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 №17

Инструкционно-технологическая карта

Тема:Защита программ от несанкционированной эксплуатации и сокрытие данных на винчестере.

Цель: научиться защищать программы от несанкционированной эксплуатации, научиться скрывать данные на винчестере.

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

Одним из основных методов защиты программ от несанкционированного доступа является использование механизмов проверки подлинности и авторизации. Для этого в программном коде могут быть реализованы механизмы, которые проверяют подлинность пользователя и его прав на выполнение определенных действий. Например, программное обеспечение может требовать от пользователя ввода пароля или использование биометрических данных для подтверждения своей личности.

Но сегодня мы поговорим о еще одном способе защиты данных.

Сокрытие данных на винчестере

Зачем нужны скрытые диски?

Допустим, вы работали на своем компьютере, но были отвлечены и оставили его без присмотра. Это делает вашу систему уязвимой, и любой, кто проходит мимо, может получить доступ к вашим личным документам.

Шифрование диска в этом случае поможет создать защиту данных, которые хранятся в системе, но нужно будет правильно настроить ее. Также такой способ охраны собственной информации поможет, если компьютером пользуется сразу несколько человек.

Но опаснее всего в этой ситуации выглядит вредоносное ПО. Именно из-за него зачастую происходит утечка данных. Скачав или просмотрев нежелательный файл, вы можете «слить» все свои личные данные мошенникам. И не страшно, если это будут фото с пикника, хуже, если киберпреступники узнают ваши логины или данные банковских платежей. Поэтому, если подобная информация хранится у вас на компьютере, лучше защитить ее шифрованием диска. Для этого существует несколько доступных способов.

Защита программ от несанкционированной эксплуатации и сокрытие данных на винчестере - это важная тема в области информационной безопасности, которая направлена на защиту программного обеспечения и данных от несанкционированного доступа и использования.

Хранить важную, конфиденциальную информацию в зашифрованном контейнере очень удобно: данное хранилище можно скопировать и перенести на другой компьютер. Но есть один минус – контейнер это файл, который все могут видеть и который можно с лёгкостью удалить.

Скрытые разделы жесткого диска дают возможность хранить вашу важную информацию в безопасности. В таком случае другие пользователи вашего компьютера не смогут их удалить. Вы можете хранить на скрытых дисках всевозможные файлы, которые можно ззашифровать.

Хранение важных файлов на скрытых разделов жёсткого диска + шифрование этих дисков – хороший метод защиты вашей конфиденциальной информации на вашем компьютере. Если вам часто нужно носить данные в зашифрованном виде — используйте зашифрованные контейнеры.

Что такое шифрование?

Это процесс преобразования данных, которые хранятся в хранилище. При этом все файлы становятся нечитаемыми для очень любопытных юзеров. Для шифрования могут быть использованы специальные утилиты или аппаратное обеспечение.

Благодаря приложениям можно зашифровать каждый бит на диске. При этом расшифровать его сможет только профессионал, который в принципе этим занимается. Неопытные пользователи и те же вредоносные программы не смогут преодолеть шифрование жесткого диска.

Методы и типы шифрования дисков

Существует множество методов сокрытия данных на винчестере, но самыми распространенными являются следующие:

Сокрытие дисков - метод, который позволяет скрыть существование дисков на компьютере. Это может быть полезно, если у вас есть конфиденциальная информация, которую вы хотите скрыть от посторонних глаз.

Шифрование дисков - метод, который позволяет защитить весь диск или отдельные разделы на нём, используя алгоритмы шифрования. Этот метод защищает данные от несанкционированного доступа и предотвращает их утечку.

Также есть 2 типа шифрования дисков:

Полное шифрование – предполагает шифрование всего содержимого диска, включая системные файлы, программы и пользовательские данные

Шифрование разделов – предназначено для защиты только определенных разделов жесткого диска.

Шифрование дисков может быть выполнено с использованием различных алгоритмов шифрования, таких как AES, Blowfish, Twofish, Serpent и др.

Однако следует отметить, что сокрытие данных и дисков не является полной гарантией конфиденциальности данных. Если злоумышленник получит доступ к вашему компьютеру, то он может использовать различные методы для получения доступа к скрытым данным и дискам. Поэтому при использовании этих методов необходимо соблюдать все меры предосторожности и дополнительно защищать свои данные.

Естественно, количество методов защиты документов на винчестере довольно большое. Некоторые из них сможет реализовать только опытный пользователь или специалист. Хотя некоторые доступны и остальным юзерам.

Прозрачное шифрование

Прозрачное шифрование – это вариант охраны личных документов на винчестере с помощью любой из существующих специальных утилит. В этом случае шифрование автоматизировано, поэтому данные либо доступны, либо недоступны для взаимодействия.

Этот способ может кодировать разделы или работать на уровне файлов. Например, в первом случае можно «спрятать» весь диск, а во втором – выбранную файловую систему.

