ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №3

з курсу «Безпека банківських систем»

ВИВЧЕННЯ СИСТЕМИ ЗАХИСТУ ДАНИХ BITLOCKER DRIVE ENCRYPTION

Харків 2023

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

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Технологія шифрування BitLocker

Технологія шифрування BitLocker вперше з'явилася 16 років тому та змінювалася з кожною версією Windows. Однак далеко не всі зміни в ній мали підвищити криптостійкість. У роботі докладно розберемо будову різних версій BitLocker.

Технологія BitLocker стала відповіддю Microsoft на зростаючу кількість офлайнових атак, які щодо комп'ютерів з Windows виконувались особливо просто. Будь-яка людина із завантажувальною флешкою може відчути себе хакером. Вона просто вимкне найближчий комп'ютер, а потім завантажить його знову – вже зі своєю ОС та портативним набором утиліт для пошуку паролів, конфіденційних даних та препарування системи.

Наприкінці робочого дня з хрестовою викруткою і зовсім можна влаштувати невеликий хрестовий похід – відкрити комп'ютери співробітників, що пішли, і витягнути з них накопичувачі. Того ж вечора у спокійній домашній обстановці вміст витягнутих дисків можна аналізувати (і навіть модифікувати) різними способами. Наступного дня достатньо прийти раніше і повернути все на свої місця.

Втім, необов'язково розкривати чужі комп'ютери на робочому місці. Багато конфіденційних даних витікає після утилізації старих комп'ютерів і заміни накопичувачів. На практиці експлуатації безпечне стирання та низькорівневе форматування списаних дисків роблять одиниці. Що ж може завадити цим діям?

Основні обмеження Windows задаються на рівні прав доступу до об'єктів NTFS, які ніяк не захищають від офлайнових атак. Windows просто звіряє дозволи на читання та запис, перш ніж обробляє будь-які команди, які звертаються до файлів чи каталогів. Цей метод досить ефективний до тих пір, поки всі користувачі працюють у налаштованій системі з обмеженими обліковими записами. Однак варто підвищити права або завантажитися в іншій операційній системі, як від такого захисту не залишиться сліду. Користувач сам себе зробить адміністратором і перепризначить права доступу або легко проігнорує їх, поставивши інший драйвер файлової системи.

Є багато взаємодоповнюючих методів протидії офлайновим атакам, включаючи фізичний захист та відеоспостереження, але найефективніші з них вимагають використання стійкої криптографії. Цифрові підписи завантажувачів перешкоджають запуску стороннього коду, а єдиний спосіб по-справжньому захистити дані на жорсткому диску – це шифрувати їх.

1.2 Як використовувати BitLocker

Розберемо практичну частину на прикладі Windows 10. BitLocker можна увімкнути через панель управління (розділ «Система і безпека», підрозділ «Шифрування диска BitLocker», рис. 1).

Однак якщо на материнській платі відсутній криптопроцесор TPM версії 1.2 або новіший, то просто так BitLocker використати не вдасться. Щоб його активувати, потрібно зайти до редактора локальної групової політики (gpedit.msc) і розкрити гілку «Конфігурація комп'ютера —> Адміністративні шаблони —> Компоненти Windows —> Шифрування диска BitLocker —> Диски операційної системи» до налаштування «Цей параметр політики дозволяє налаштувати вимогу додаткової автентифікації під час запуску». У ньому необхідно знайти налаштування «Дозволити використання BitLocker без сумісного TPM...» та увімкнути його (рис. 2).

