Модуль:

Практична вправа:
«Створення захищеного флеш-накопичувача»

Навчальна мета заняття: створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go та програми VeraCrypt.

Час проведення: 1 год. *Місце проведення:* комп'ютерний клас.

Устаткування:
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go, який повністю шифрує вміст флеш-накопичувача на рівні файлової системи. У випадку фізичної втрати флеш-накопичувача дані залишаться недоступними для читання.

Вставити флеш-накопичувач у USB порт та відкрити «Провідник файлів». Увімкнути BitLocker для диску флеш-накопичувача: клацнути правою кнопкою миші диск у вікні «Провідника файлів», а потім вибрати команду «Увімкнути BitLocker». Якщо немає цього параметра у контекстному меню, то, ймовірно, у вас не Windows Pro або Enterprise, і знадобиться шукати інше рішення для шифрування (рис. 1).

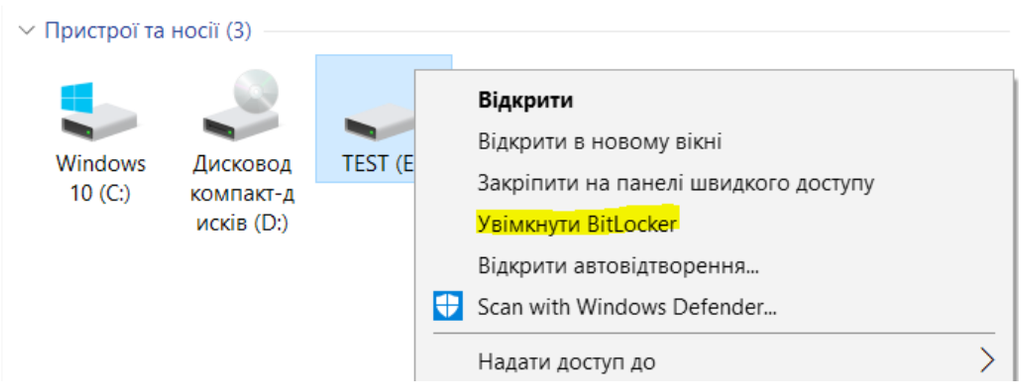

Рис. 1. Увімкнення BitLocker

Зачекати, поки BitLocker здійснить ініціалізацію диску, далі обрати спосіб розблокування диску – за допомогою паролю, обрати надійний пароль (рис. 2).

