

Навчально-науковий інститут інформаційних технологій  
Харківський національний економічний університет  
імені Семена Кузнеця

Звіт  
З Виконання лабораторної роботи №3  
за дисципліною: “ Безпека банківських систем ”  
на тему: “ВИВЧЕННЯ СИСТЕМИ ЗАХИСТУ ДАНИХ BITLOCKER DRIVE  
ENCRYPTION”

Виконав: студент кафедри  
Кібербезпеки та інформаційних  
технологій

4 курсу, спец. Кібербезпека,  
групи 6.04.125.010.21.2

Бойко Вадим Віталійович

Перевірив:  
Лимаренко Вячеслав Володимирович

ХНЕУ ім. С. Кузнеця

2024

Мета: вивчити алгоритми симетричного шифрування та одностороннього хешування. Ознайомитись з можливостями сучасних програм шифрування даних на прикладі програми BitLocker Drive Encryption.

Завдання:

1. За допомогою програми BitLocker створити зашифрований том на USB-носії.
2. Створити текстовий файл із певною послідовністю символів, помістити файл на змонтований носій, розмонтувати, спробувати виявити послідовність під час перегляду файлу звичайними засобами перегляду.
3. Спробувати змонтувати USB-носії при неправильному паролі.
4. Перенести USB-носії на інший комп'ютер та спробувати його змонтувати і переглянути файл.
5. Виконати аналіз джерел Інтернет на наявність інформації про надійність та можливість обходу BitLocker.

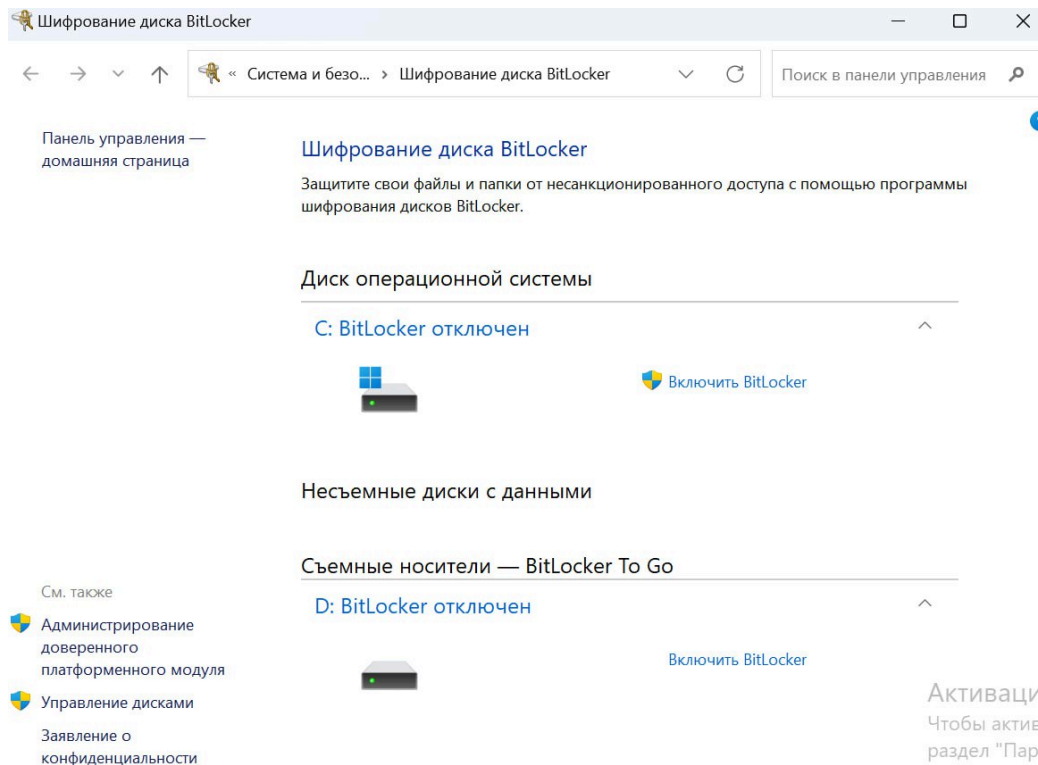
Контрольні питання:

1. Назвіть основні можливості BitLocker.
2. Який принцип роботи BitLocker?
3. Чи можна за допомогою BitLocker заборонити використання на ПК стороннього завантажувального USB-носія?
4. Чи можна файли, що зашифровані за допомогою BitLocker на USB-носії, переглянути на іншому комп'ютері?