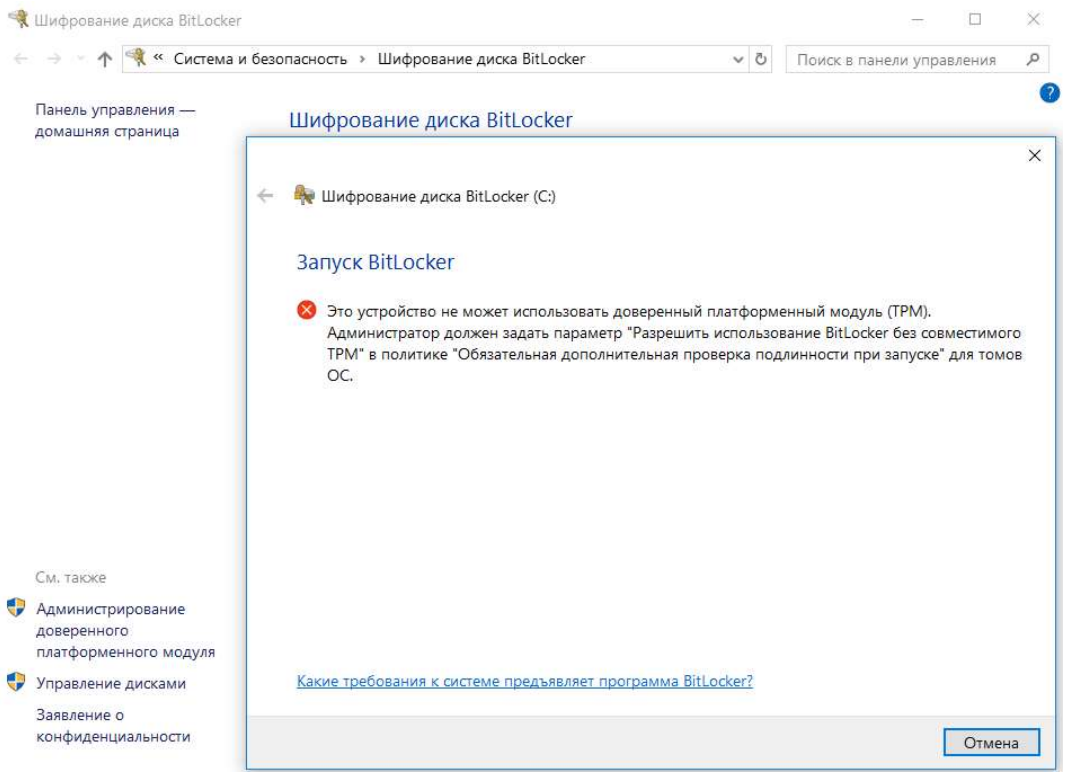

Рисунок 1 – Запуск BitLocker

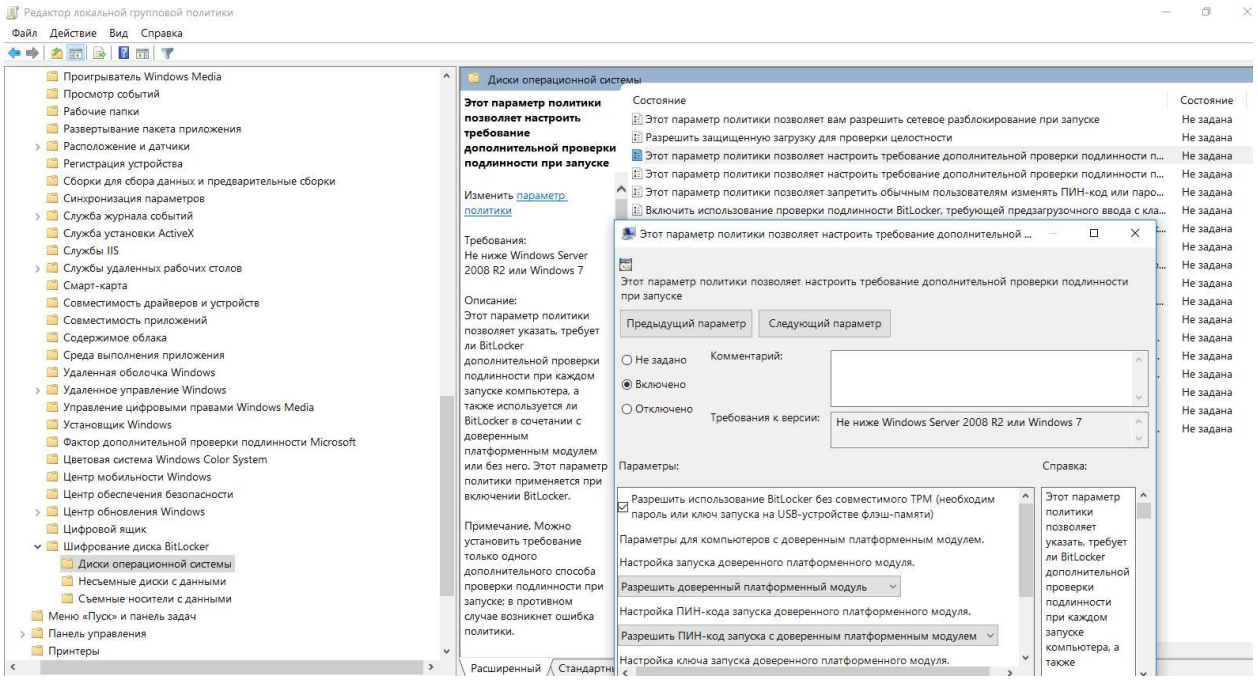

Рисунок 2 – Запуск BitLocker без криптопроцесору TPM

У сусідніх секціях локальних політик можна встановити додаткові налаштування BitLocker, у тому числі довжину ключа і режим шифрування за стандартом AES (рис. 3)