На уровне файловой системы

Это еще один способ шифрования диска. Его можно считать подразделом предыдущего варианта. Он помогает «прятать» каждый файл, а получение доступа осуществляется с помощью аутентификации. Этот вариант кратко можно называть FLE.

Некоторые ОС имеют встроенный инструмент для работы с этим шифрованием. В случае нехватки должны аппаратных утилит, можно использовать сторонние проекты. В этом случае каждый, кто может изучать файловую систему, также может узнать метаданные и имена зашифрованных документов.

Кодирование файловой системы отличается от защиты всего диска тем, что во втором случае нужно пройти простую загрузку и в этом случае можно получить данные с архива. Первый же случай предполагает аутентификацию и получению к каждому файлу, который зашифрован.

**О программе**

Cryptainer Lite — это бесплатная программа для шифрования файлов и папок на компьютере. Она позволяет создавать зашифрованные виртуальные диски, на которые можно сохранять конфиденциальные данные и файлы. Кроме того, программа обеспечивает защиту от несанкционированного доступа к виртуальным дискам путем автоматического отключения диска при неактивности.

После установки Cryptainer Lite, вы можете создать виртуальный диск и назначить ему имя и размер. Затем вы можете выбрать пароль для доступа к этому диску. После создания виртуального диска пользователь может копировать в него файлы и папки так же, как если бы это была обычная папка на компьютере. Но при этом данные будут автоматически зашифрованы при сохранении на виртуальный диск.

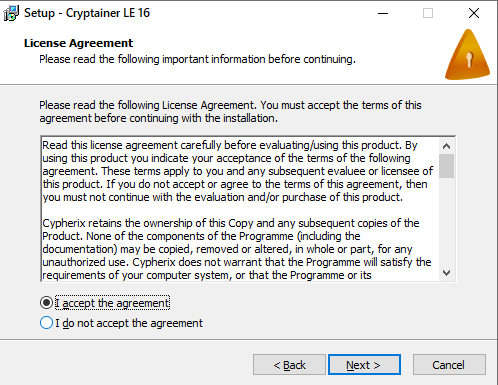
Установка Cryptainer Lite

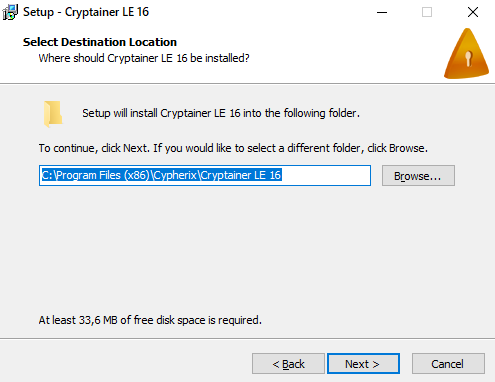
Переходим на сайт:

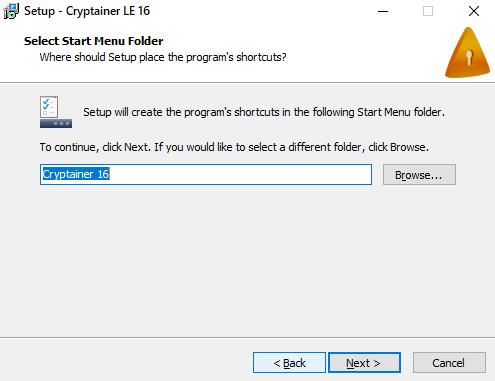
[Download Cryptainer Lite Free Encryption Software (cypherix.com)](https://www.cypherix.com/cryptainer-le-download-center.html) и устанавливаем программу

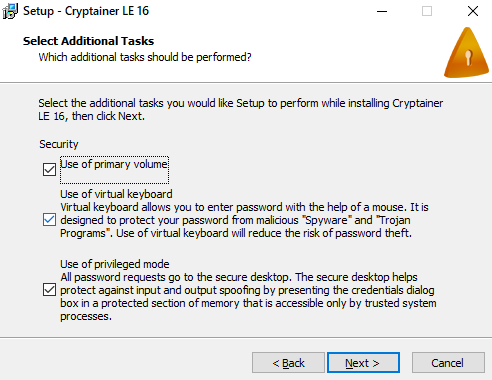
Ссылка: <https://www.cypherix.com/cryptainer-le-download-center.html>





