Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

BITLOCKER И BITLOCKER TO GO

отчет о лабораторной работе №12

по дисциплине
ОПЕРАЦИОННЫЕ СИСТЕМЫ И ИХ БЕЗОПАСНОСТЬ

Выполнила: студент гр. 230711 Павлова В.С.

Проверил: доцент каф. ИБ Антонов Д.М.

Тула, 2023 г

Лабораторная работа – Bitlocker and Bitlocker To Go

Введение

Шифрование может защитить данные на вашем устройстве, делая доступ к ним только авторизованными людьми. Если шифрование устройства недоступно на вашем устройстве, вы можете вместо этого включить стандартное шифрование BitLocker.

Примечание . BitLocker доступен только в следующих версиях Windows:

- Максимальная и Корпоративная версии Windows 7
- Версии Pro и Enterprise для Windows 8 и 8.1
- Профессиональная, корпоративная и образовательная версии Windows 10.

В этой лабораторной работе вы включите шифрование BitLocker на съемном диске с данными и на системном диске компьютера.

Рекомендуемое оборудование

- ПК под управлением Windows
- Съемный USB-накопитель

инструкции

Part 1: Используйте BitLocker для перехода

В этой части вы будете использовать BitLocker to Go для шифрования съемного накопителя.

Step 1: Зашифруйте съемный диск.

a. Вставьте съемный диск, например USB-накопитель, в компьютер.

b. BitLocker отключен по умолчанию и должен быть включен для каждого диска, которому требуется шифрование. Чтобы включить и настроить BitLocker, перейдите в **Панель управления** > в представлении «Мелкие значки» нажмите **«Шифрование диска BitLocker** ».

c. В разделе **Съемные диски с данными** разверните список по мере необходимости. Выберите **Включить BitLocker** для нужного съемного диска.

d. В окне **Выберите, как вы хотите разблокировать этот диск** , установите флажок **Использовать пароль для разблокировки диска** , а затем введите пароль. Нажмите **Далее** , чтобы продолжить.

e. В разделе **Как вы хотите создать резервную копию ключа восстановления** выберите **Печать** или **Сохранить в файл** , а затем нажмите кнопку **Далее** .

f. В окне **Выберите объем диска для шифрования** выберите **«Зашифровать весь диск»** и нажмите **«Далее»** .

g. Если вам будет предложено окно **«Выберите режим шифрования»**, выберите «**Совместимый режим»** и нажмите **«Далее»**, чтобы продолжить.

h. В окне **Готовы ли вы зашифровать этот диск** нажмите **Начать шифрование** .

i. Через несколько минут съемный диск будет зашифрован. Теперь его можно удалить.

Step 2: Получите доступ к зашифрованному диску.

a. Вставьте съемный диск, предварительно зашифрованный на предыдущем шаге, в USB-порт компьютера.

b. Перейдите к USB-накопителю в **проводнике** или **проводнике Windows** и откройте USB-накопитель. (Если вам не удается открыть USB-накопитель, щелкните правой кнопкой мыши зашифрованный диск и выберите **Разблокировать диск** .)

c. Нажмите кнопку **Дополнительные параметры** . Обратите внимание, что есть возможность ввести ключ восстановления. Если пароль забыт, для разблокировки диска можно использовать сохраненный или распечатанный ключ восстановления из предыдущего шага.

Вопрос:

Почему важно сохранять ключ восстановления BitLocker?

Это важно, поскольку он позволяет разблокировать и получить доступ к зашифрованному диску в случае утери или забывания пароля

d. Введите пароль, чтобы разблокировать USB-накопитель. Теперь вы можете получить доступ к содержимому зашифрованного диска.

Step 3: Расшифровать диск.

a. Перейдите к **панели управления** > в представлении «Мелкие значки» нажмите **«Шифрование диска BitLocker**».

b. Выберите зашифрованный съемный диск. Если диск заблокирован, введите пароль, чтобы разблокировать его. Щелкните **Отключить BitLocker** .

c. Нажмите **«Отключить BitLocker»** , когда появится сообщение о том, что процесс расшифровки может занять некоторое время. Обратите внимание на предупреждающее сообщение, чтобы не повредить содержимое диска.

d. Нажмите **«Закрыть»** , когда процесс расшифровки завершится.

Part 2: Зашифровать диск операционной системы

В этой части лабораторной работы вы будете использовать BitLocker для шифрования диска операционной системы.

Step 1: Включите BitLocker.

a. Вернитесь в **Панель управления > Система и безопасность > Шифрование диска BitLocker** , чтобы включить BitLocker для диска операционной системы.

b. В **разделе «Диск операционной системы»** выберите **«Включить BitLocker»** .

Примечание . Если появляется сообщение об ошибке, в котором говорится, что устройство не может использовать доверенный платформенный модуль, необходимо выполнить некоторые дополнительные действия, чтобы разрешить дополнительную аутентификацию при запуске. Нажмите **«Отмена»** и выполните следующие дополнительные действия:

1) Введите **gpedit.msc** в **поиске Windows** , чтобы открыть **редактор локальной групповой политики** .

2) Разверните узел **Административные шаблоны** на левой панели и щелкните **Компоненты Windows** .

3) В списке компонентов Windows выберите **Шифрование диска BitLocker** . Выберите **Диски операционной системы** . Выберите **Требовать дополнительную аутентификацию при запуске** .

4) В окне **«Требовать дополнительную аутентификацию** при запуске» нажмите кнопку **«Включено»** , затем нажмите **«Применить** » и **«ОК»** , чтобы закрыть окно.

5) Закройте **редактор локальной групповой политики** , чтобы вернуться в окно **BitLocker Drive Encryption** , и нажмите **«Включить BitLocker»** .

c. Откроется окно Выберите **, как вы хотите разблокировать этот диск .** В этом окне установите флажок « **Использовать пароль для разблокировки диска»,** выберите **«Ввести пароль»** , затем введите пароль и нажмите « **Далее»** .

d. В разделе **Как вы хотите создать резервную копию ключа восстановления** выберите **«Печать»** или **«Сохранить в файл»** , а затем нажмите **«Далее»** .

e. В окне **Выберите объем диска для шифрования** выберите **«Шифровать только занятое место на диске»** и нажмите **«Далее»** .

f. В окне **Выберите, какой режим шифрования использовать** , выберите **Новый режим шифрования** и нажмите **Далее** .

g. В окне **«Готовы ли вы зашифровать этот диск»** убедитесь, что установлен флажок « **Запустить систему BitLocker» , и нажмите «Продолжить».** Появится сообщение о том, что компьютер необходимо перезагрузить.

h. Щелкните **Перезагрузить сейчас** , чтобы перезагрузить компьютер.

i. Когда компьютер перезагрузится, вам будет предложено ввести пароль, чтобы разблокировать компьютер.

Вопрос:

Какова функция TPM по отношению к BitLocker?

TPM (Trusted Platform Module) предоставляет аппаратную основу для хранения ключей, шифрования и обеспечения окружения (платформы) для процесса шифрования, т.е. общая функция TPM в контексте BitLocker заключается в обеспечении безопасности процесса шифрования и защите ключей шифрования, что делает данные на зашифрованном диске более надежными и защищенными от несанкционированного доступа.

Step 2: Отключите BitLocker.

a. Чтобы отключить BitLocker, вернитесь в **Панель управления** > **Система и безопасность** > **Шифрование диска BitLocker** и выберите **Отключить BitLocker** .

b. Щелкните **Отключить BitLocker, чтобы** расшифровать диск. Этот процесс может занять некоторое время в зависимости от размера диска.