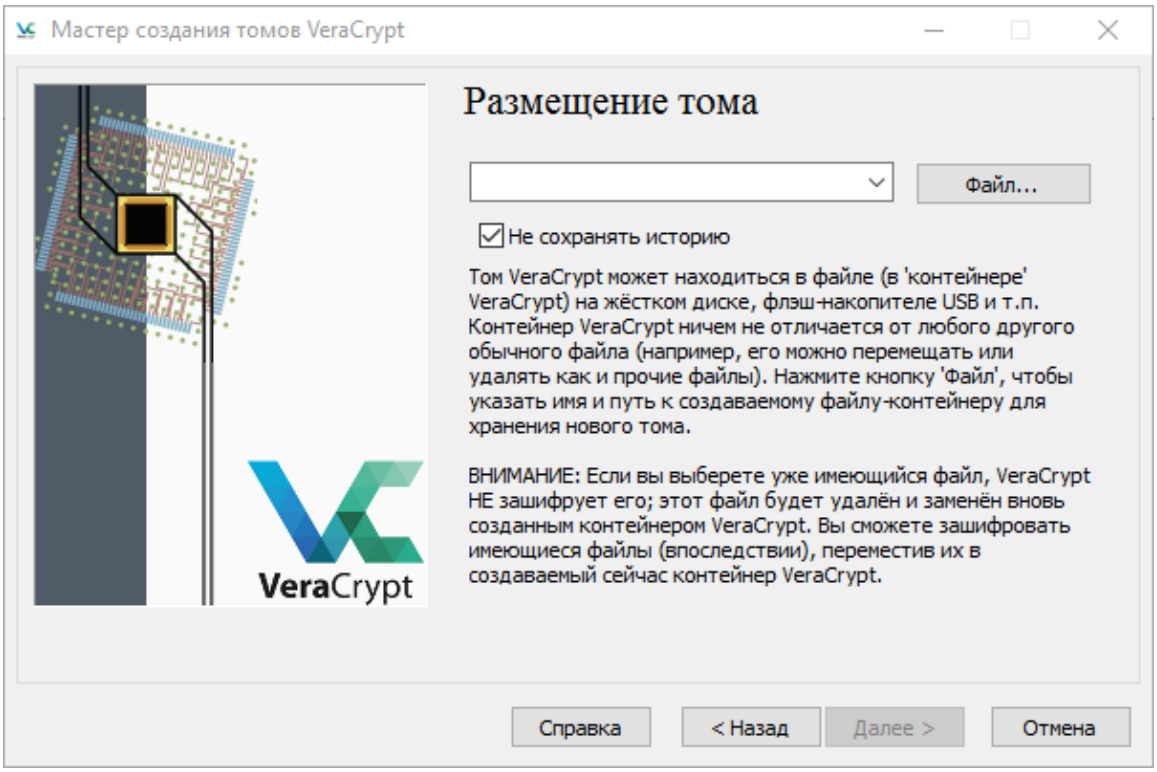
Файл-контейнер* VeraCrypt** – зашифрованный том, который хранится в одном файле. Этот *контейнер* можно переименовывать, перемещать, копировать или удалять, как любой иной файл. Мы создадим ***файл-контейнер.

Шаг 4. Нажми кнопку **[Далее]**.

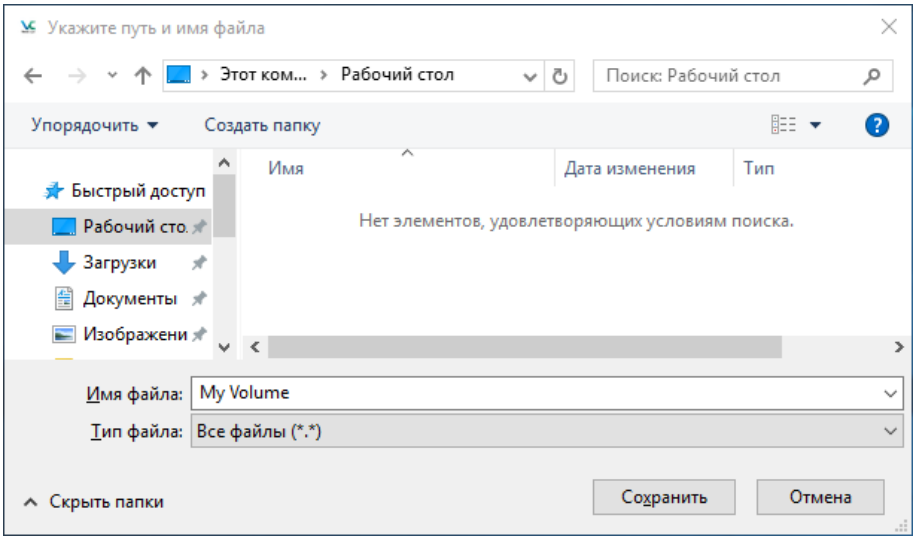


В этом окне можно выбрать, какой том ты хочешь создать: *обычный* или *скрытый*.

Шаг 5. Убедись, что выбран *Обычный том VeraCrypt*. **Нажми** кнопку **[Далее]**, чтобы выбрать название и место для *контейнера* VeraCrypt.



Шаг 6. Нажми кнопку **[Файл…]**, чтобы выбрать место для контейнера VeraCrypt и название файла.

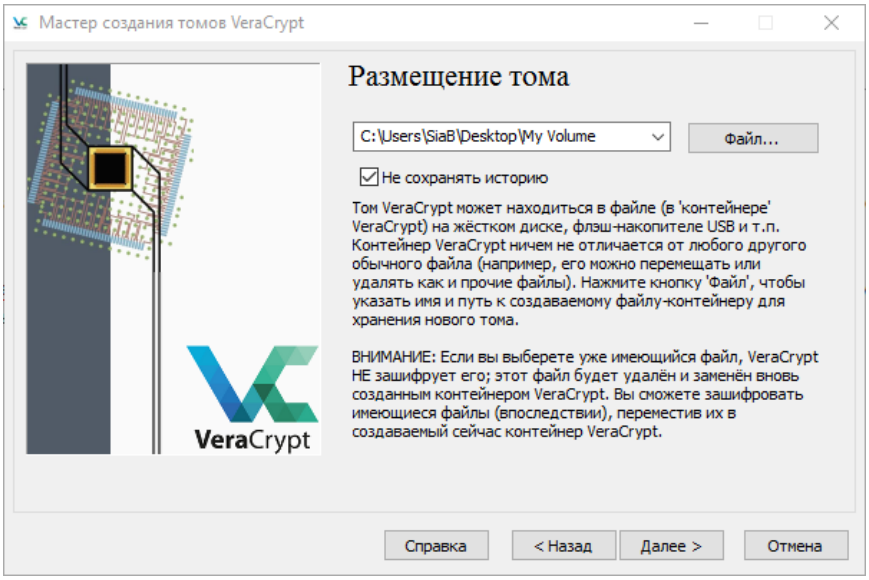


Шаг 7. Выбери папку и имя файла для своего будущего *контейнера* **VeraCrypt**.

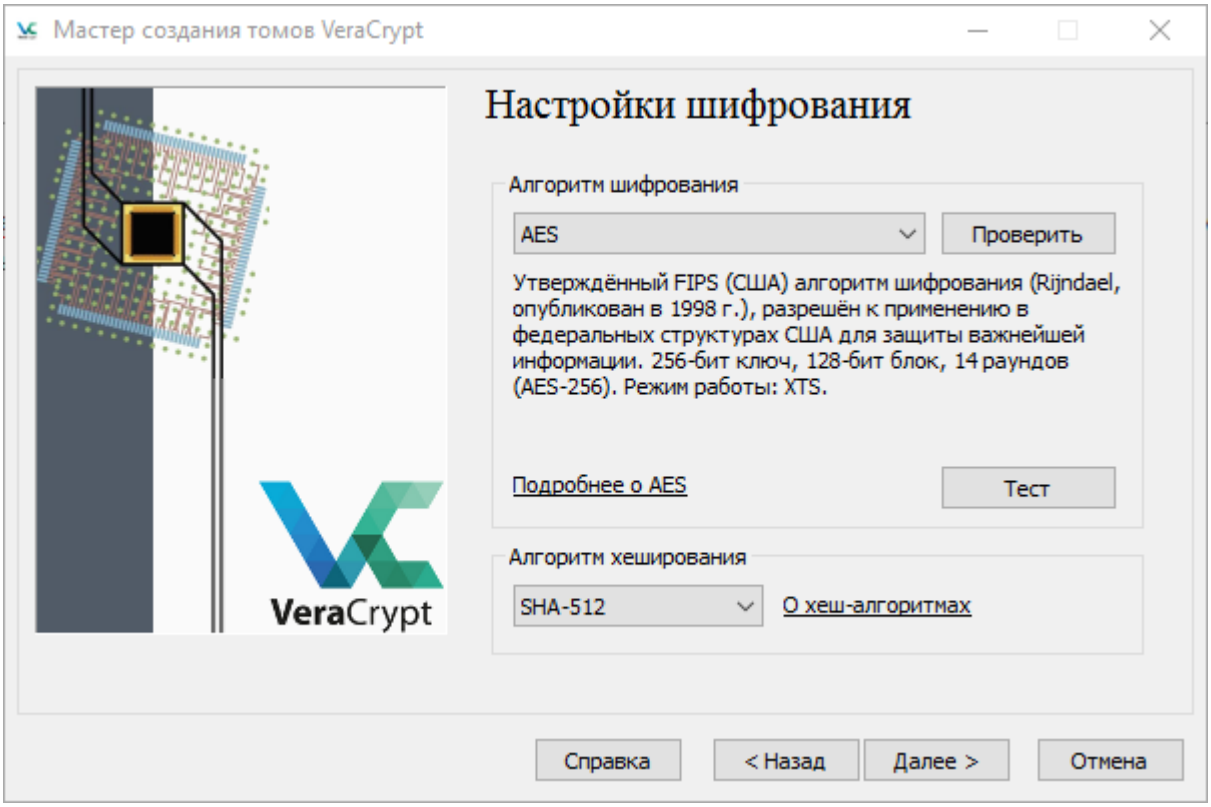
Нужно запомнить место и имя файла. В данном примере мы создадим *контейнер* с названием **My Volume** на **Рабочем столе**. Если ты хочешь создать контейнер **VeraCrypt** на **USB-устройстве** (например, флешке), просто открой нужную папку на ней (не на жестком диске компьютера) перед тем, как выбрать имя файла.

В нашем примере мы создаем *контейнер* (*том*) на *Рабочем столе*, но твой *контейнер* может иметь любое название и файловое расширение. Например, ты можете назвать его курсовая*.docx* или *holidays.mpg* в надежде на то, что случайный человек подумает, будто это документ Microsoft Word или видеофайл. Это один из способов замаскировать наличие контейнера VeraCrypt, хотя он вряд ли сработает против того, у кого достаточно времени и ресурсов для внимательного изучения вашего устройства.

Шаг 8. Когда ты выбрал место и название файла для контейнера VeraCrypt, **нажми** кнопку **[Сохранить]**.