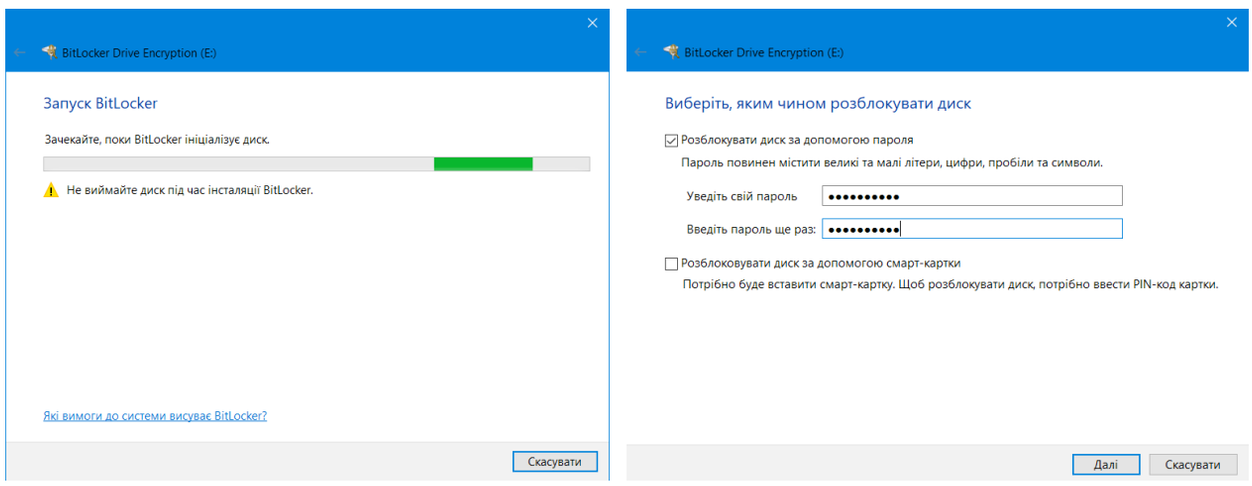

Рис. 2. Ініціалізація BitLocker та вибір способу розблокування диску

Далі BitLocker надає можливість створити ключ відновлення, який можна використовувати для доступу до зашифрованих файлів, якщо ви, наприклад, забудете пароль (рис. 3). Ключ відновлення можна зберегти у своєму обліковому записі Microsoft, на диску USB, файлі або навіть роздрукувати. Ці параметри є однаковими, якщо ви шифруєте системний або несистемний диск. Зберегти ключ відновлення у файл – зміст цього файлу можна скопіювати у парольний менеджер та видалити файл.

Далі обрати шифрування всього диску (рис. 3), режим сумісності для різних версій Windows та запустити шифрування диску (рис. 4).