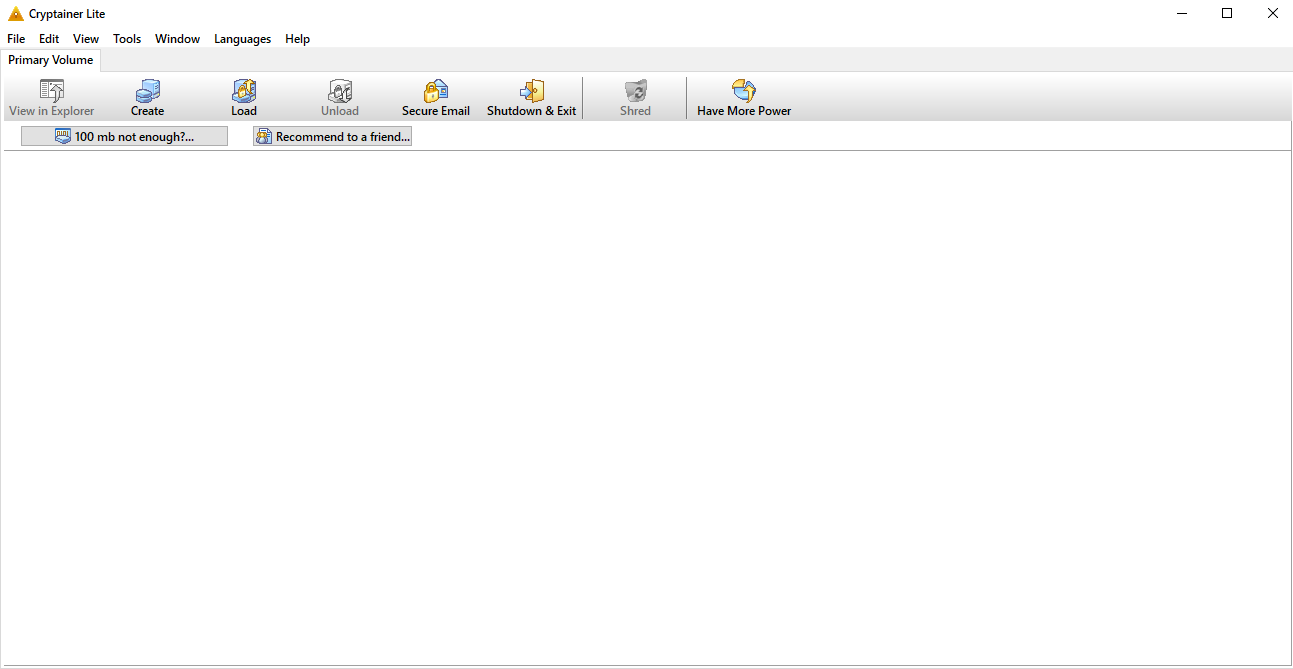




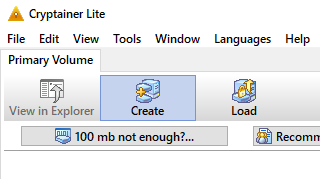




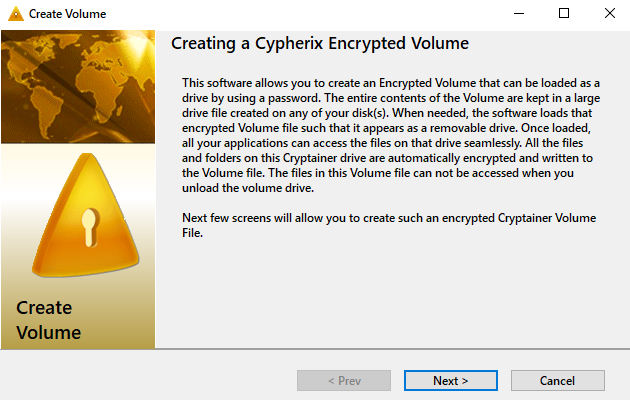
После установки программы, запустите ее



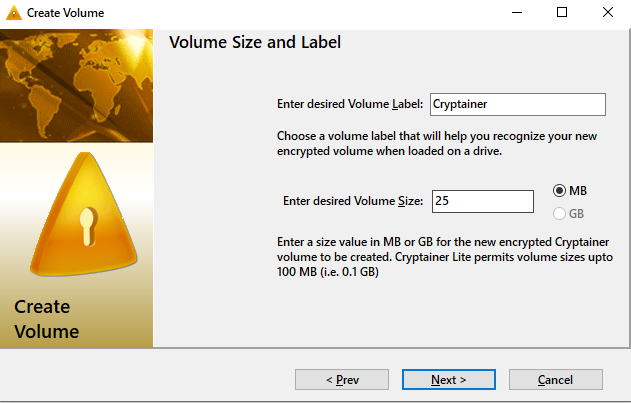
Для того чтобы создать диск, на главной панели нажмите Create