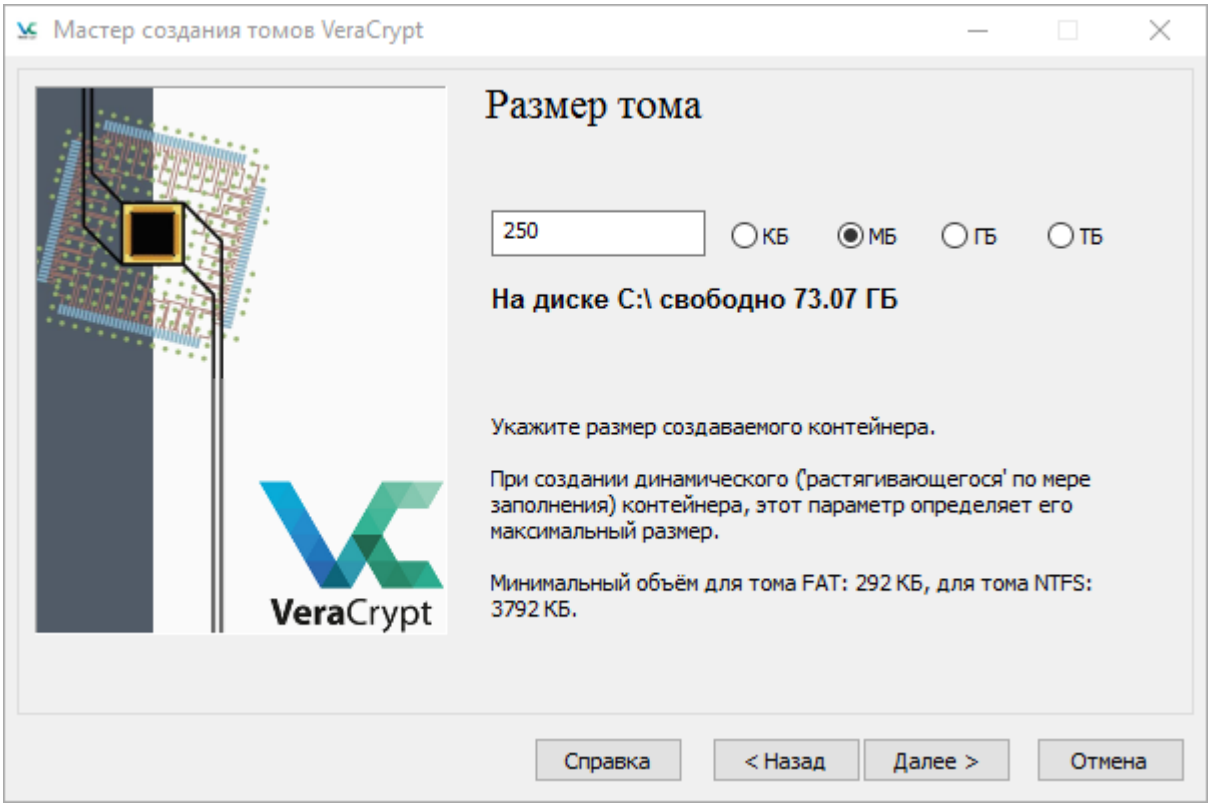


Шаг 9. Нажми кнопку **[Далее]** для выбора *параметров шифрования*.



Здесь вы можете выбрать метод (*алгоритм*) для шифрования и расшифровки файлов внутри вашего контейнера **VeraCrypt**. *Параметры по умолчанию можно считать безопасными,* есть смысл ничего не менять.

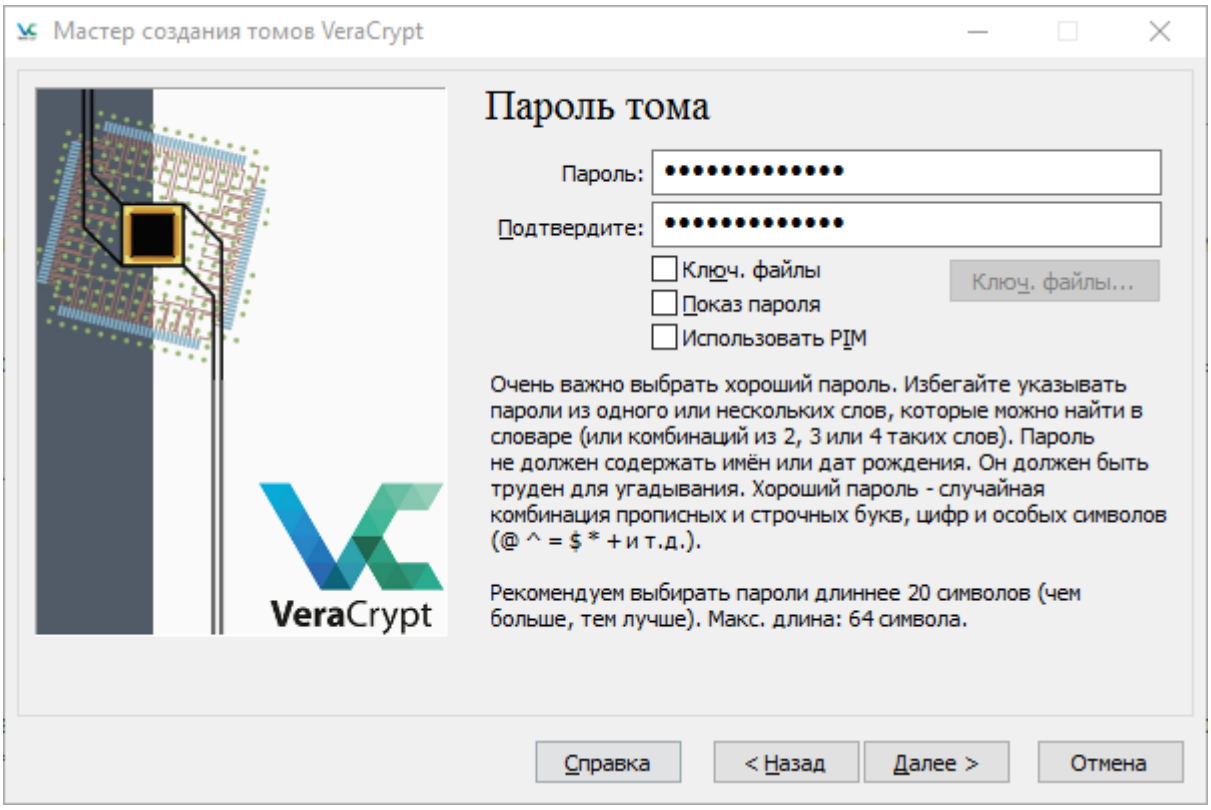
Шаг 10. Нажмикнопку **[Далее]** для выбора *размера тома*.



Окно *Размер тома* позволяет указать размер создаваемого *контейнера*. В качестве примера мы создадим контейнер 250 Мб, но ты можешь выбрать другой размер.

Оцени, сколько файлов ты туда хочешь записать, и, что более важно, *типы* этих файлов. Например, изображения и видео могут очень быстро заполнить небольшой контейнер VeraCrypt.

Шаг 11. Укажи размер тома, который собираешься создать. Убедись, что выбрал правильное значение в килобайтах, мегабайтах, гигабайтах или терабайтах. Потом **нажми** кнопку **[Далее]** для выбора пароля.

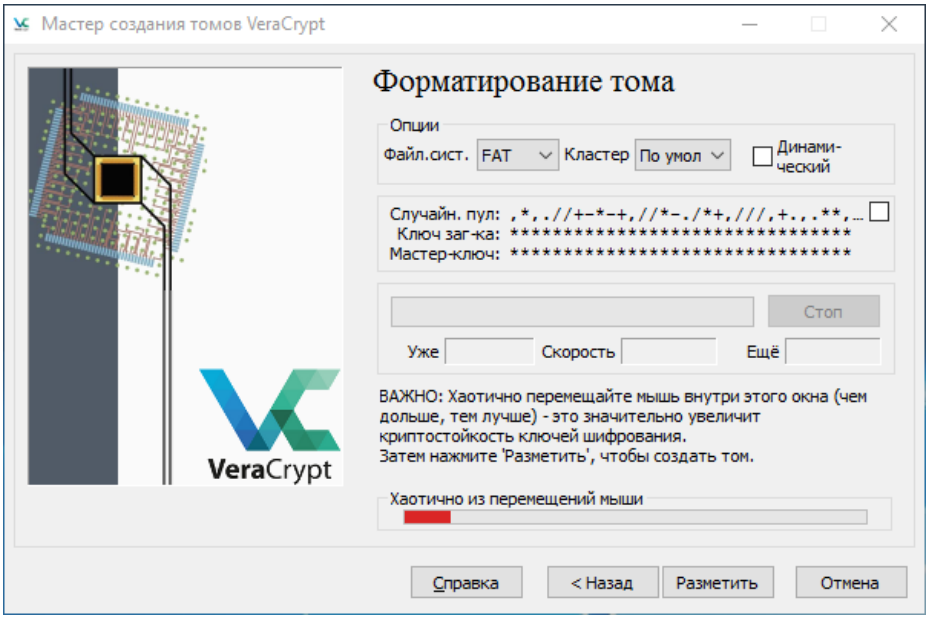


ВАЖНО. Выбор сложного пароля – один из самых ответственных шагов при создании тома VeraCrypt. Чем серьезнее пароль, тем лучше. Чтобы не ломать голову, придумывая и запоминая сложные пароли, можно воспользоваться *менеджером паролей* вроде **KeePassX**.

Шаг 12. Введи пароль и подтверди его.

Важно. Кнопка "Далее" останется серой, пока ты не введешь пароль дважды. Если пароль слабый, ты увидишь предупреждение. Подумай, не следует ли его изменить? Хотя **VeraCrypt** "согласится" с любым вашим паролем, информацию нельзя считать защищенной, если пароль слабый..

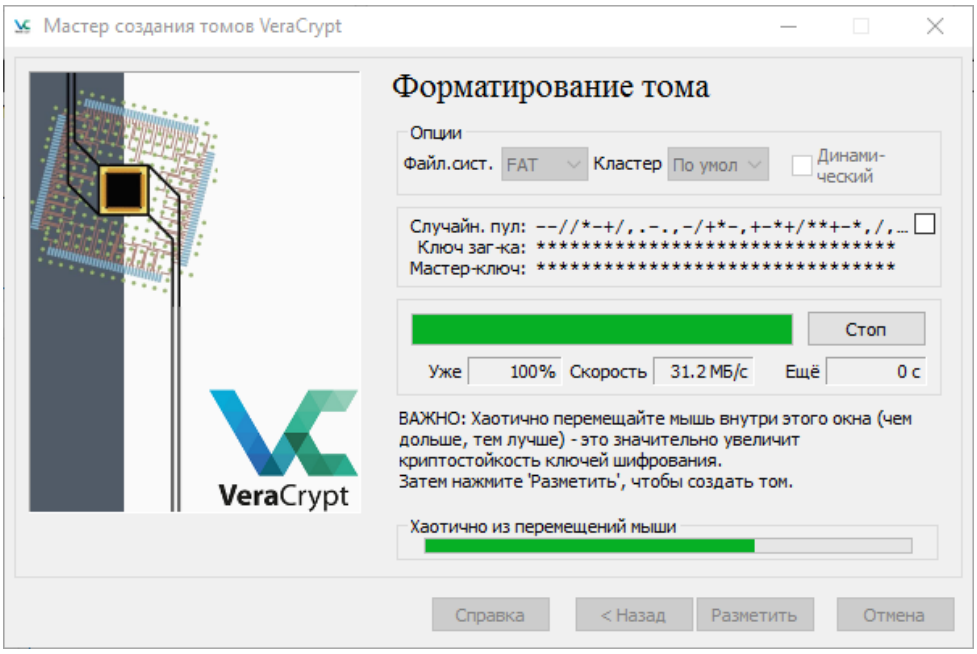
Шаг 13. Нажми кнопку **[Далее]**.



