Міністерство освіти і науки України
Національний авіаційний університет
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютеризованих систем управління

Лабораторна робота № 2.3
з дисципліни «Захист інформації в комп'ютерних системах»
на тему «Криптографічний захист даних у файлових системах»

Виконав:
студент ФККПІ
групи СП-425
Клокун В. Д.
Перевірила:
Супрун О. М.

Київ 2019

1. Мета роботи

Ознайомитися з основними проблемами захисту інформації у файлових системах та засобами їх розв'язання.

2. Завдання роботи

Встановити програмне забезпечення для криптографічного захисту даних у файлових системах та навчитися використовувати його функції.

3. Хід роботи

Щоб виконати завдання лабораторної роботи, встановлюємо та запускаємо програму VeraCrypt. Після запуску бачимо головне меню програми (рис. 1)

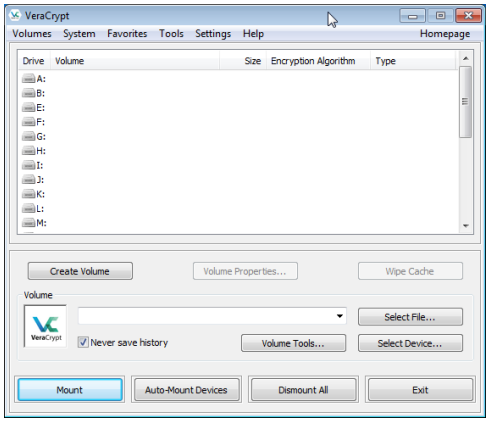


Рис. 1: Головне меню програми VeraCrypt

Створюємо новий том. Для цього у головному меню натискаємо кнопку «Create Volume»; з'явиться помічник зі створення тому (рис. 2). У помічнику можна обрати, як створити том: створити зашифрований файл-контейнер, зашифрувати несистемну партицію або диск чи зашифрувати системну партицію або диск. Обираємо створення зашифрованого контейнера і переходимо далі.

Після переходу далі відкрився екран вибору типу створюваного тому: стандартного або прихованого (рис. 3). Стандартний том створює звичайний зашифрований контейнер, тоді як прихований том — це ще один том VeraCrypt, який знаходиться всередині стандартного тому VeraCrypt.

Обравши тип тому, обираємо, де його зберігати. Для цього натискаємо кнопку «Select File...» і вказуємо розміщення і ім'я файлу, в якому зберігатиметься контейнер (рис. 4).