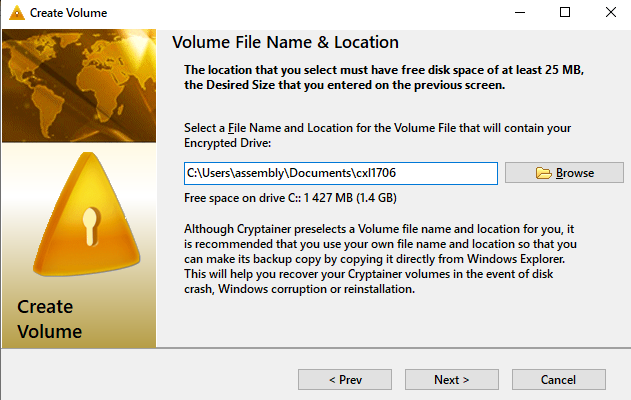
Далее открывается шифрование и создание диска. Делаем все как на скриншотах



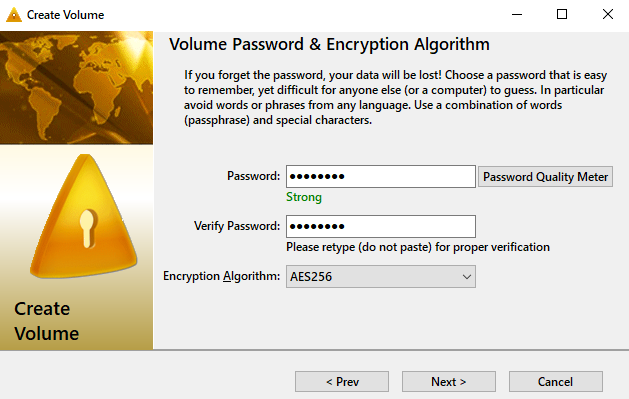
Можете изменить название диска и выбрать размер.



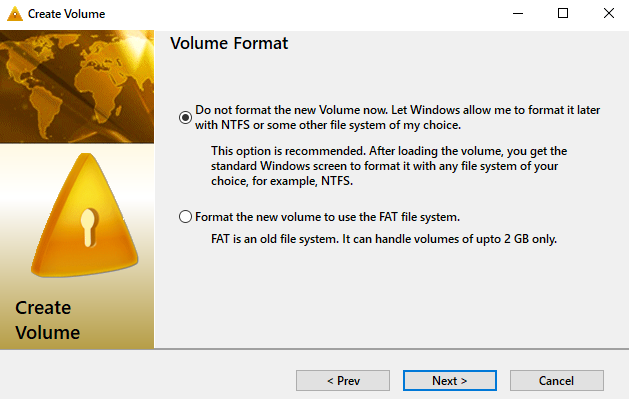
Обязательно запомните путь, ведь там будут храниться все ваши созданные разделы дисков



Придумываем пароль для нашего диска. Пароль нужен будет для открытия/сокрытия диска.



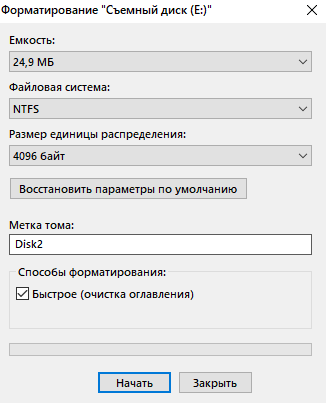
Выбираем формат файла как на картинке



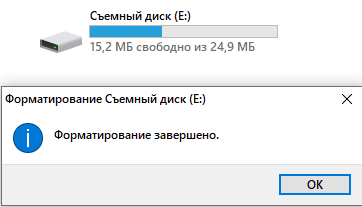
Готово, осталось отформатировать диск под нужный формат



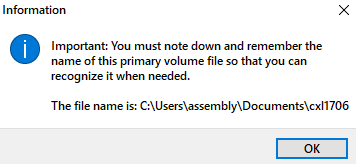
Выбирайте вкладку «Файловая система» из предложенных вариантов ставьте NTFS



После чего у вас создастся диск



Вас уведомят запомнить путь к файлу. Теперь ваш созданный диск готов к работе.



Для того, чтобы скрыть диск найдите на главной панели Unload. После нажатия, ваш диск скроется.

1. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

С помощью реализованного приложения выполнить задания, описанные выше.

1. КОНТРОЛЬНЫЕ ВОПРОСЫ:
2. Какие преимущества и недостатки есть у контейнера для хранения данных?
3. Каких два типа шифрования дисков существуют. Опишите их?
4. Для чего нужны скрытые разделы жесткого диска?
5. Является ли сокрытие данных и дисков полной гарантией конфиденциальности данных?
6. Что такое прозрачное шифрование ?

4. ЛИТЕРАТУРА

1. Ким Х. Сокрытие данных на винчестере. – Издательство "БХВ-Петербург", 2018.
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. Черный В. Компьютерная безопасность. – Издательство "Питер", 2019.
6. У. Столлингс. Шифрование и криптография.

Преподаватель Д.А. Бунькевич

Рассмотрено на заседании цикловой комиссии

программного обеспечения информационных технологий

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2022

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