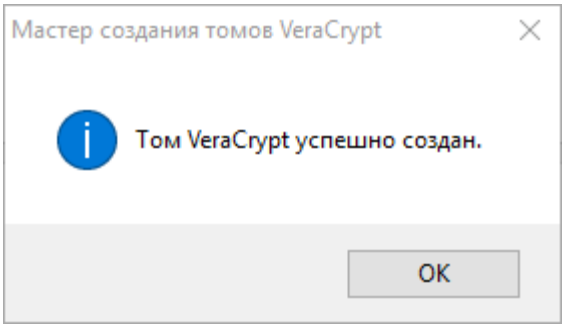
Примечание. По умолчанию предлагается система *FAT*. Она подойдет для большинства ситуаций и совместима с компьютерами Windows, Mac OS X и Linux. Но если ты намерен хранить файлы по 4 Гб и больше, тебе лучше выбрать другую *файловую систему*. *NTFS* будет работать на компьютерах Windows и *большинстве* компьютеров Linux.

Шаг 14. Нажми кнопку **[Разметить]**, чтобы начать создание обычного тома.

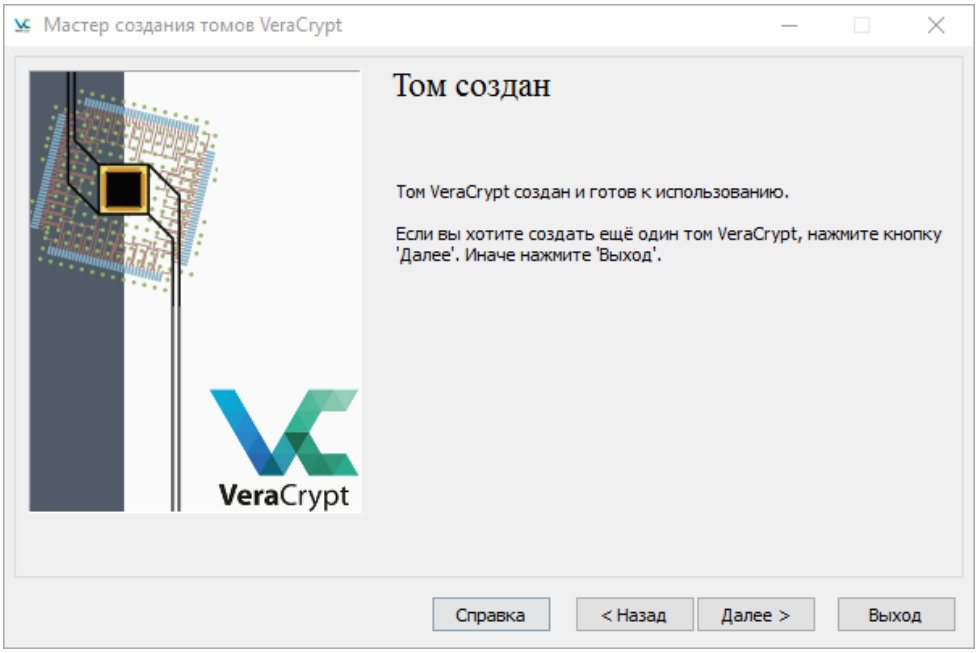
VeraCrypt готов к созданию *обычного зашифрованного тома внутри файла-контейнера*. Если ты станешь перемещать курсор мыши внутри окна форматирования тома, начнется генерирование случайных данных. Это поможет сделать шифрование более надежным.



VeraCrypt создаст файл с именем *My Volume* на *рабочем столе*. Это *обычный контейнер* **VeraCrypt** размером 250 Мб, в котором можно хранить важные файлы. **VeraCrypt** сообщит, когда процесс завершится.

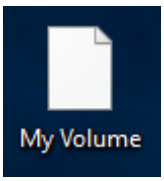


Шаг 15. Нажмите кнопку **[OK]**.



Шаг 16. Нажми кнопку **[Выход]**, чтобы закрыть *Мастер создания томов VeraCrypt* и вернуться в главное окно программы. (Если нажмешь **[Next]**, VeraCrypt начнет создавать еще один том).

Теперь можете видеть файл-*контейнер* 250 Мб в том месте, которое указали ранее.



Создание скрытого тома

В программе VeraCrypt скрытый том *помещается в зашифрованный* обычный том. *О наличии скрытого тома нельзя просто догадаться. Даже когда твой обычный том*

смонтирован*, невозможно определить, существует ли внутри скрытый том, если не знать пароль к нему. Пароли для обычного и скрытого томов разные*.

Скрытый том в некоторой степени похож на потайное отделение запертого чемодана. В самом чемодане ты хранишь файлы *для декорации*. Если они достанутся злоумышленнику (вместе с чемоданом), не случится большой беды. Самые важные файлы хранятся в потайном отделении. Смысл *скрытого тома* – сохранить в секрете само его существование (и, соответственно, все файлы, которые в нем находятся), даже если тебе придется выдать пароль к *обычному тому*. Тот, кто требует пароль к вашим файлам, получает его, видит файлы и остается удовлетворенным.

Чтобы этот прием работал – наши советы:

Запиши в *обычный том* несколько секретных документов, которыми ты готов рискнуть. Эта информация должна выглядеть достаточно важной, чтобы хранить ее в защищенном месте.

Периодически обновляй файлы в обычном томе. Создастся впечатление, словно ты действительно работаешь с ними.

Будьте готовы к тому, что злоумышленник в принципе может знать о скрытых томах. ***Главное:*** если ты правильно используешь VeraCrypt, этот человек будет не в состоянии *доказать* существование скрытого тома.

Как упоминалось выше, *скрытый том* технически находится внутри *обычного тома*. Вот почему VeraCrypt иногда называет их соответственно "внутренним" и "внешним". К счастью, нет нужды *монтировать* внешний том, чтобы добраться до внутреннего. VeraCrypt позволяет оперировать двумя разными паролями: один открывает внешний *обычный том*, другой – внутренний *скрытый том*.

Как создать скрытый том

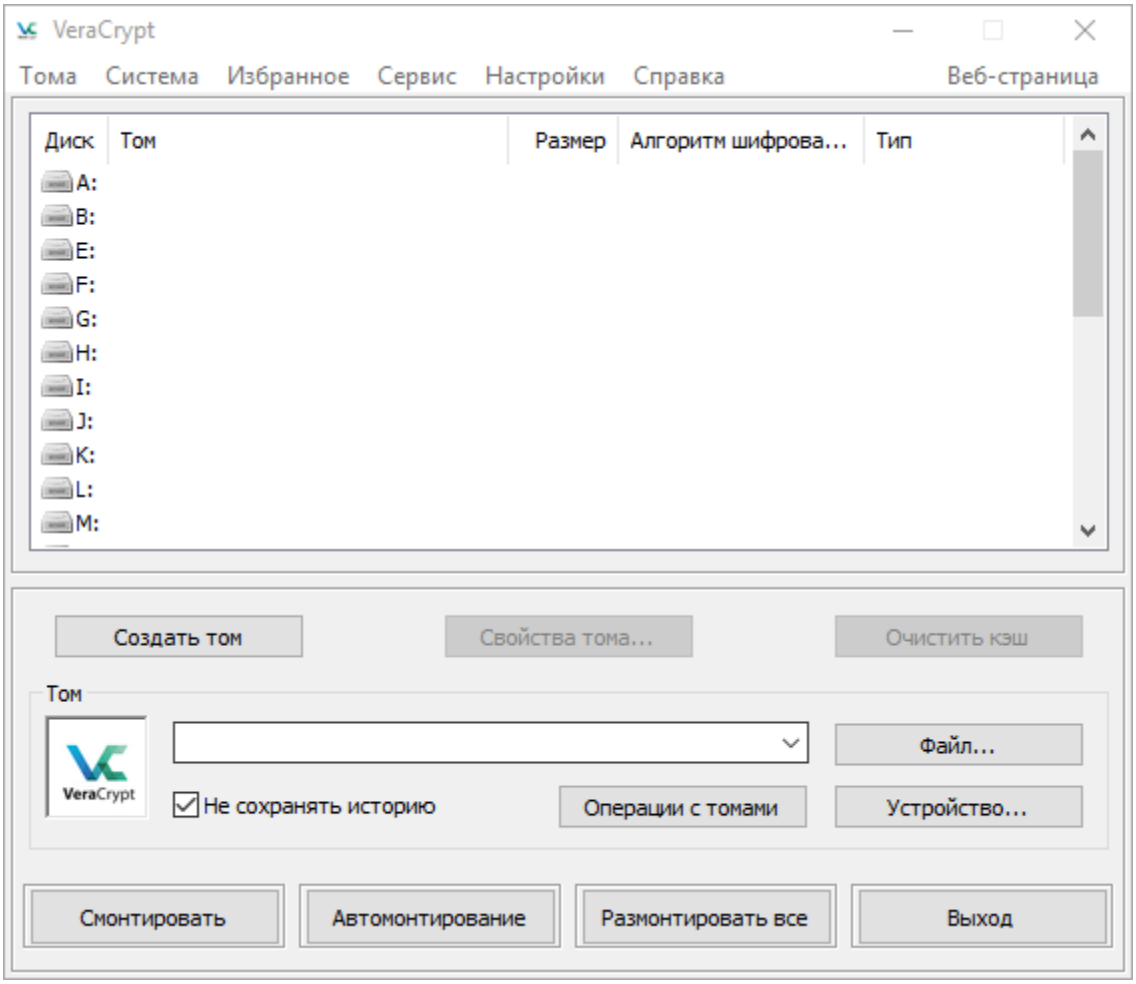
Есть два подхода к созданию *скрытого тома*. Оба они очень похожи на процесс создания *обычного тома*.

Обычный режим: сначала создаем *обычный том*, а потом внутри него *скрытый том*. (Как будто ты мастеришь чемодан с потайным отделением).