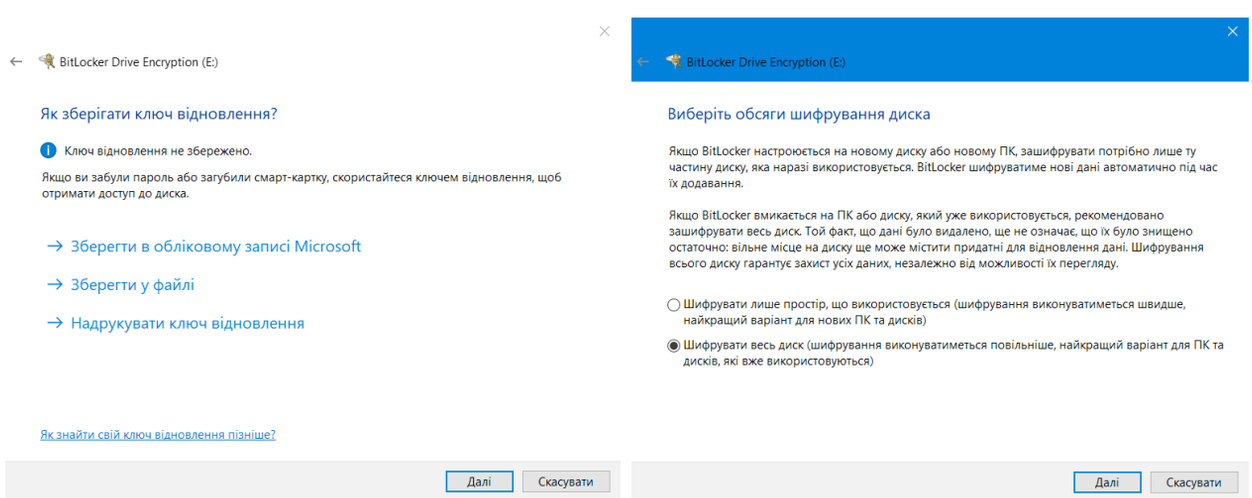

Рис. 3. Збереження ключа відновлення та вибір обсягу шифрування диску

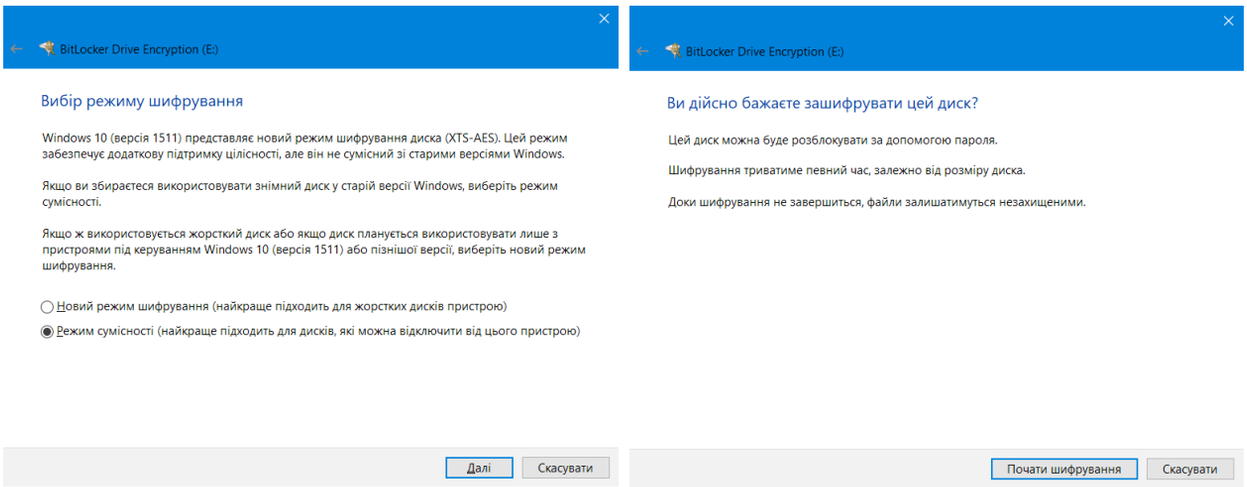

Рис. 4. Вибір режиму шифрування та початок шифрування

Після завершення шифрування у «Провіднику файлів» з'явиться відповідна піктограма розшифрованого диску, яка зміниться, якщо витягти диск і знову вставити, а також з'явиться запрошення ввести пароль для розшифрування диску (рис. 5).

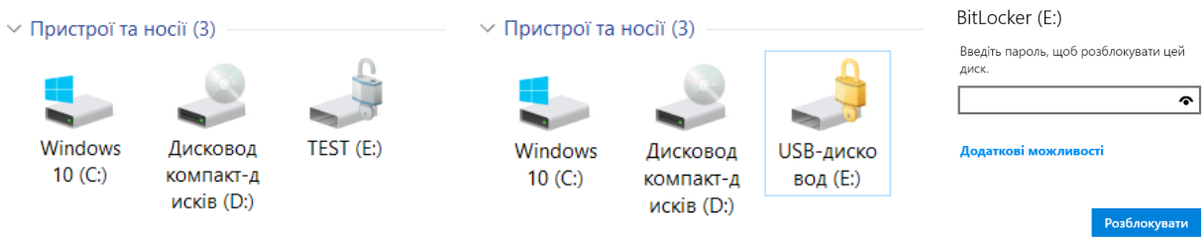

Рис. 5. Піктограми розшифрованого та зашифрованого диску, запрошення ввести пароль

Записати на розшифрований диск довільні файли, витягнути флеш-накопичувач та повторити процедуру розблокування, щоб переконатися у цілісності файлів після розшифрування.

Створити захищений флеш-накопичувач за допомогою безкоштовної утиліти з відкритим кодом «VeraCrypt», яка побудована на базі останньої версії TrueCrypt.

VeraCrypt використовує так званий контейнер. Стосовно VeraCrypt, контейнер – це оболонка, в якій у зашифрованому вигляді зберігаються всі файли. Фізично контейнер – це один файл. Отримати доступ до файлів, що є всередині контейнера-оболонки, можна тільки одним способом – ввівши правильний пароль. Процедура введення пароля і підключення контейнера називається «монтуванням».

Файли у VeraCrypt шифруються не по одному, а контейнерами. Коли програма підключає контейнер (монтує його), контейнер виглядає як флешка: з'являється новий диск, з яким можна робити будь-які операції – копіювати туди файли, відкривати файли, видаляти файли, редагувати файли. Роблячи це, не потрібно думати про шифрування: все, що всередині контейнера, вже надійно зашифровано і зберігається / шифрується в реальному часі. І як тільки вимкнути контейнер, то вхід до нього надійно закриється.

Завантажити архів портативної версії утиліти (portable version for Windows, https://www.veracrypt.fr/en/Downloads.html) та запустити розпакування.

З теки VeraCrypt запустити файл VeraCrypt-x64.exe та у меню «Settings» змінити мову програми на українську. Для цього клацнути на меню «Settings», там вибрати «Language ...» та обрати «Українська». Далі натиснути «Створити том» (том – це те саме, що і контейнер) (рис. 6).

