Міністерство освіти і науки України
Національний університет водного господарства та природокористування
Кафедра обчислювальної техніки

04-04-279М

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з освітньої компоненти «Дослідження та оптимізація комп'ютерних систем» для здобувачів вищої освіти другого (магістерського) рівня за освітньою програмою «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання.

Частина 4.

Рекомендовано науково-методичною радою
з якості ННІКІТІ
Протокол №9 від 30.08.2024 р.

Рівне – 2024

Методичні вказівки до виконання лабораторних робіт з освітньої компоненти «Дослідження та оптимізація комп'ютерних систем» для здобувачів вищої освіти другого (магістерського) рівня за освітньою програмою «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання. Частина 4. [Електронне видання] / Круліковський Б. Б. – Рівне : НУВГП. – 35 с.

Укладач: Круліковський Б. Б., кандидат технічних наук, доцент кафедри обчислювальної техніки.

Відповідальний за випуск: Сидор А. І., завідувач кафедри обчислювальної техніки.

Керівник (гарант) освітньої програми «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» Круліковський Б. Б.

Протокол №1 засідання кафедри обчислювальної техніки від 27.08.2024 р.

ЗМІСТ

Вступ

Частина 4 дійсних методичних вказівок присвячена ознайомленню здобувачів спеціальності 123 «Комп’ютерна інженерія» другого (магістерського) рівня вищої освіти з найбільш поширеними і доступними інструментами дослідження та оптимізації персональних комп'ютерів, що працюють під керуванням операційних систем сімейства Windows. Особлива увага приділена засобам захисту інформації, що обробляється в системі, від спотворень внаслідок впливу зовнішніх дестабілізуючих факторів, роботи шкідливих програм та застосувань, завантажених з Internet, а також деструктивних дій зловмисників.

Зважаючи на військові обставини в методичних вказівках наводяться відомості тільки про безкоштовні та умовно-безкоштовні програмні засоби для вирішення проблем захищеності комп'ютерних систем. Використання такого програмного забезпечення дозволяє в значній степені підвищити продуктивність ПК, досягти оптимальних параметрів захищеності систем без додаткових матеріальних витрат.

Методична розробка містить короткі теоретичні відомості з кожної використаної утиліти і порядок виконання процедур захисту системи.

Лабораторна робота № 13.

Тема: Захист ПК від деструктивних дій за допомогою Shadow Defender

Мета: Набуття компетенції досліджувати, проектувати та реалізовувати апаратне та програмне забезпечення, оптимізовувати обчислювальні алгоритми та принципові електронні схеми спеціалізованих інформаційних систем.

Одна з найкращих на даний момент систем захисту ПК - це програмне забезпечення **Shadow Defender**. Ні один антивірус не здатен так захистити систему [1].

Суть програми полягає в тому, щоб захистити ПК від будь-яких шкідливих дій і небажаних змін як окремо взятої програми, так і всієї операційної системи в цілому. Shadow Defender після запуску створює динамічну копію вибраних користувачем папок та файлів, жорстких дисків, після чого будь-які зміни в системі не зачіплять фізичний зміст об'єктів, що захищаються, так як всі зміни будуть відбуватися в тіньовій