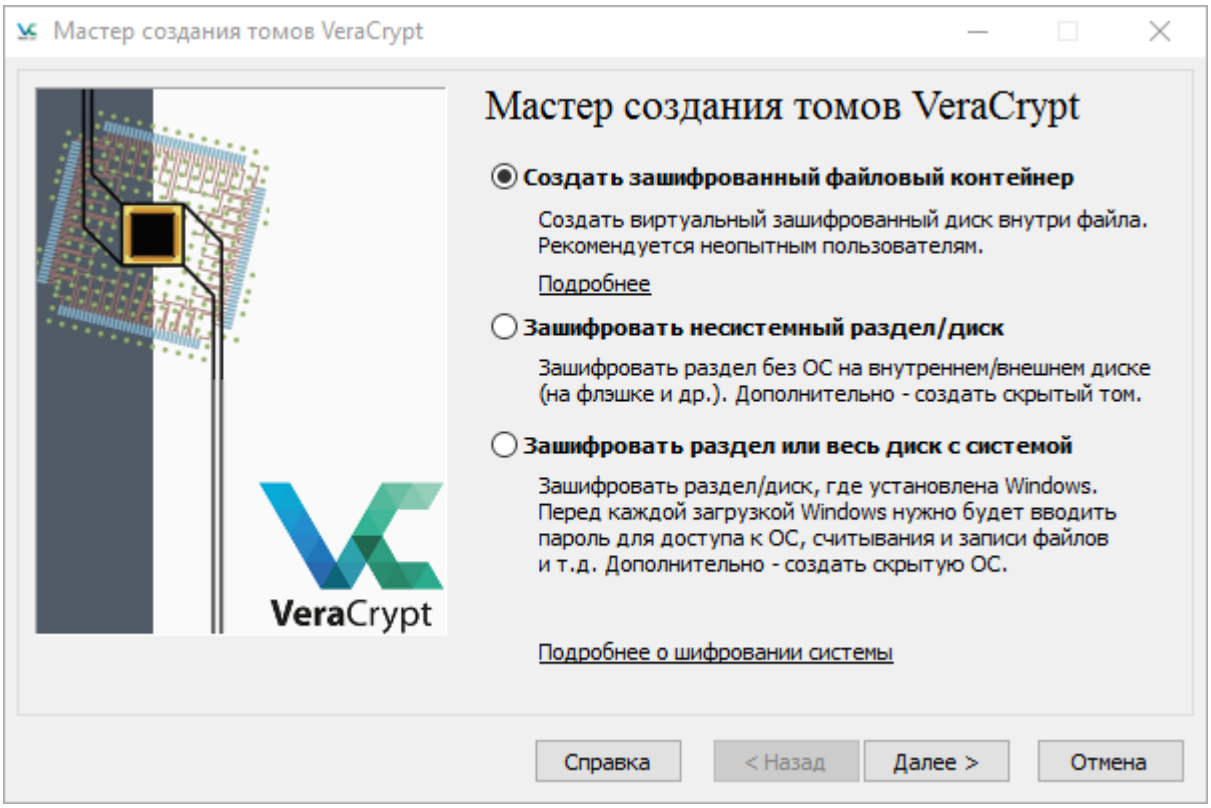
Прямой режим: у тебя уже есть *обычный том*, внутри которого ты создаешь *скрытый том*. (Чемодан имеется, нужно добавить потайное отделение).

В нашем случае мы ***используем*** **прямой режим**.

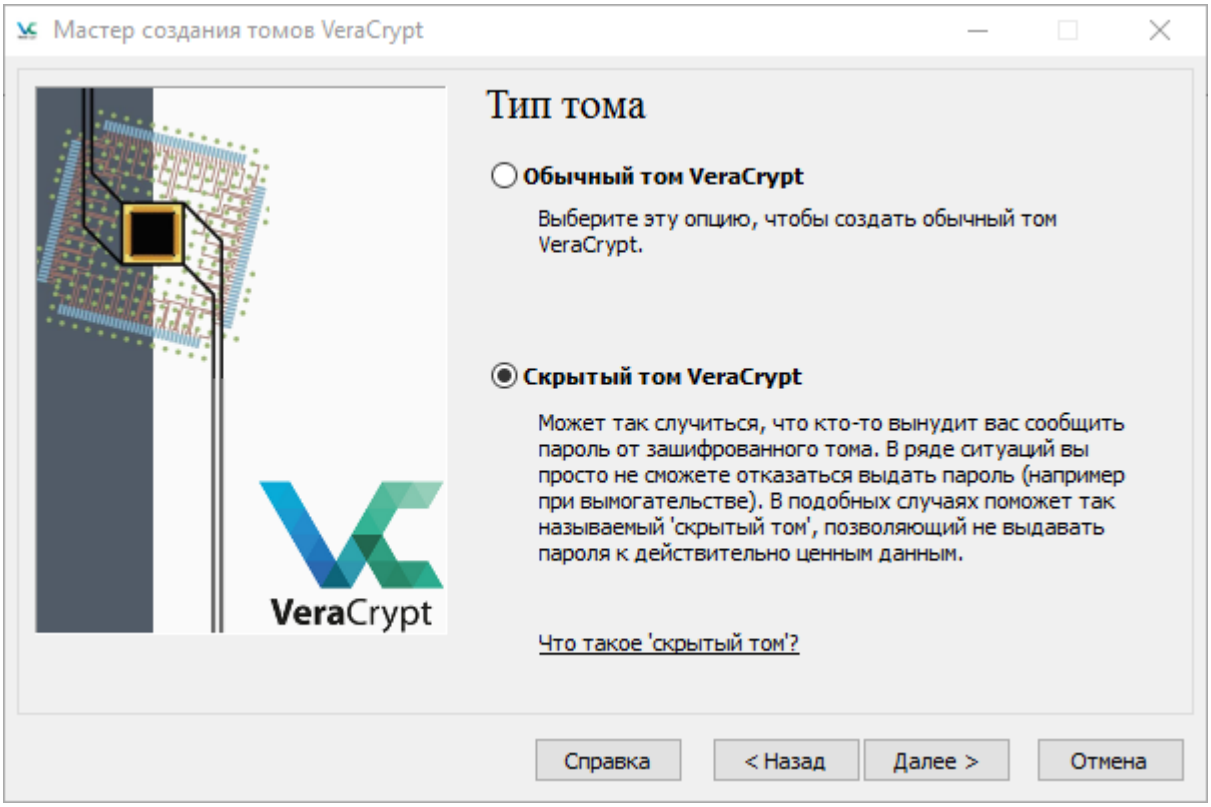
Шаг 1. Запусти VeraCrypt.



Нажми кнопку **[Создать том]**, чтобы запустить мастер создания томов.

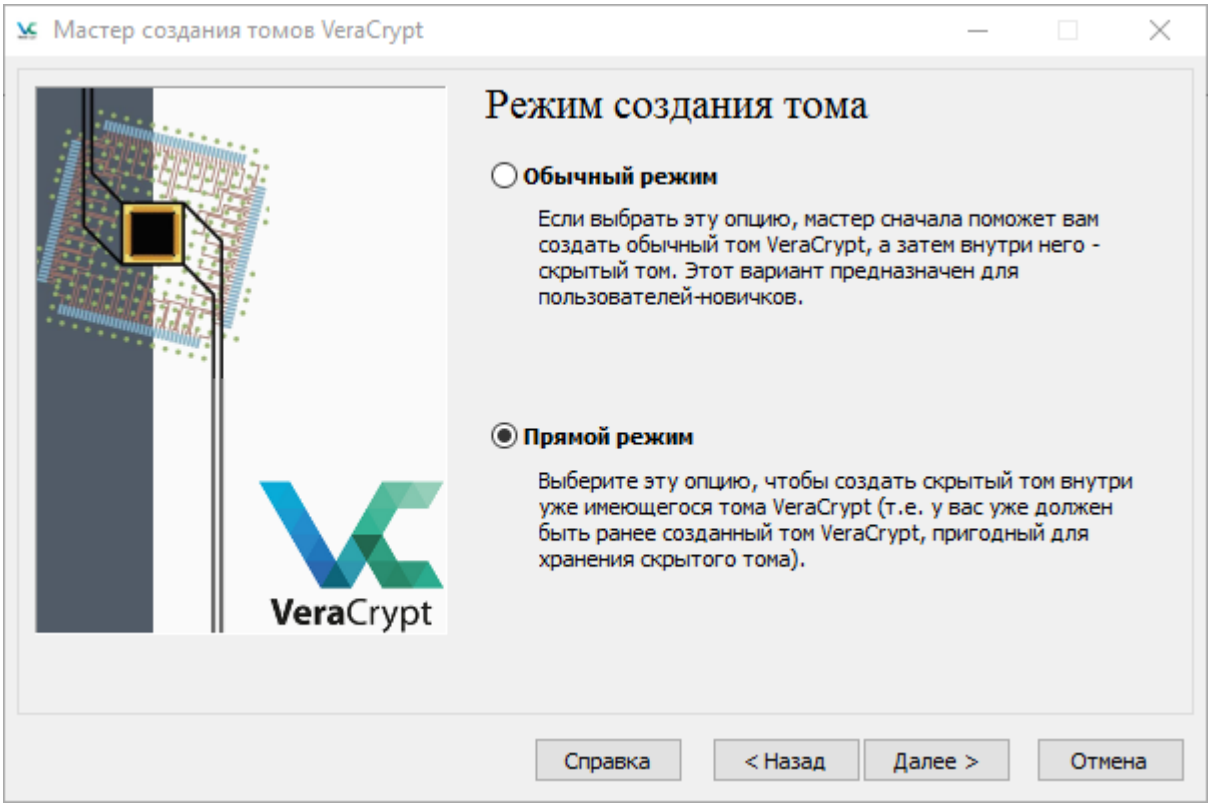


Шаг 2. Нажми кнопку **[Далее]**.



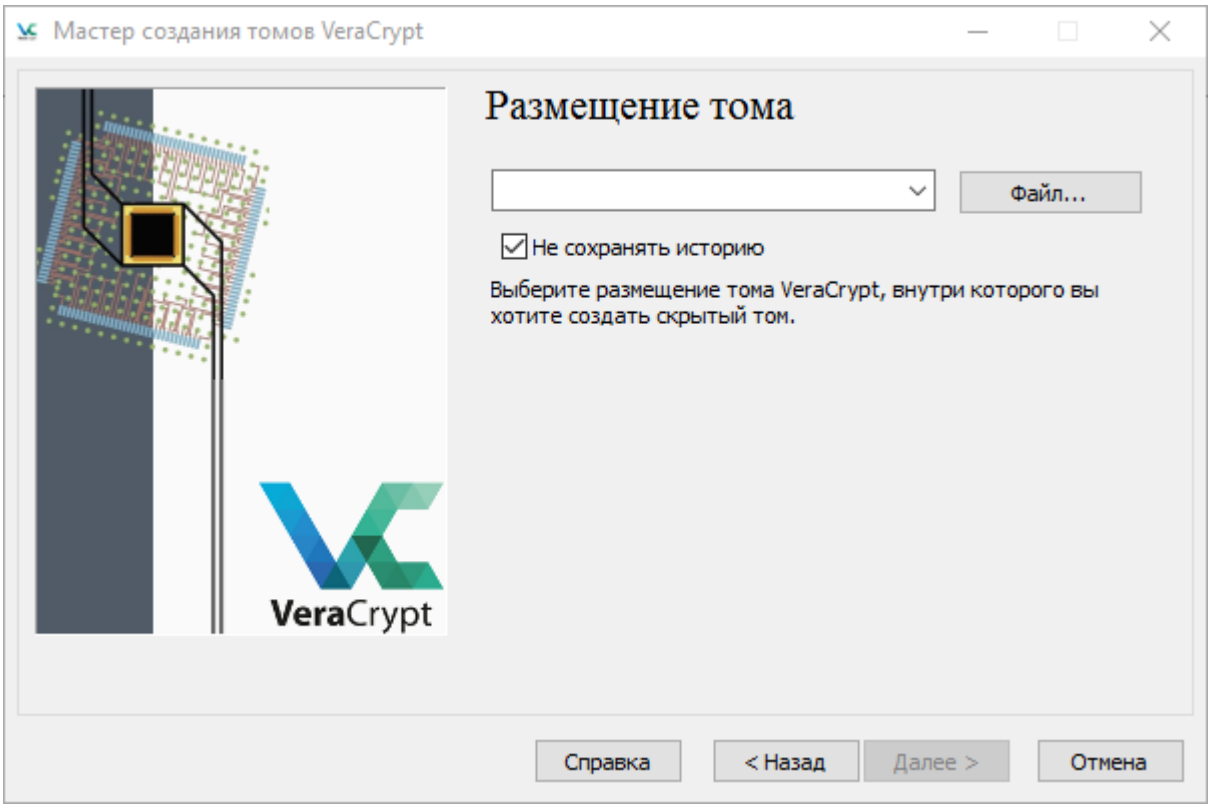
Шаг 4. Выбери вариант **[Скрытый том VeraCrypt]**.