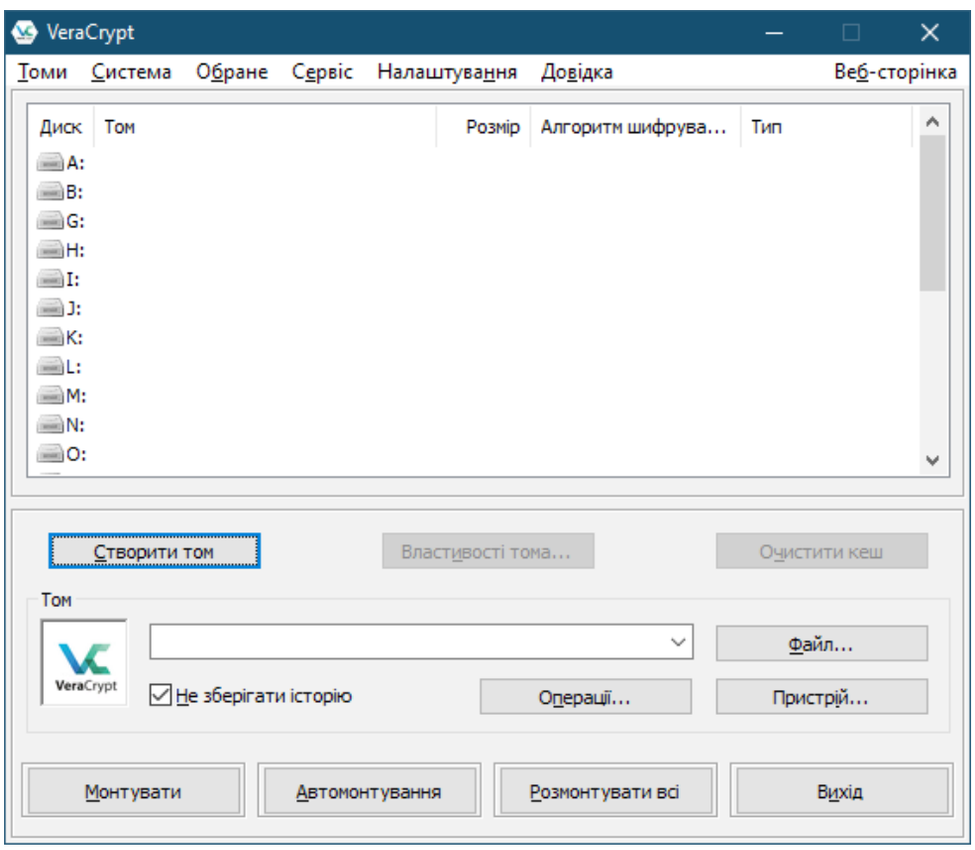

Рис. 6. Головне вікно VeraCrypt

Обрати «Зашифрувати несистемний розділ/диск», «Звичайний том VeraCrypt». Вибрати розміщення тома, вказавши як пристрій флеш-накопичувач. **ВАЖЛИВО: перевірити правильність вибору пристрою, який потім буде форматуватися.** Вибрати режим створення тома «Створити зашифрований том і відформатувати його» (рис. 7).