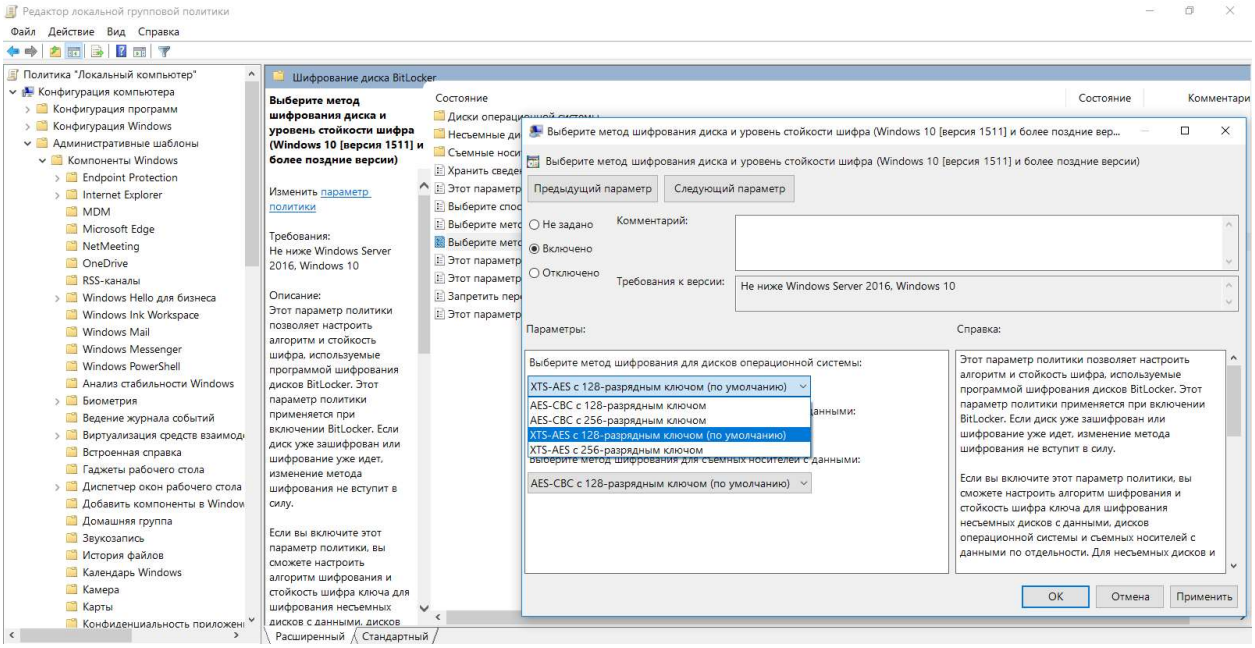

Рисунок 3 – Додаткові налаштування BitLocker

Після застосування нових політик повертаємося в панель управління та дотримуємося вказівок майстра налаштування шифрування. Як додатковий захист можна вибрати введення пароля або підключення певної флешки USB (рис. 4).