Обравши розміщення тому, обираємо параметри шифрування, яке буде ви-

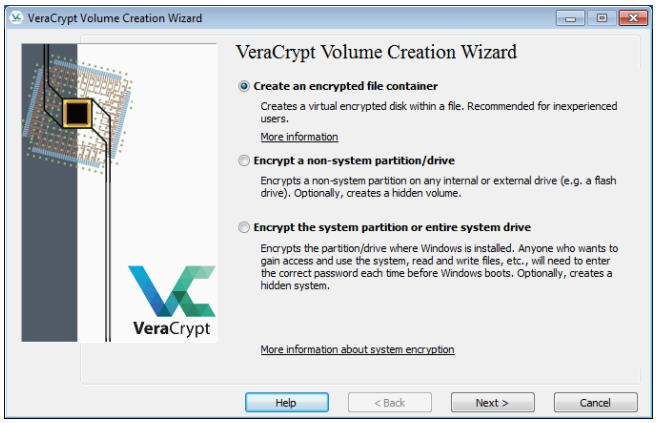


Рис. 2: Помічник зі створення тому VeraCrypt

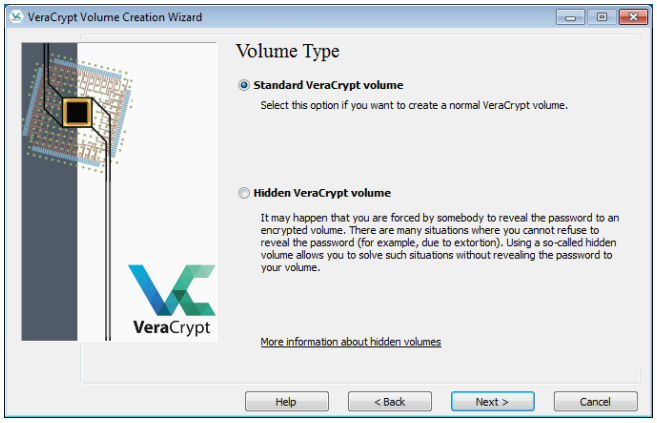


Рис. 3: Вибір типу тому VeraCrypt

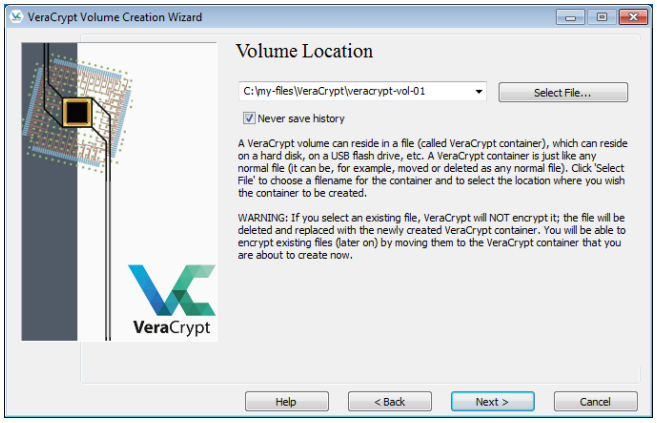


Рис. 4: Вибір розміщення тому VeraCrypt

користовуватись у ньому (рис. 5). За замовчуванням встановлені надійні значення, тому більшості користувачів варто залишити їх якими вони є.

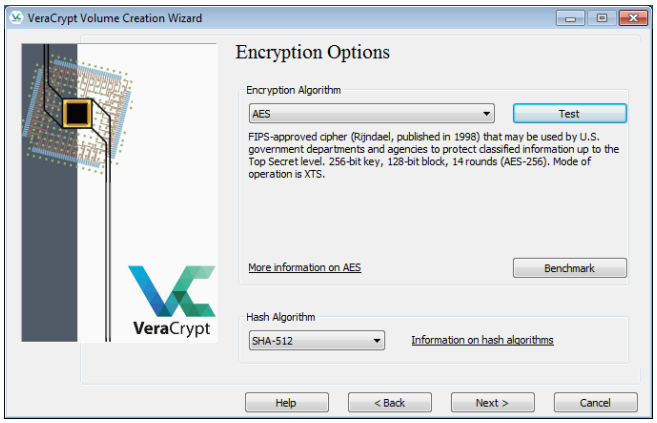


Рис. 5: Вибір налаштувань шифрування тому VeraCrypt

Після налаштування параметрів шифрування, необхідно задати розмір тому (рис. 6). Мінімальний розмір залежить від файлової системи, а максимальний обмежений лише вільним місцем на диску.

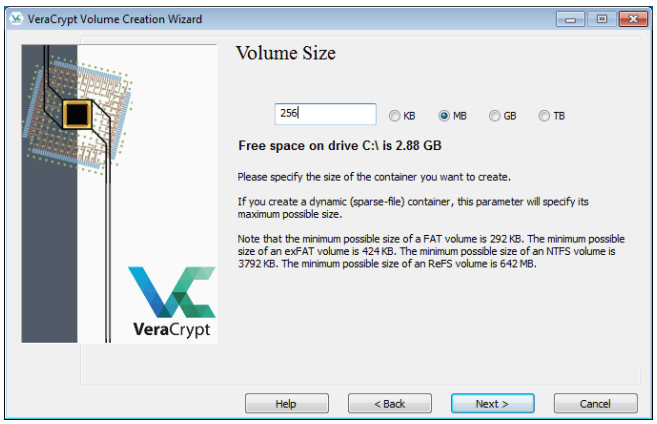


Рис. 6: Установка розміру тому VeraCrypt

Коли розмір тому встановлений, необхідно задати для нього пароль (рис. 7). Пароль має бути надійним, адже від нього залежить безпека усіх даних, які зберігаються у томі.