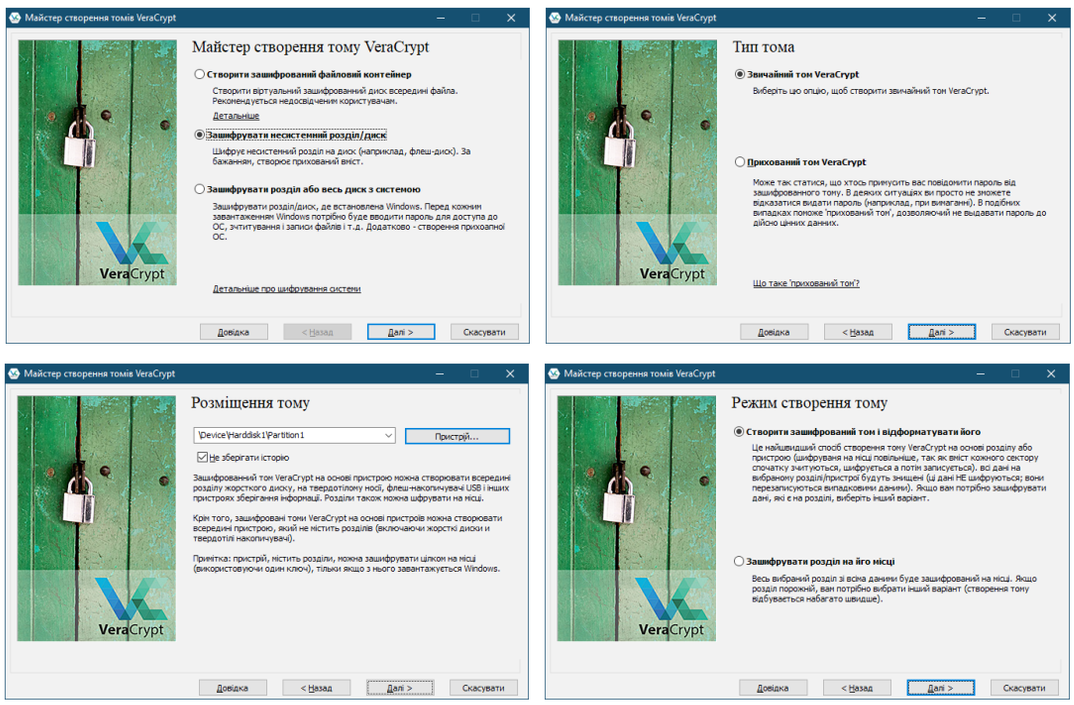

Рис. 7. Майстер створення тома

Налаштування шифрування залишити за замовчуванням. Встановити пароль тома, дотримуючись рекомендацій, що будуть запропоновані у вікні вибору паролю. Важливо запам'ятати пароль і ніде не записувати. Як рекомендація – взяти перші (останні) літери улюбленої довгої фрази із заміною деяких літер цифрами і символами. Для форматування тома випадковим чином рухати мишкою деякий час, а потім ініціювати форматування носія.

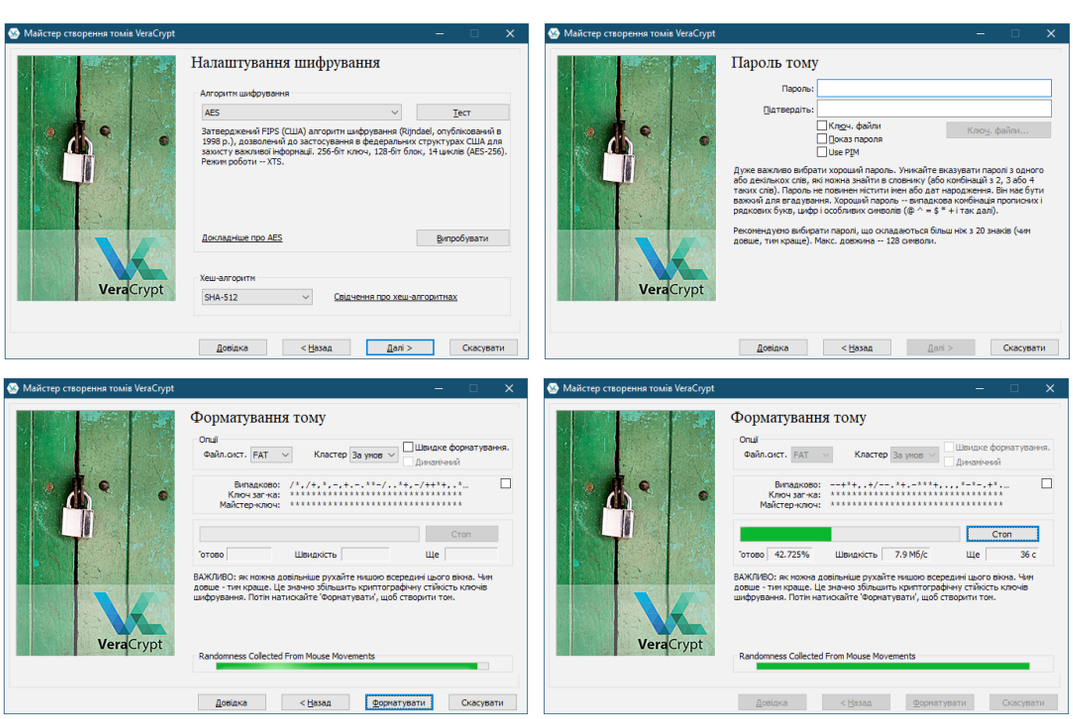

Рис. 8. Налаштування шифрування та форматування тома

Після форматування ознайомитися із порядком монтування тома. Захищений флеш-накопичувач створено.