Шаг 5. Нажми кнопку **[Далее]** для дальнейшего выбора режима (*обычный* или *прямой*).



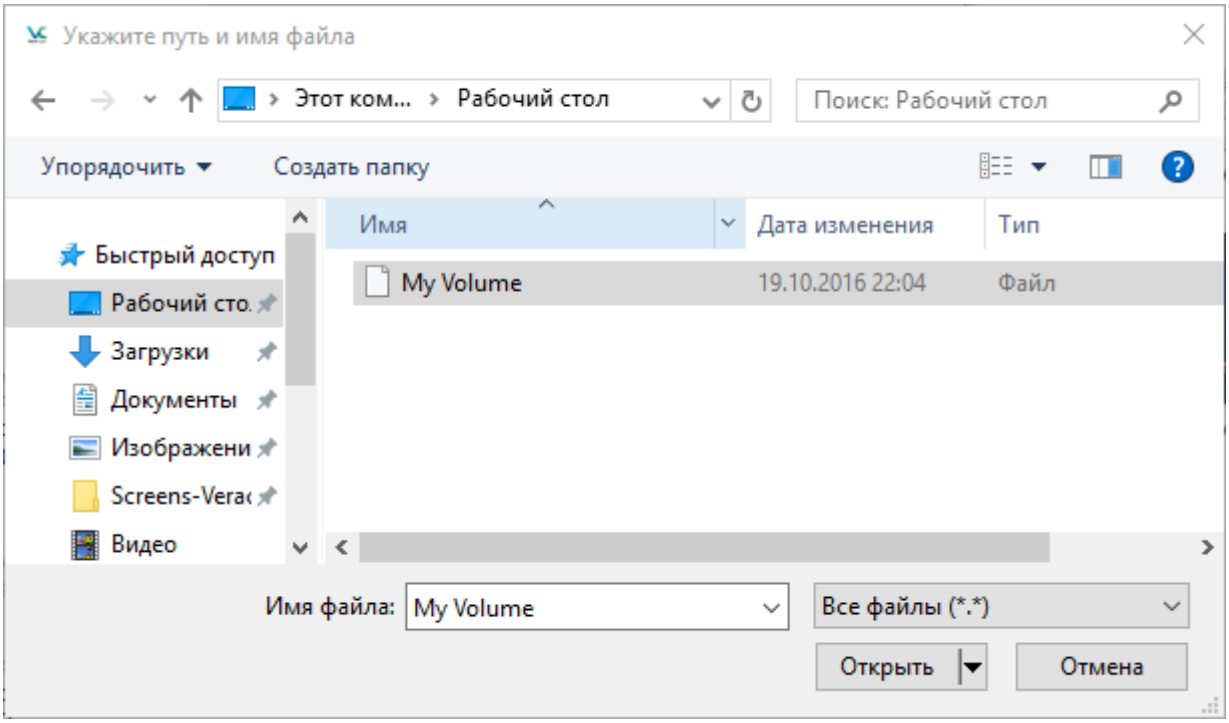
Шаг 6. Выбери вариант **[Прямой режим]**.

Шаг 7. Нажми кнопку **[Далее]**, чтобы выбрать нужный *файл-контейнер*.



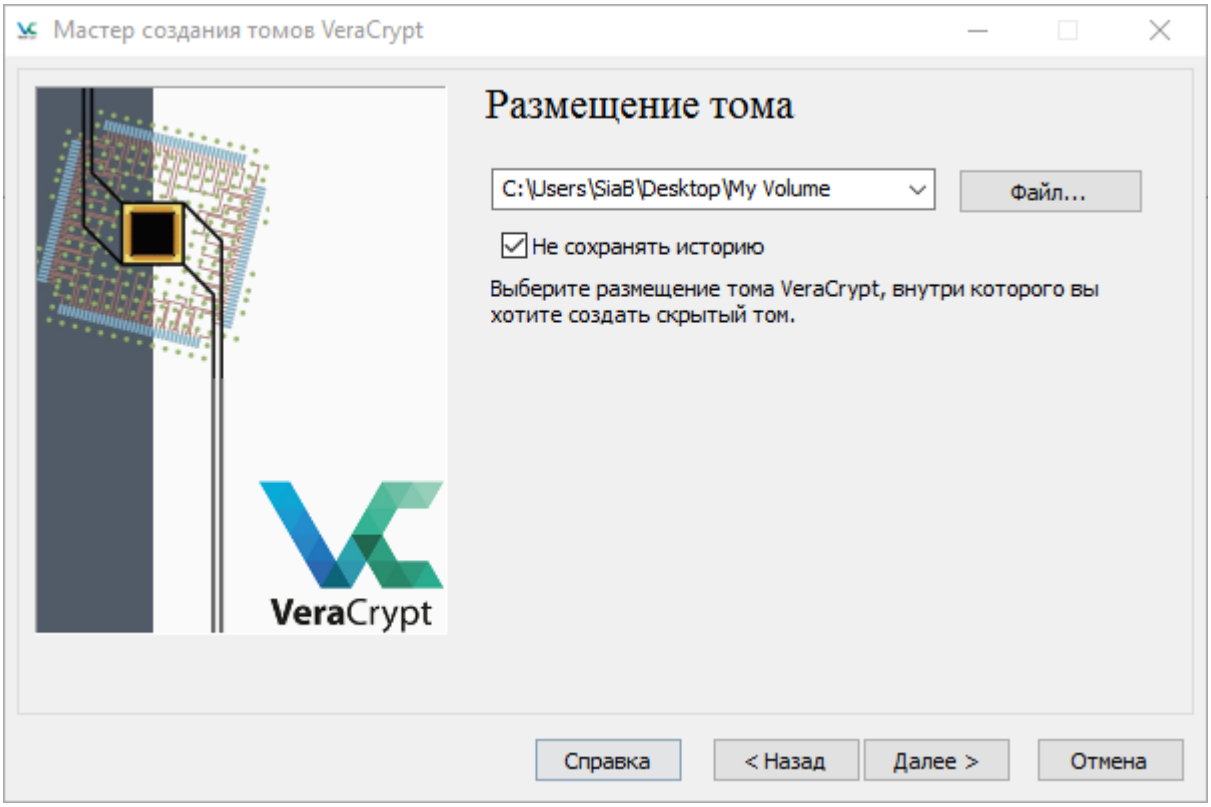
Примечание. Убедись, что твой *обычный том* размонтирован.

Шаг 8. Нажми кнопку **[Файл...]** и выбери *файл-контейнер*.

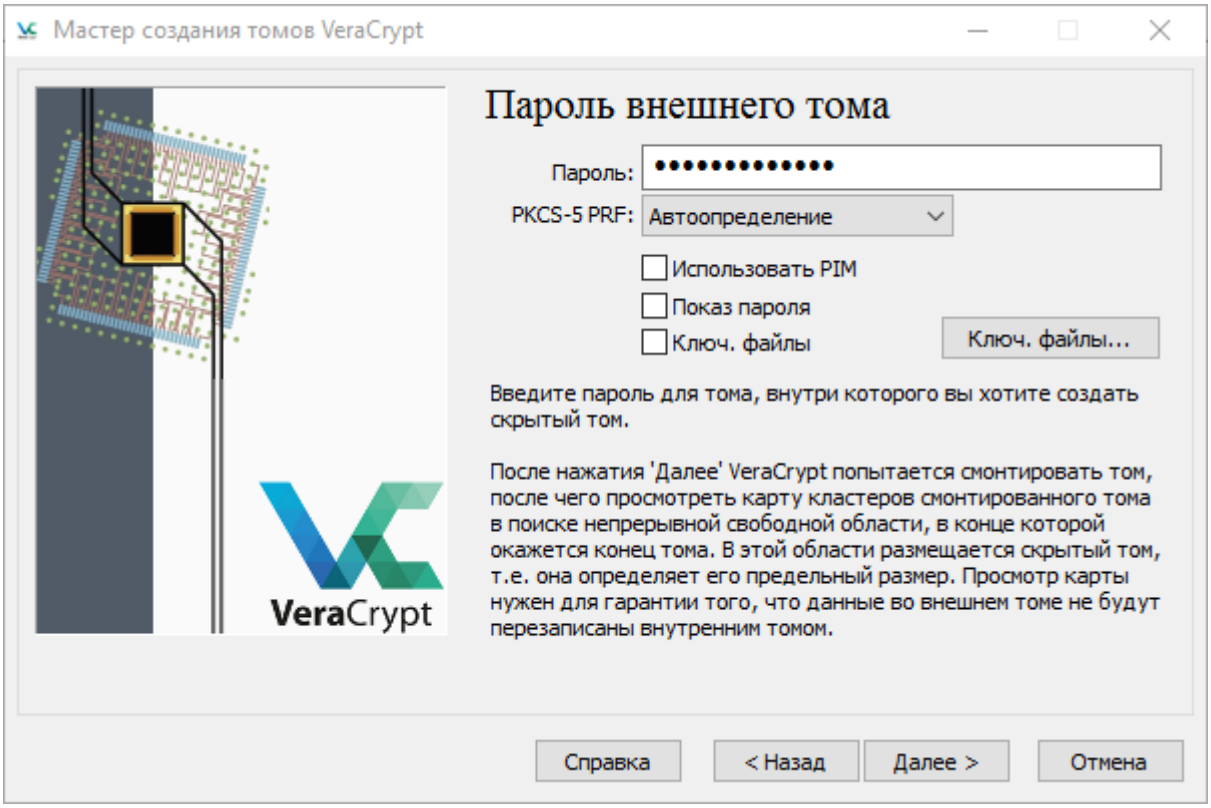


Шаг 9. Выберите файл-контейнер.