Після установки пароля програмі необхідні випадкові дані. Для цього вона збирає їх, зчитуючи рух користувача мишкою (рис. 8).

Зібравши необхідну кількість випадкових даних, програма створює контейнер, повідомляє користувача за допомогою відповідного повідомлення і переходить до фінального вікна (рис. 9).

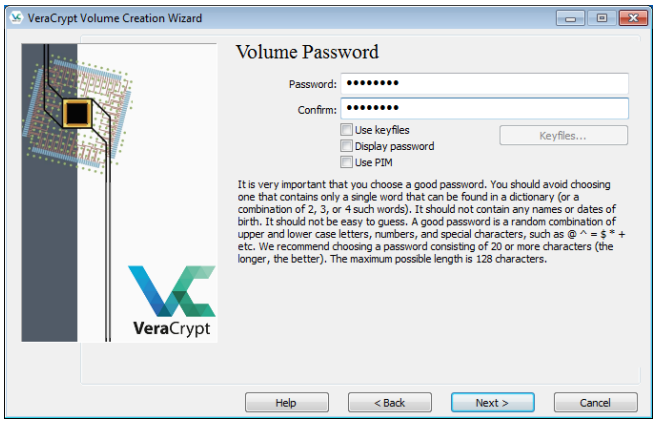


Рис. 7: Установка пароля тому VeraCrypt

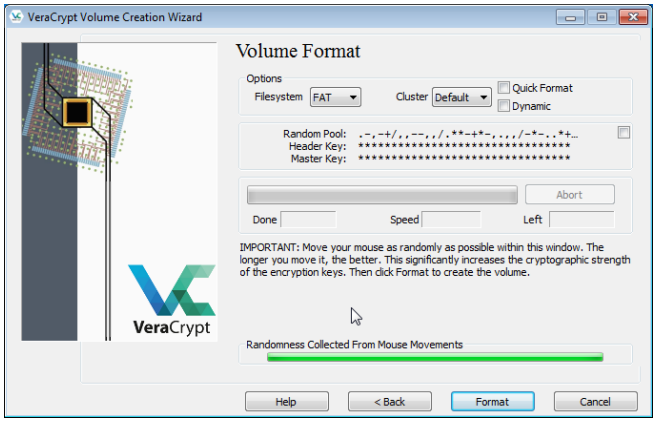


Рис. 8: Збір випадкових даних програмою VeraCrypt

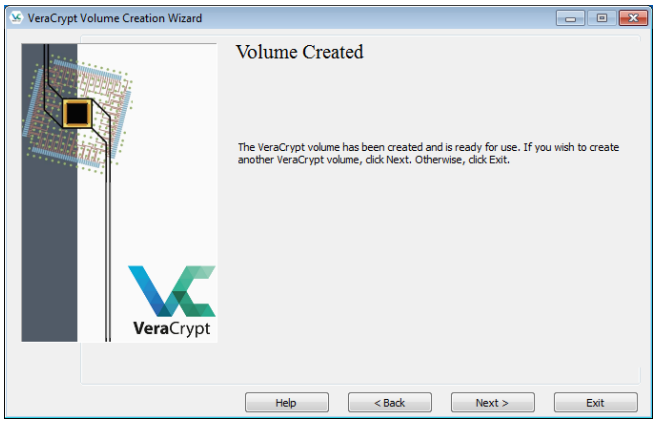


Рис. 9: Фінальне вікно помічника зі створення зашифрованого контейнера програми VeraCrypt

Тепер, коли контейнер створений, можна змонтувати його і працювати з його даними. Для цього відкриваємо головне меню програми VeraCrypt, обираємо файл з контейнером і натискаємо кнопку «Mount» (рис.10).