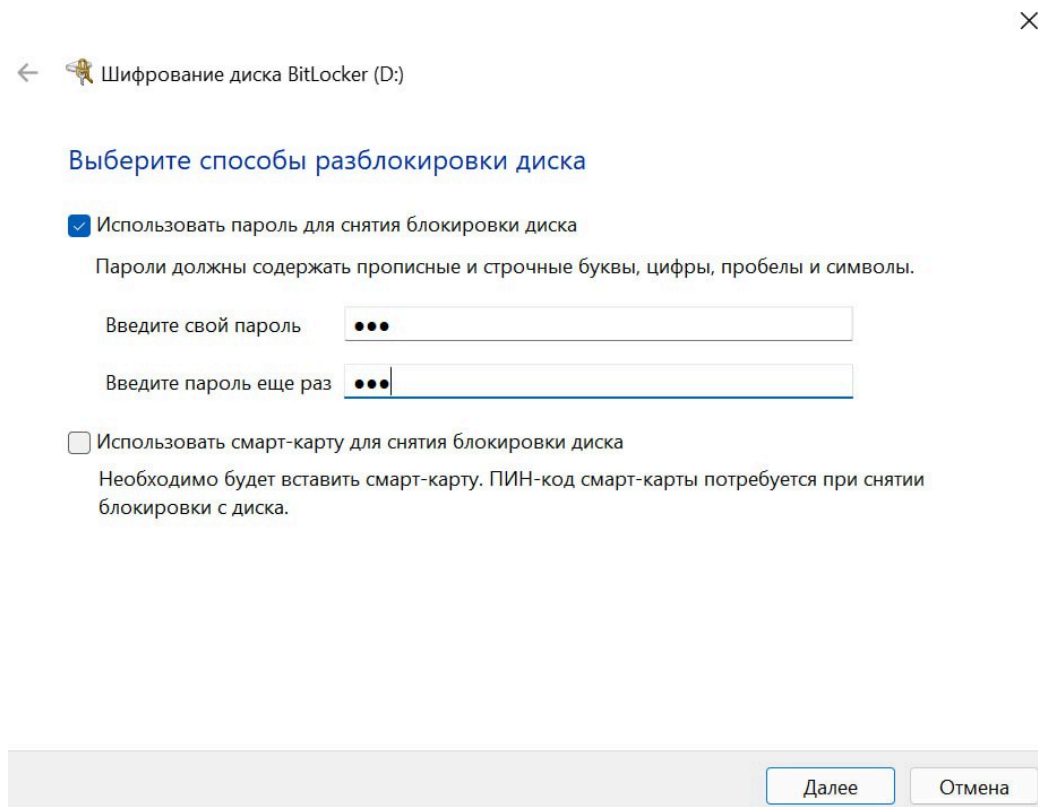
Хід роботи:

## Завдання № 1

Переходжу до налаштувань й обираю “Включить BitLocker” для диска “D”



Встановлюю пароль для доступа до носія




## Після встановлення паролю збережу ключ для відновлення



←  Шифрование диска BitLocker (D:)

### Как вы хотите архивировать свой ключ восстановления?

 Некоторыми параметрами управляет системный администратор.

Если вы забыли свой пароль или потеряли смарт-карту, вы можете использовать ключ восстановления для доступа к диску.

→ Сохранить в вашу учетную запись [Майкрософт](#)

→ Сохранить в файл

→ Напечатать [ключ восстановления](#)


[Как найти позже ключ восстановления?](#)

Далее

Отмена

## Оберу зашифрувати весь диск



←  Шифрование диска BitLocker (D:)

### Укажите, какую часть диска требуется зашифровать

Если вы настраиваете BitLocker на новом диске или ПК, вам достаточно зашифровать только ту часть диска, которая сейчас используется. BitLocker зашифровывает новые данные автоматически по мере их добавления.

Если вы включаете BitLocker на уже используемом ПК или диске, рекомендуется зашифровать весь диск. Это гарантирует защиту всех данных — даже удаленных, но еще содержащих извлекаемые сведения.

☐ Шифровать только занятое место на диске (выполняется быстрее, оптимально для новых ПК и дисков)


☒ Шифровать весь диск (выполняется медленнее, подходит для уже используемых ПК и дисков)

Далее

Отмена

## Оберу режим шифрування



←  Шифрование диска BitLocker (D:)

### Выбрать режим шифрования для использования

В обновлении Windows 10 (версия 1511) представлен новый режим шифрования дисков (XTS-AES). Этот режим обеспечивает дополнительную поддержку целостности, но не совместим с более ранними версиями Windows.

Если вы собираетесь использовать съемный носитель с более ранней версией Windows, следует выбрать режим совместимости.