Шаг 10. Нажмите кнопку **[Открыть]**.

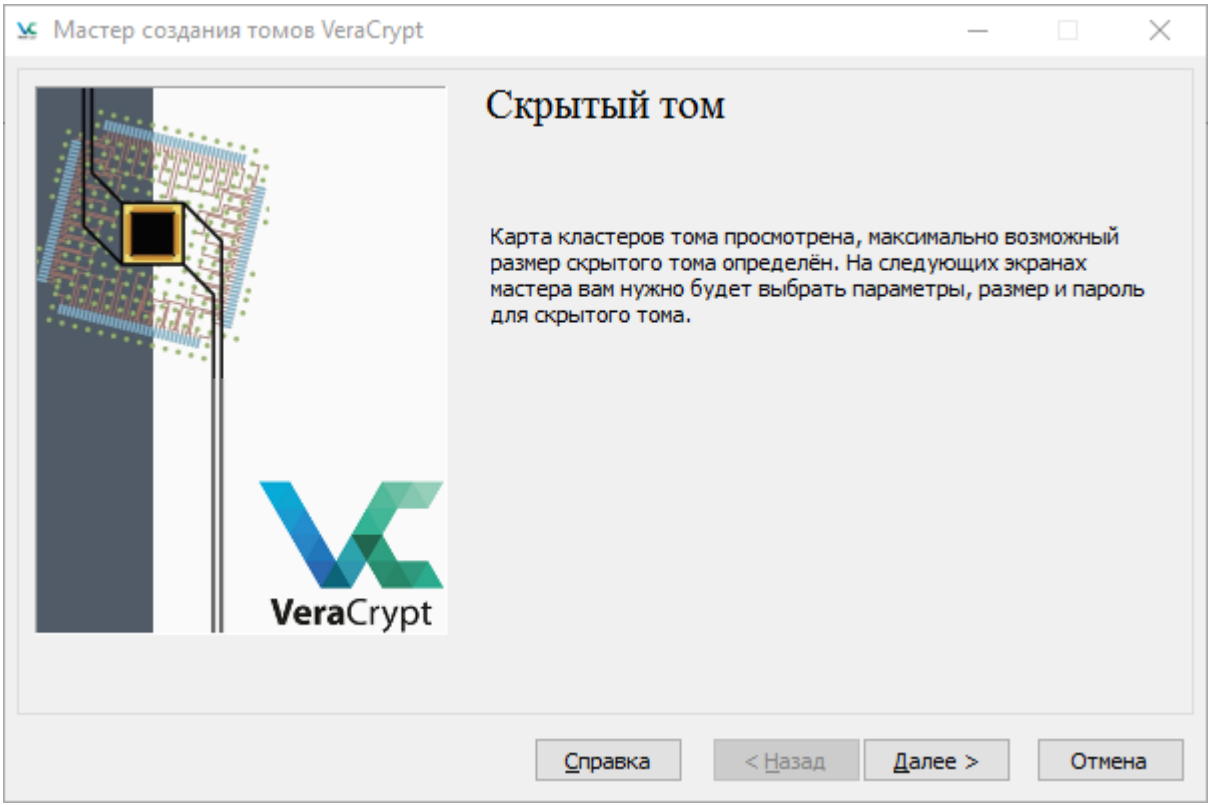


Шаг 11. Нажми кнопку **[Далее]**, чтобы ввести пароль к существующему обычному тому.

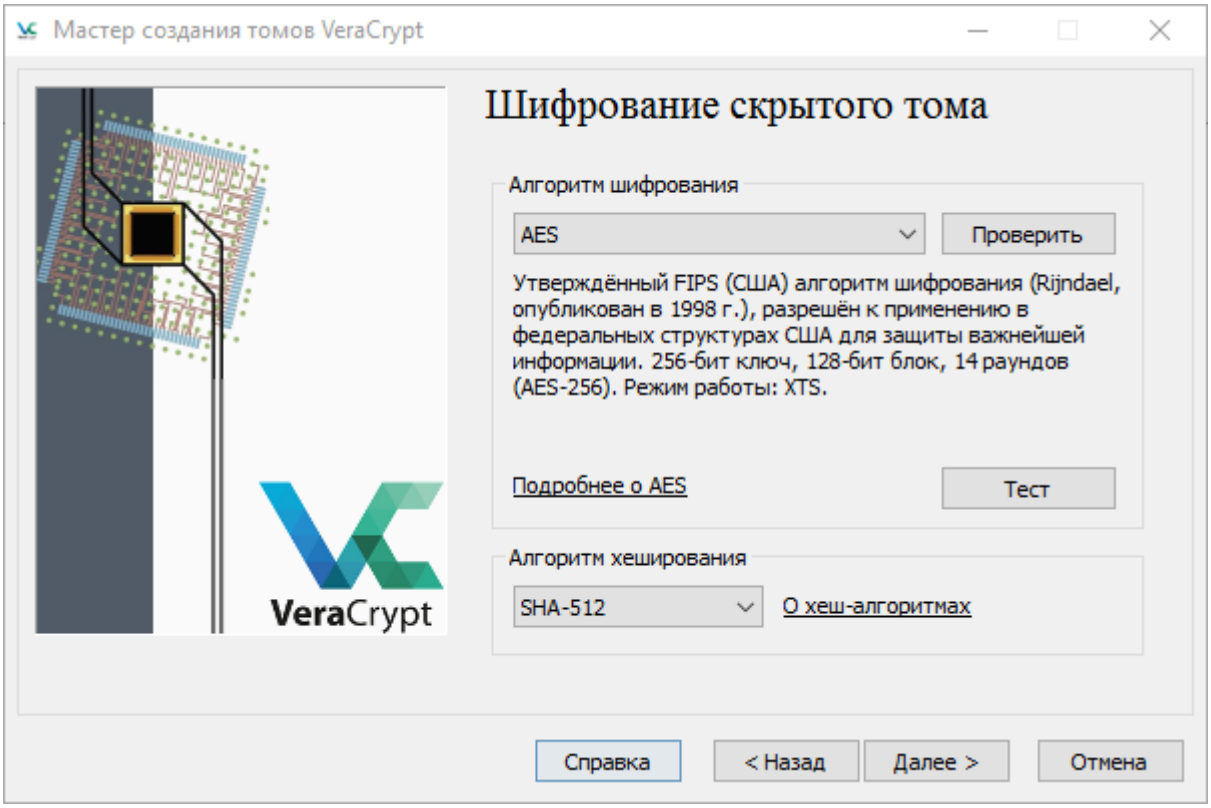


Шаг 12. Введи пароль, который ты использовал при создании *обычного тома*.

Шаг 13. Нажми кнопку **[Далее]** чтобы подготовить этот *обычный том* к дополнению в виде *скрытого тома*.

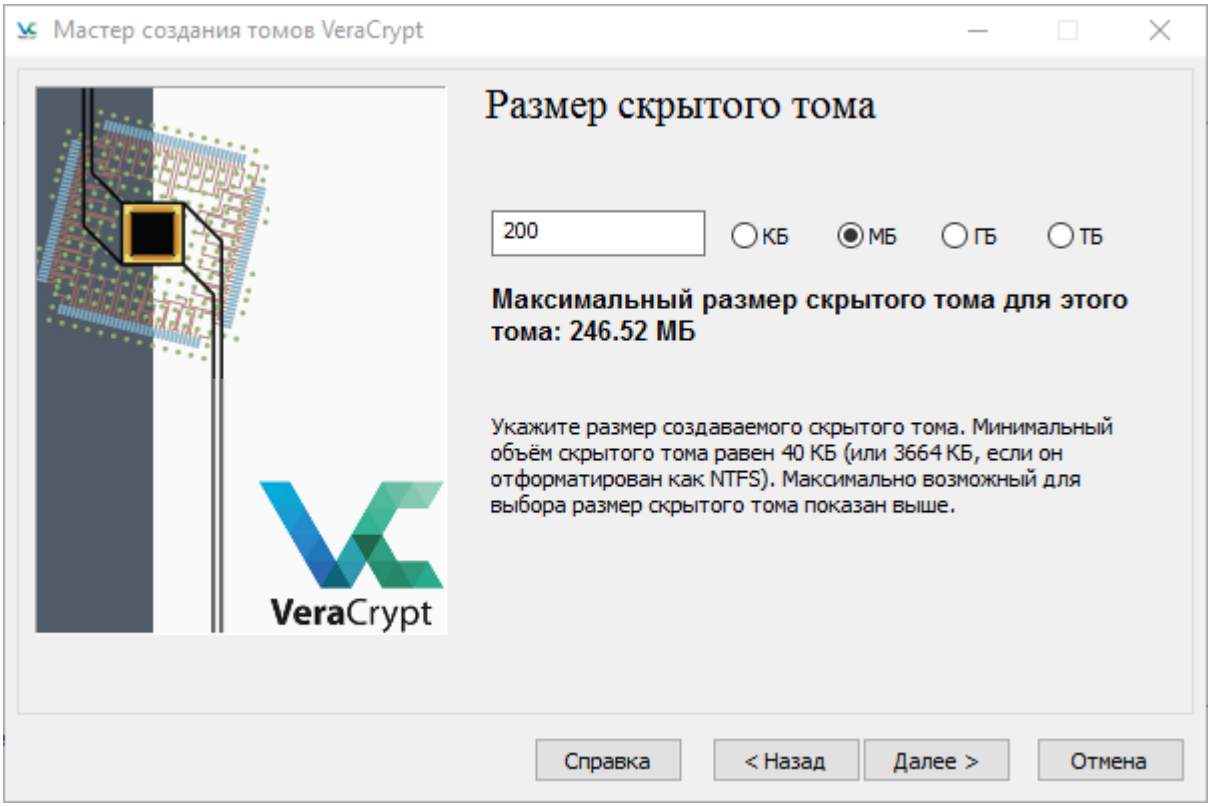


Шаг 14. Нажми кнопку **[Далее]** для настройки параметров шифрования скрытого тома.



Шаг 15. Нажми кнопку **[Далее]** для выбора размера скрытого тома.