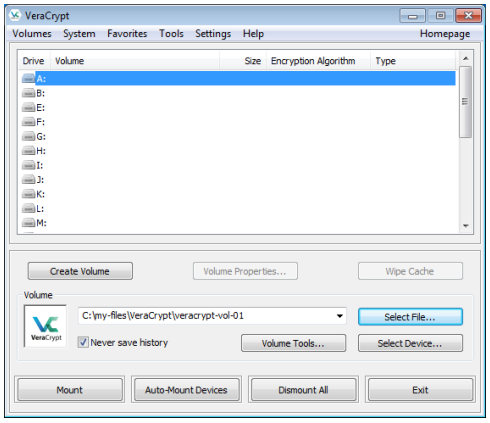


Рис. 10: Вибір зашифрованого контейнера для монтування

Після натискання на кнопку з'явиться діалогове вікно, яке запросить користувача ввести пароль або підтвердити свою особистість іншим способом, щоб змонтувати контейнер (рис. 11).

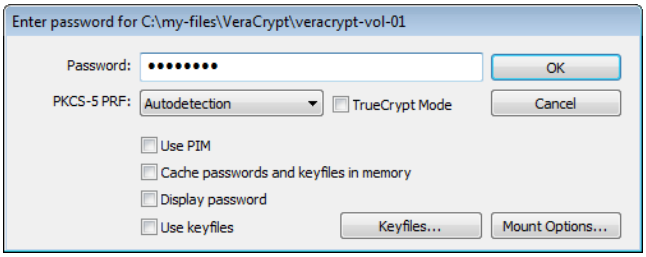


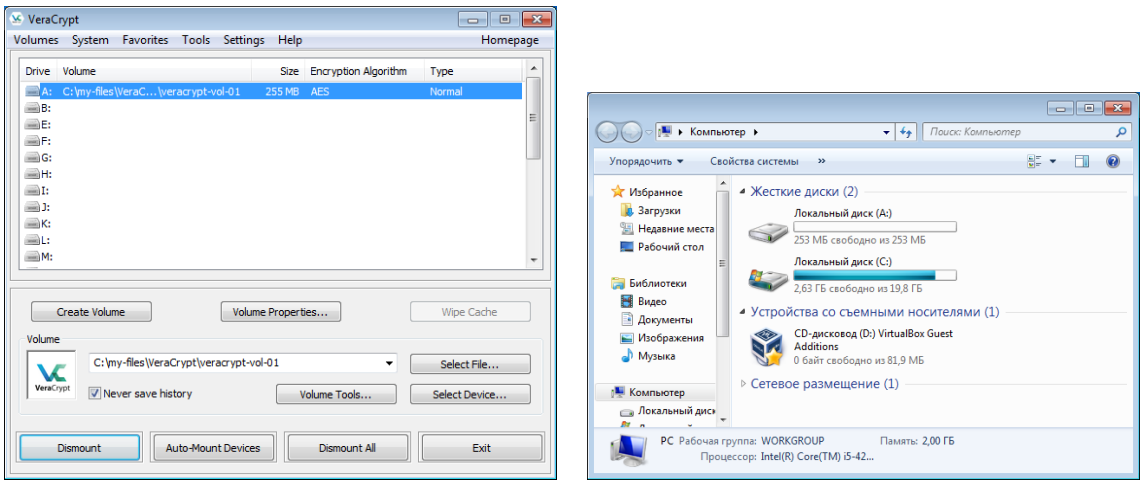
Рис. 11: Діалогове вікно для монтування контейнера

Зчитавши пароль, програма спробує змонтувати контейнер і в разі успіху він з'явиться у головному меню навпроти літери, яку користувач обрав під час монтування (рис. 12а). Також, контейнер буде підключений і доступний з Провідника Windows (рис. 12б).

Отже, тепер контейнер змонтований і готовий до роботи з його файлами.

4. Висновок

Виконуючи дану лабораторну роботу, ми ознайомилися з основними проблемами захисту інформації у файлових системах та засобами їх розв'язання.



а) б)

Рис. 12: Результат монтування контейнера