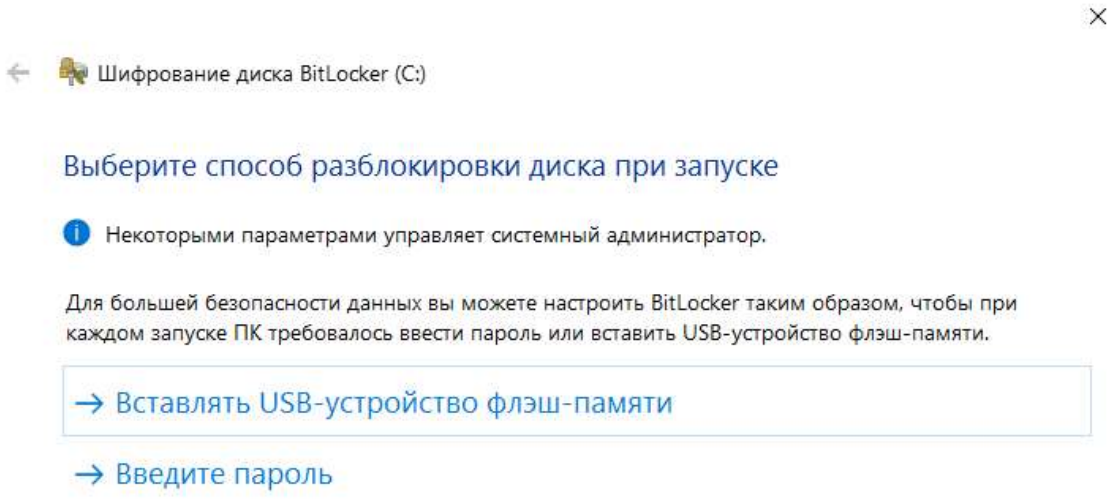

Рисунок 4 – Налаштовуємо розблокування комп'ютера під час увімкнення

На наступному етапі нам запропонують зберегти копію ключа у разі відновлення. За замовчуванням пропонується надіслати її на сервери Microsoft, записати у файл або навіть надрукувати (рис. 5).

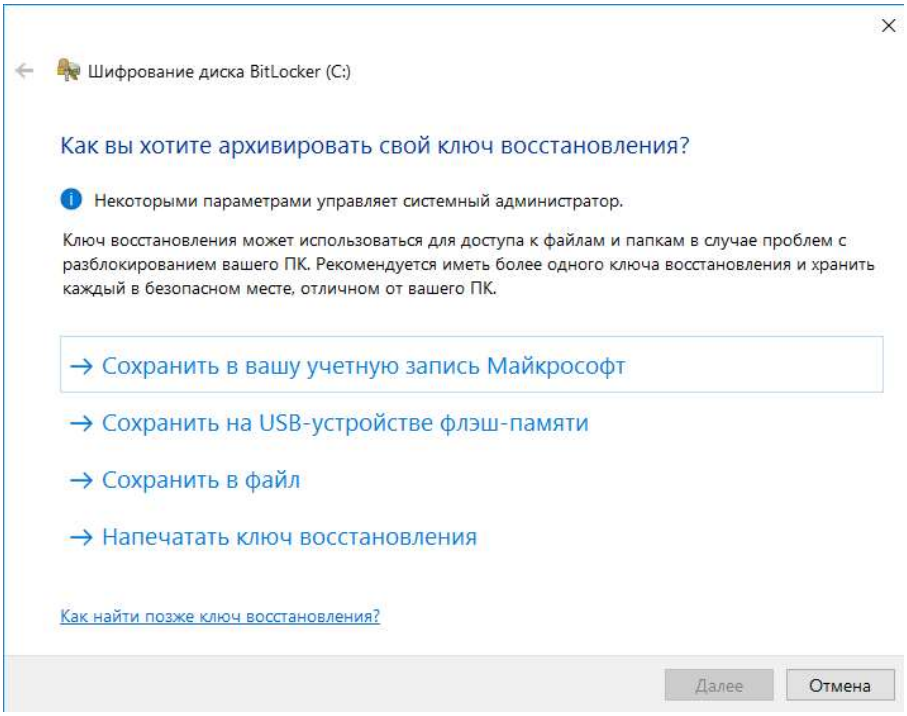

Рисунок 5 – Збереження ключа відновлення

Хоча BitLocker і вважається технологією повнодискового шифрування, вона дозволяє виконувати часткове шифрування лише зайнятих секторів. Це швидше, ніж шифрувати все поспіль, але такий спосіб вважається менш надійним. Хоча б тому, що при цьому видалені, але ще не перезаписані файли залишаються доступними для прямого читання (рис. 6).