Если будет использоваться несъемный диск или этот диск будет использоваться на устройствах под управлением обновления Windows 10 (версия 1511) или более поздних версий, следует выбрать новый режим совместимости

- ☐ Новый режим шифрования (оптимально для несъемных дисков на этом устройстве)
- ☒ Режим совместимости (оптимально для дисков, которые могут быть перемещены с этого устройства)

Далее

Отмена

## Й почну шифрування



←  Шифрование диска BitLocker (D:)

### Зашифровать этот диск?

Вы сможете разблокировать этот диск с помощью пароля.

Процесс шифрования может быть долгим, его длительность зависит от размера диска.

До завершения шифрования защита файлов не обеспечивается.

Начать шифрование

Отмена

Й починаю доки шифрування буде виконано

## Шифрование диска BitLocker



Выполняется шифрование...

Диск D: завершено: 1.1%



Пауза

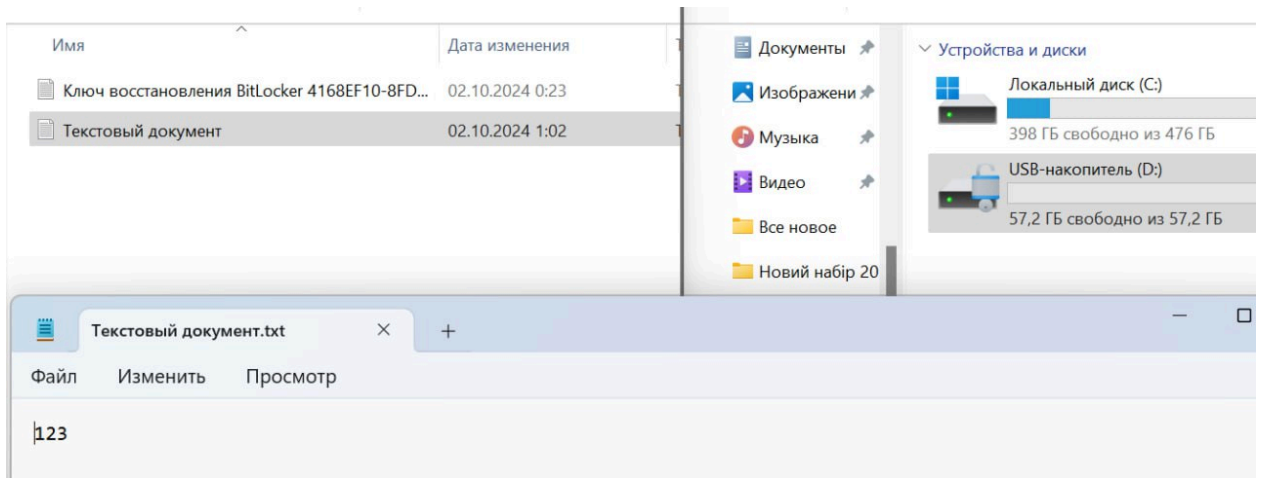


Во избежание повреждения файлов на диске  
приостановите шифрование перед удалением диска.

[Управление BitLocker](#)