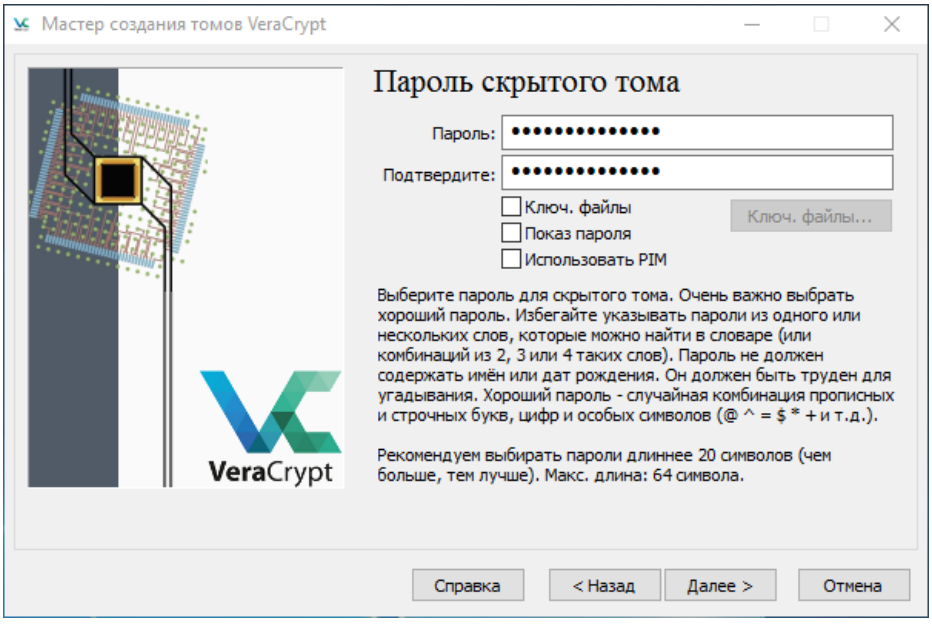
Примечание. Оставь параметры *Алгоритм шифрования* и *Алгоритм хеширования* для скрытого тома без изменений.



Как и при создании *обычного тома*, нужно помнить о количестве и типах файлов, которые ты планируешь хранить в *скрытом томе*. Изображения и видео, например, могут быстро привести к переполнению контейнера VeraCrypt, если тот чересчур мал. Кроме того, оставь немного места для *декоративных* файлов в *обычном контейнере*. Если ты выберешь для *скрытого тома* максимально допустимый размер, то не сможешь добавлять файлы в *обычный том*. (В нашем примере мы создадим *скрытый том* объемом 200 Мб внутри *обычного тома* объемом 250 Мб. Это даст нам примерно 50 Мб места для *декораций*).

Шаг 16. Введи размер тома, который собираешься создать. Убедись, что выбрал правильное значение в килобайтах, мегабайтах, гигабайтах или терабайтах.

Шаг 17. Нажми кнопку **[Далее]** для перехода к выбору пароля.

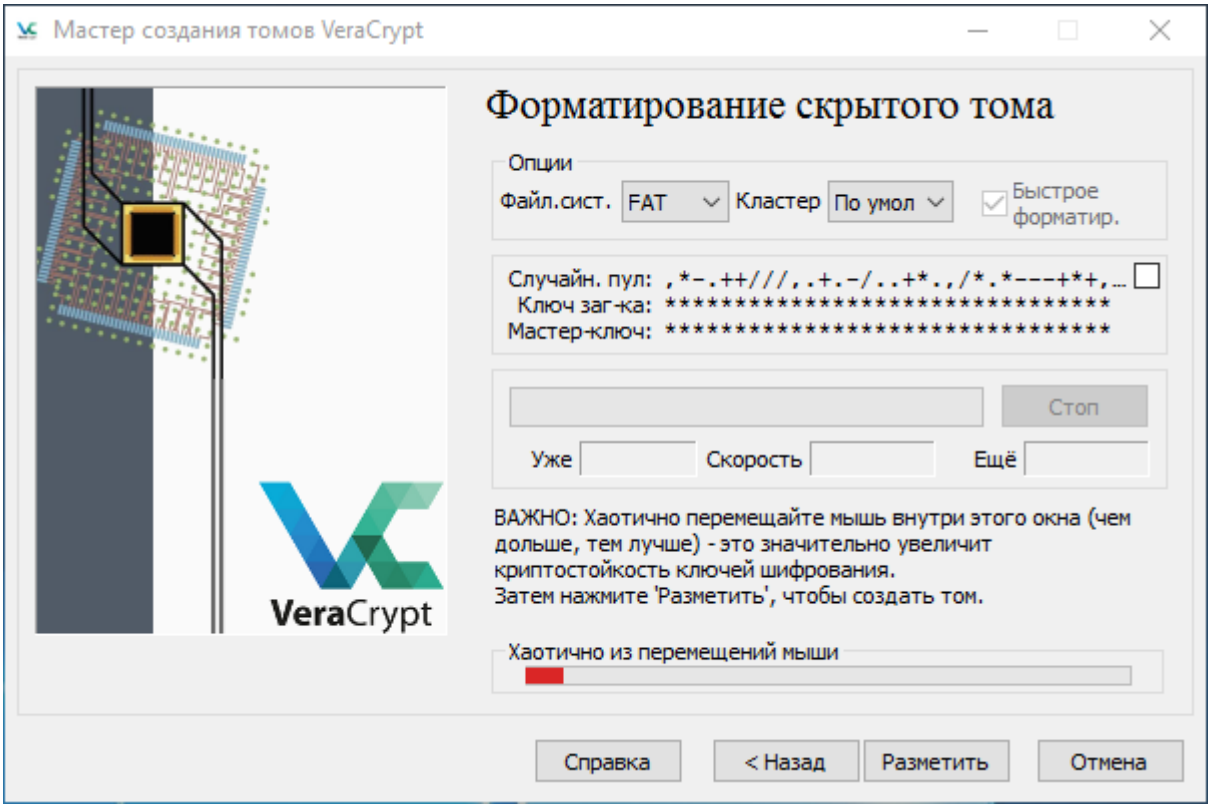


Теперь нужно выбрать пароль к *скрытому тому*, который должен *отличаться* от пароля к *обычному тому*. Напомним еще раз: используй сложные пароли!

Совет. Если ты используешь *менеджер паролей*, такой как **KeePassX**, и чувствуешь вероятность того, что на тебя могут оказать давление и получить доступ к обычному тому **VeraCrypt**, можешь хранить пароль для внешнего (декоративного) *обычного тома* в **KeePassX**, а вот пароль к *скрытому тому* придется запомнить.

Шаг 18. Выбери пароль и **введи** его дважды.

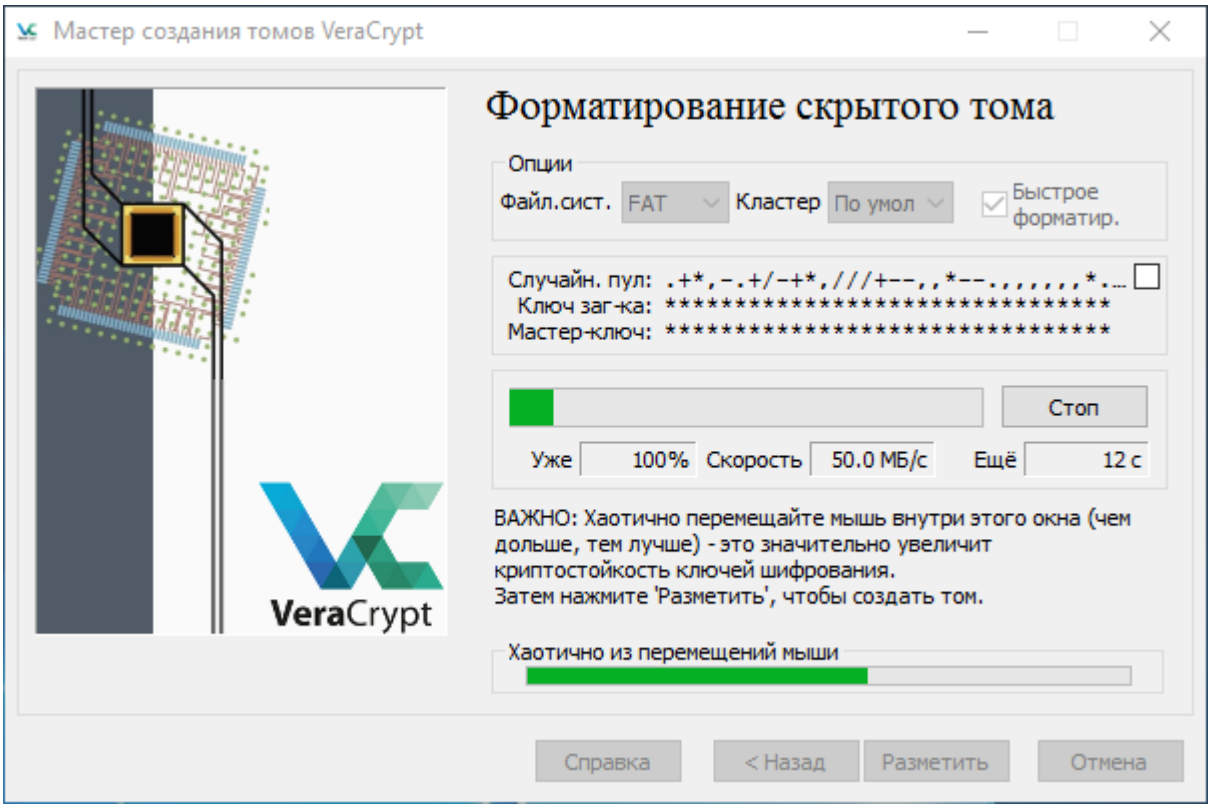
Шаг 19. Нажми кнопку **[Далее]**.



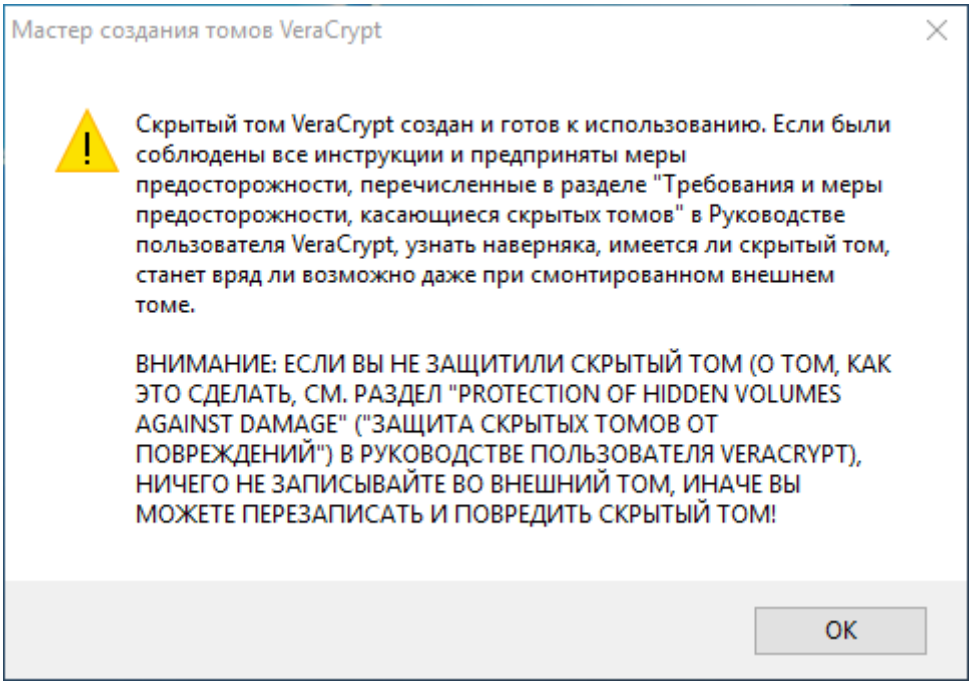
Примечание. По умолчанию предлагается система *FAT*. Она подойдет для большинства ситуаций и совместима с компьютерами Windows, Mac OS X и Linux. Но если вы намерены хранить файлы по 4 Гб и больше, тебе лучше выбрать другую *файловую систему*. *NTFS* будет работать на компьютерах Windows и *большинстве* компьютеров Linux.