Для користуванням захищеним носієм у головному вікні VeraCrypt вибрати у розділі «Пристрій» диск флеш-накопичувача, вільну літеру для диску, що буде змонтований, та натиснути «Монтувати» або «Автомонтування» (рис. 9).

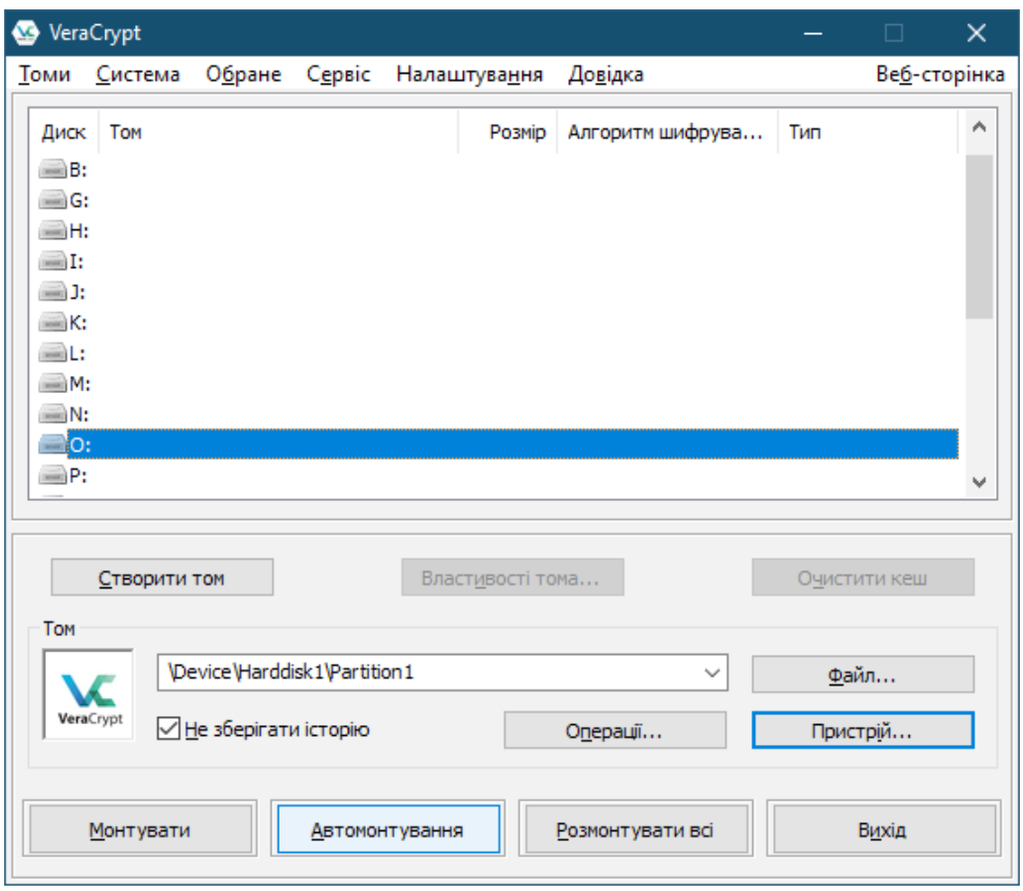

Рис. 9. Підключення зашифрованого диску

На запит ввести пароль, і буде створений новий логічний диск, з яким можна працювати: записувати і редагувати файли, запускати програми.

По закінченні роботи зі змонтованим диском у головному вікні VeraCrypt натиснути «Розмонтувати всі».

Перевірити надійність захисту інформації здійснити шляхом обміну змінними носіями і спробою відкрити диски.