Після налаштування всіх параметрів залишиться перезавантаження. Windows вимагає ввести пароль (або вставити флешку), а потім запуститься у звичайному режимі та почне фоновий процес шифрування тома (рис. 7).

Залежно від вибраних налаштувань, обсягу диска, частоти процесора та підтримки ним окремих команд AES, шифрування може зайняти від кількох хвилин до кількох годин.

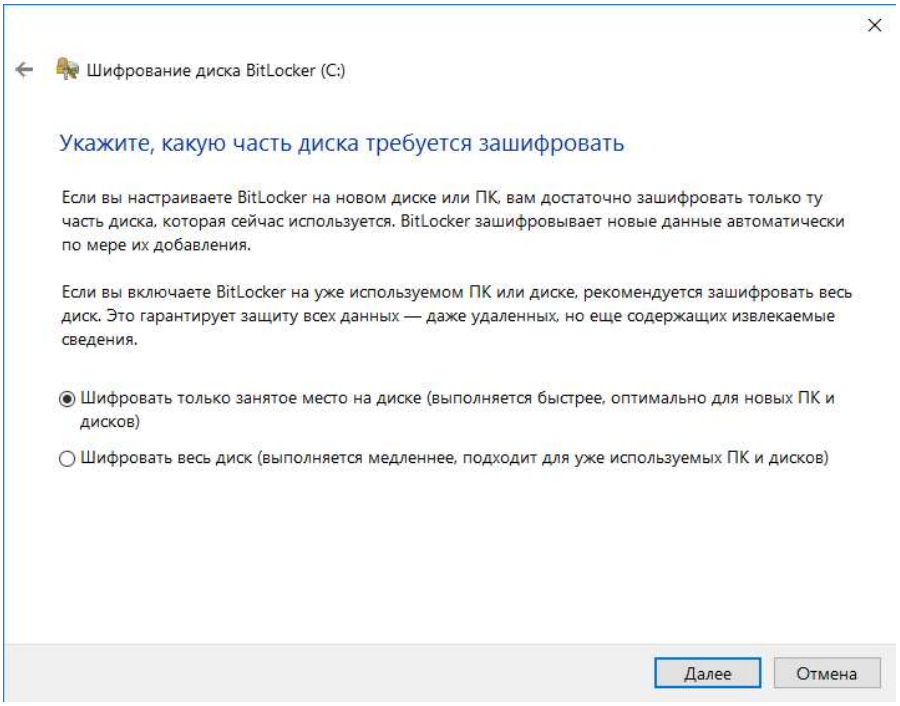

Рисунок 6 – Повне та часткове шифрування

Рисунок 7 – Запит пароля перед запуском Windows

Після завершення цього процесу в контекстному меню «Провідника» з'являться нові пункти: зміна пароля та швидкий перехід до налаштувань BitLocker (рис. 8).

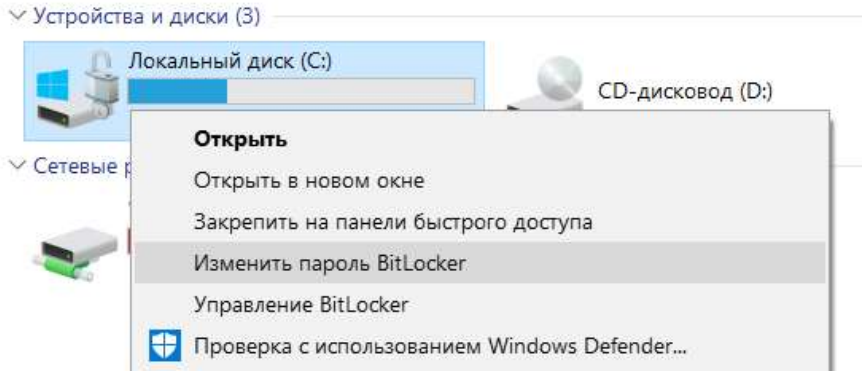

Рисунок 8 – Інтеграція BitLocker у контекстне меню

Зверніть увагу, що для всіх дій, крім зміни пароля, потрібні права адміністратора.

На цьому процес активації BitLocker закінчено.

3 ІНДИВІДУАЛЬНЕ 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-носій при неправильному паролі.

4. Перенести USB-носій 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?