Программа **VeraCrypt** готова к созданию *скрытого тома*. Если ты наведешь курсор мыши на окно *Форматирование скрытого тома*, начнется генерирование случайных данных, которые помогают сделать шифрование более надежным.

Шаг 20. Нажми кнопку **[Разметить]**, чтобы начать создание скрытого тома.



Когда процесс завершится, ты увидишь предупреждение о важности защиты *скрытого тома* при добавлении файлов в *обычный том*.



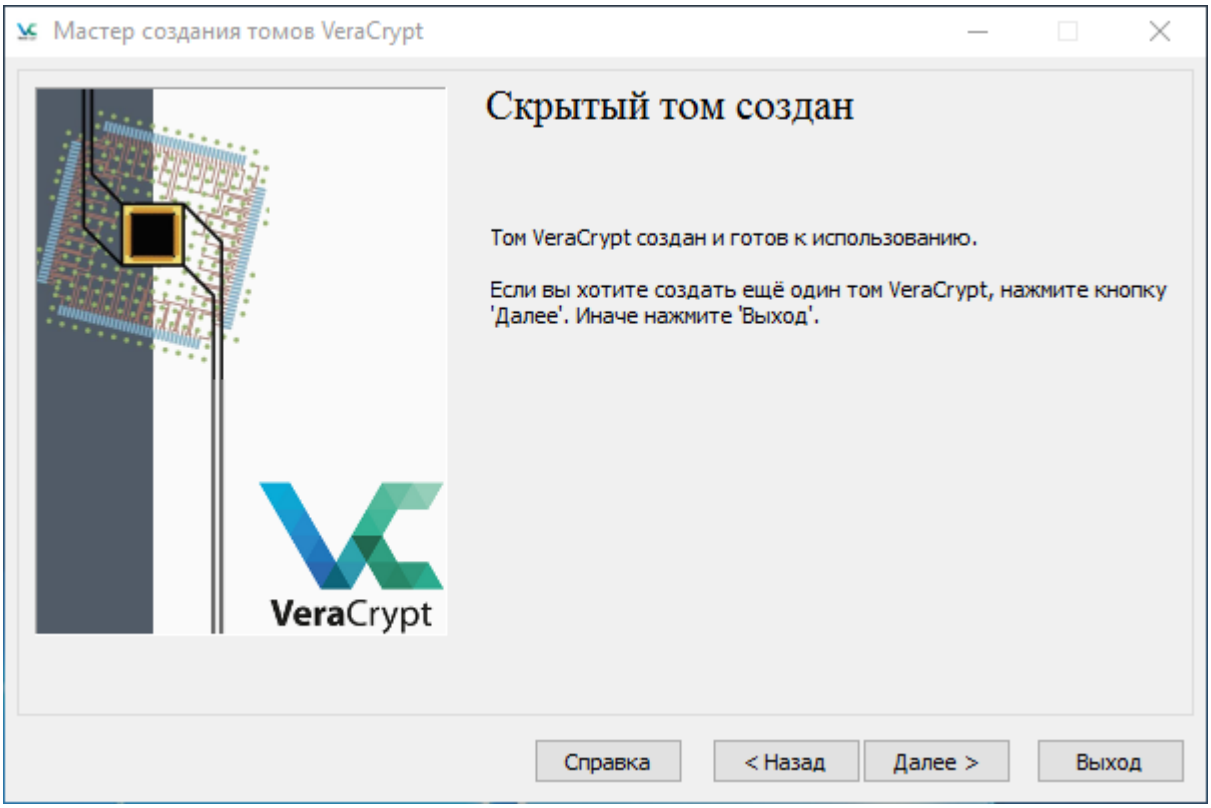
Важно. Это предупреждение связано с тем, как VeraCrypt маскирует наличие *скрытого тома*. При обычных обстоятельствах, когда ты открываешь *обычный том* (внешний), и VeraCrypt, и Windows *считают*, что этот том занимает весь объем *контейнера* (в нашем примере около 250 Мб). На самом деле, мы создали *скрытый том* размером 200 Мб и оставили только 50 Мб пространства для "декоративных" файлов в *обычном томе*.) Если ты попытаешься записать в *обычный том* файлы

общим размером, допустим, 60 Мб, VeraCrypt не сообщит об ошибке. Если бы такое сообщение появлялось, злоумышленник мог бы узнать о существовании *скрытого тома*. Таким образом, 60 Мб будут записаны, *а файлы внутри скрытого тома будут повреждены или удалены*.

Другими словами, программа воплощает идею о том, что вы лучше *потеряете* свои данные в *скрытом томе*, чем о них узнает злоумышленник.

Всякий раз, когда добавляешь "декоративные" файлы во *внешний том*, не забывай *включать защиту скрытого тома* (конечно, придется вводить пароли как для *скрытого тома*, так и для *обычного тома*). Если ты будешь пользоваться этой опцией, VeraCrypt *станет* предупреждать тебя о ситуациях, когда копирование файлов в *обычный* том начнет представлять угрозу содержимому *скрытого тома*. (Обратите внимание: если кто-нибудь наблюдает за тем, как ты вводишь оба пароля, это также будет свидетельствовать о наличии *скрытого тома*, так что вводи пароли только в одиночестве или в присутствии людей, которым полностью доверяешь).

Шаг 21. Нажав кнопку **[OK]** ты увидишь сообщение, что скрытый том создан.



Шаг 22. Нажми кнопку **[OK]**, чтобы вернуться в главное меню программы.

Теперь можно хранить файлы в *скрытом томе*. О его существовании не узнает даже тот, кто получит пароль к *обычному тому*.

Анонимность в реальной жизни

Начнем с самого очевидного. С того, что на поверхности.

Близкие. Какого бы возраста ты бы не был, всегда есть близкие, родные, друзья, люди, которые следят за вашей жизнью. Для начала - элементарно ничего не говорить о своих темных делах, да и вообще о своем присутствии в интернете. Если твое ближайшее окружение будет думать, что ты просто задрот в комп и подписчик известных блоггеров, вероятность неудобных вопросов будет меньше. Даже самым близким друзьям не стоит говорить о теневой сфере.

Повседневная жизнь. Первое - не подавать признаков хакера или мошенника. Не умничать в таких вопросах, совсем не умничать. Лучше, чтобы у тебя было хобби и что бы соседи, коллеги и друзья его знали, видели, понимали, разделяли с тобой. Каково же будет удивление знакомых, если 10 лет в подряд ты по утрам бегаешь, а тут раз, и перестал. Это начнет вызывать много вопросов, все начнут интересоваться тобой, такими радикальными переменами в твоей жизни (для того, чтобы тобой не интересовались, ты не должен выделяться в компании коллег, знакомых и друзей. Также не стоит включать максимального зануду, подозрения тоже будут). Не стоит совершать незапланированные покупки техники и прочего дорогого (откуда же у тебя такие деньги, если ты весь день на совершенно обычной работе, а ночью за компом? Кхм...странно).

Интернет (и техника в целом). Проси помощи, притворяйся, что не можешь элементарно переустановить винду и сдавай пк в ремонт (с преждевременно извлеченным доп. жестким диском [тот самый, который мы зашифровали VeraCrypt]) например из-за поломки разъема, пыли и всего прочего. Когда ты занимаешься чем-то противозаконным, лучше включать Steam и какую-то игру (если у тебя много знакомых, с которыми ты лично встречаешься и играете в игры), в Стим показывает сколько и когда часов ты проводишь в игре, это охарактеризует тебя, как задрота, что нам на руку. Никогда не упоминай имя, фамилию, город, телефон, реальные данные карт и всего прочего. Также не стоит заигрываться. Пример: у тебя есть поставщик картона. Ты часто заказываешь у него картон, каждый раз примерно на одинаковую сумму. Настал день, когда ты просишь у него партию х10, т.е. заказываешь намного больше, чем раньше. Конечно, вы же уже старые друзья, продавец надежный, почему бы не внести предоплату в размере 100% суммы и ОП! Он не отвечает уже вторую неделю. Бинго. Никогда не зазнавайся и все-все-все проверяй по 7 раз.

Плати наличными. Совершая покупки связанные со своей личностью, плати наличными. Когда оплата наличными не возможна, рассмотри оплату с предоплаченной карты, которую купил за наличные деньги. Тебе не нужны банковские отчеты или выписки по кредитной карте, устанавливающие связь между тобой и местами в которых ты “никогда не был”, или сайтами, которые ты “никогда не использовал”.

Быть распознанным - провал. Не проводи тайные встречи в местах, которые ты часто посещаешь в своей нормальной жизни. Требуется всего один сотрудник, любовник, друг и т.д. чтобы раскрыть тебя, назвав тебя неправильным именем, и полностью уничтожив твое прикрытие.
Выбери место где ты с наименьшей долей вероятности будешь распознан, оденься по-другому, и не посещай место для тайных встреч в повседневной жизни. Выходя из дома, отключай мобильный телефон. твоя тайная встреча перестанет быть тайной, если у тебя и твоего собеседника включены мобильные телефоны в момент встречи. Это является прямым доказательством того, что вы были рядом какое-то время.

Поддерживай самообладание.
Если ты хочешь, что бы тебе сошло с рук то, что ты хранишь в тайне - ты должен сохранять спокойствие. Помни это, когда нервничаешь или переживаешь. Не хихикай каждый раз, когда кто-то говорит слово “тайна”. Знай о своих выражениях лица и своих реакциях на людей вокруг тебя. Будь внимателен на какие имена ты отзываешься. Оставайся спокоен (Это все мы подробно разберем в разделе «Социальная инженерия»)

Не становись дерзким.
Обслуживание тайной личности требует постоянной бдительности. Личную безопасность никогда нельзя гарантировать, и не нужно забывать об этом. Дерзость порождает небрежность , небрежность приводит к обнаружению.

Совершенство требует практики.
Ни один из этих навыков не является врожденным. Все они нуждаются в обширной практике. Ты обнаружишь, что часто будет приходиться начинать сначала и постоянно подправлять ошибки снова и снова. Нет ничего постыдного в провалах, но важно помнить, что интернет никогда ничего не забывает; Лучше всегда ошибаться будучи осторожным и добавлять дополнительную информацию, и понимать как ты движешься, после правильной оценки рисков.

Следует понимать что это ни в коем случае не исчерпывающий список всех возможных мер предосторожности которые можно предпринять. А так же эти меры предосторожности не могут быть полезны против противников с большим количеством времени и ресурсов. Это абсолютно простой способ свести к минимуму риск от сталкеров, опасных членов семьи, любопытных работодателей, а так же потенциально от государственных чиновников и законников низкого уровня.

Социальные сети могут являться большой угрозой для многих из нас, но при тщательном управлении своей личностью, можно свести на нет некоторые из этих опасностей, сохраняя при этом надежное присутствие в Интернете.