## Завдання № 2

Створю текстовий документ та додаю його до носію



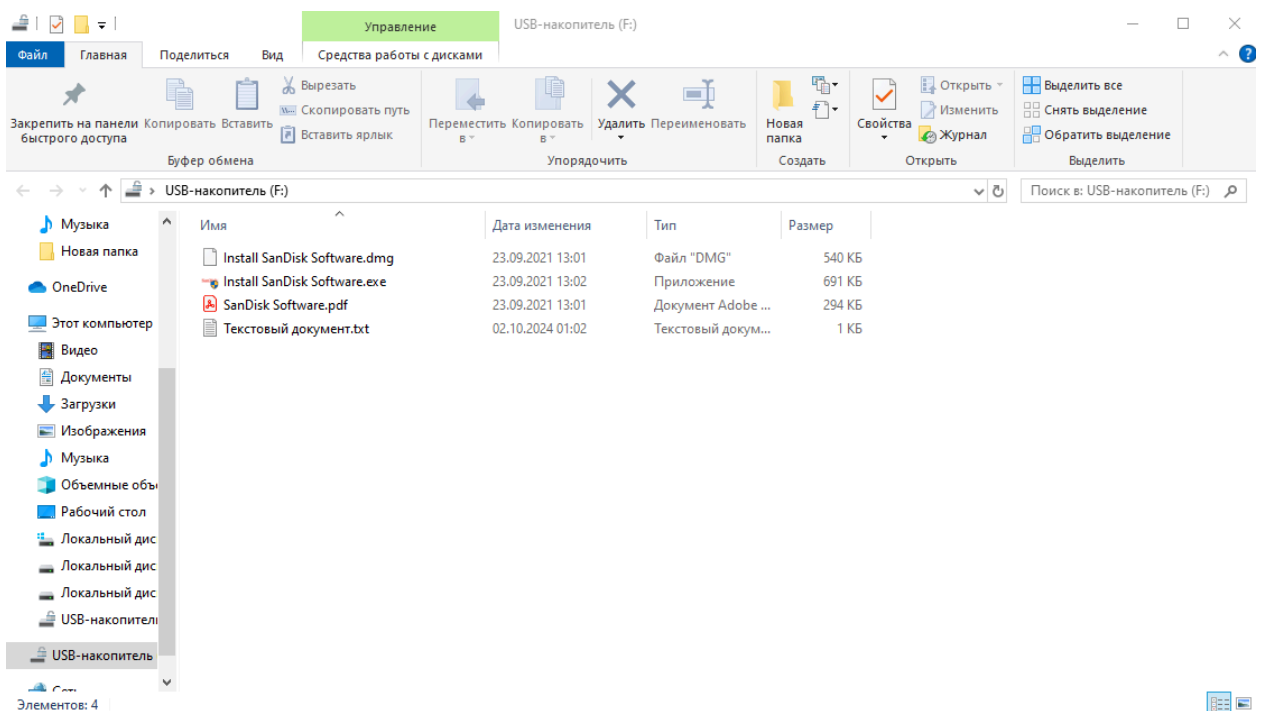
в результаті, якщо розмонтувати диск, тоді не має доступу до файлу

## Завдання № 3, 4

Спробую ввести не вірний пароль

Пише, що пароль не вірний

В результаті як тільки пароль буде вірний - ми отримаємо доступ до носія



## Завдання №5

Після пошуку в інтернеті можна знайти статтю, що BitLocker можна обійти

Посилання на статтю: <https://xakep.ru/2017/02/23/bitlocker-hacking/>



Відповіді на контрольні запитання:

1. Назвіть основні можливості BitLocker.

BitLocker – це потужний інструмент шифрування дисків, вбудований в операційні системи Windows, який пропонує наступні основні можливості:

- a. Шифрування цілих томів: BitLocker дозволяє зашифрувати весь фізичний або логічний диск, включаючи системний розділ. Це забезпечує захист усіх даних на диску, навіть якщо він буде вилучений з системи.
- b. Підтримка різних алгоритмів шифрування: BitLocker підтримує декілька сильних алгоритмів шифрування, таких як AES-128, AES-256, що гарантує високий рівень безпеки даних.
- c. Апаратне шифрування: Для підвищення продуктивності та безпеки BitLocker може використовувати апаратні модулі TPM (Trusted Platform Module), якщо вони доступні в системі.
- d. Гнучкі варіанти розблокування: Для доступу до зашифрованого диска можна використовувати різні методи аутентифікації, такі як пароль, PIN-код, смарт-карта або USB-ключ.
- e. Підтримка різних сценаріїв використання: BitLocker може бути налаштований для різних сценаріїв, включаючи використання в корпоративних мережах і для захисту персональних даних.

2. Який принцип роботи BitLocker?

BitLocker працює шляхом шифрування всього вмісту диска за допомогою вибраного алгоритму шифрування. При кожному завантаженні системи або доступі до зашифрованого диска BitLocker вимагає введення ключа розблокування. Після введення правильного ключа система дешифрує диск і дозволяє доступ до даних.

3. Чи можна за допомогою BitLocker заборонити використання на ПК стороннього завантажувального USB-носія?

BitLocker працює шляхом шифрування всього вмісту диска за

допомогою вибраного алгоритму шифрування. При кожному завантаженні системи або доступі до зашифрованого диска BitLocker вимагає введення ключа розблокування. Після введення правильного ключа система дешифрує диск і дозволяє доступ до даних.

4. Чи можна файли, що зашифровані за допомогою BitLocker на USB-носії, переглянути на іншому комп'ютері?

Так, файли, зашифровані за допомогою BitLocker на USB-носії, можна переглянути на іншому комп'ютері, якщо на цьому комп'ютері встановлено BitLocker і ви маєте ключ розблокування. Для цього необхідно:

- a. Підключити USB-носії до іншого комп'ютера.
- b. Розблокувати том: Ввести правильний ключ розблокування.
- c. Відкрити файли: Після розблокування ви зможете відкривати файли на USB-носії за допомогою стандартних засобів операційної системи.