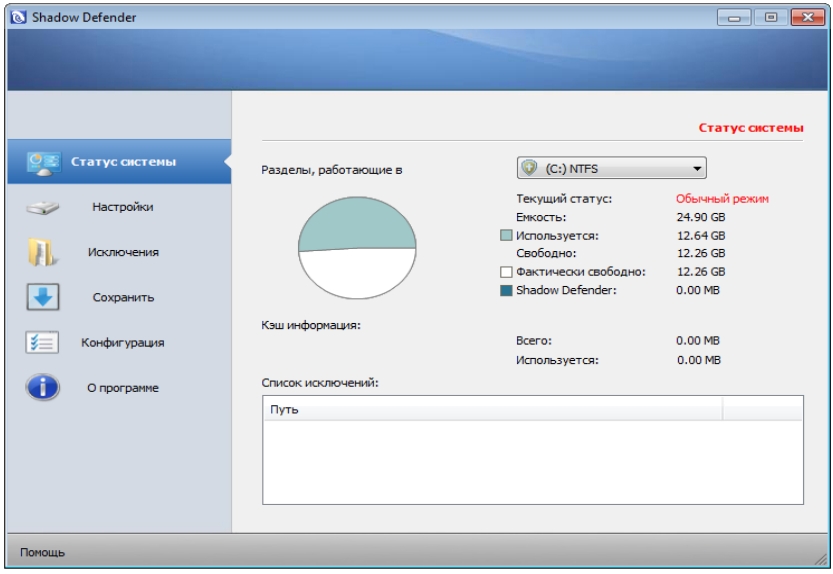


Рис.1. Головне вікно програми Shadow Defender.

копії. В настроюваннях Shadow Defender можна створити папки виключення. Наприклад, ви поставили весь розділ в захищений режим, а вам потрібно, щоб зміни в браузері зберіглись, тоді вам просто треба знайти папку збереження історії та інших файлів і відмітити її. Можна помітити поштові програми, програми для спілкування і так далі. Опис процедури встановлення та використання програми наведено в [2].

Дана програма дозволяє відкотити систему до потрібного стану і таким чином скасувати внесені несанкціоновані зміни.

Меню головного вікна програми містить наступні пункти:

1. System Status – видає на екран інформацію про загальну ємність, занятий та вільний простір системного диску.
2. Mode Setting – містить інформацію про всі жорсткі диски в системі: файлові системи, ємність та вільний простір кожного тому.
3. File Exclusion List – перелік файлів і папок, що мають бути виключені з приховано захищеного тому.
4. Registry Exclution List – список виключень з реєстру, що мають бути виключені від захисту.
5. Запустити програму і відмітити ті диски, що мають працювати в захищеному режимі, наприклад С: Натиснути «Enter Shadow Mode» і вибирається час, коли з нього треба вийти. Вибравши першу опцію, можна буде перезавантажувати ПК і залишатись в захищеному режимі. Вийти з нього можна тільки при натисканні кнопки «Відключити весь захист».

Друга опція дозволяє автоматично виходити із захищеного режиму при перезавантаженні. Тепер можна робити з диском С все, що завгодно, а при перезавантаженні система буде знаходитись в тому режимі, в якому вона була до натискання кнопки «Захищений режим». Провести маніпуляції з інформацією на диску: дещо добавити, дещо видалити,… Після перезавантаження системи все відновлюється в початковий стан.

Існує багато варіантів використання Shadow Defender.

Можна встановлювати драйвери пристроїв в захищеному режимі, потім експортувати їх у Tvitter а після перезавантаження імпортувати чисті експортовані драйвери. Також можна виконувати налаштування периферії через фірмові доданки. Зайти в захищений режим.

Встановити потрібний доданок, налаштувати все як треба, а після перезавантаження ніяких надлишкових програм не буде.

Також можна тестувати встановлювані додатки. Якщо програма не сподобалась, або просто виявилась не потрібною, виконується перезавантаження і програми як не було. Це значно корисніше, замість пробної інсталяції так як не залишається сміття та слідів в реєстрі.

Shadow Defender корисний для тих, хто турбується про свою безпеку. Захищений режим пригодиться при відкритті файлів або програм з неперевірених джерел, або для запуску доданків з неперевірених джерел. Така система дуже корисна при проведенні експериментів над системою без остраху виведення її з ладу

Порядок виконання роботи

1. Завантажити програму shadowdefender і запустити на виконання.
2. Провести експеримент з шифрування розділу жорсткого диску з наступним зняттям шифру.
3. Висловити власне розуміння програми та принципів роботи з нею.

Вміст звіту

1) Тема, мета роботи.
2) Вікно з переліком файлів та розділів диску, що були зашифрованими і відновленими.
3) Висновки по роботі.

Лабораторнра робота № 14.

Тема: Захист даних за допомогою TrueCrypt

Мета: Набуття компетенції досліджувати, проектувати та реалізовувати апаратне та програмне забезпечення, оптимізовувати обчислювальні алгоритми та принципові електронні схеми спеціалізованих інформаційних систем.

TrueCrypt був випущений у 2004 році на основі програмного забезпечення E4M (шифрування мас). Його розробку було припинено 28 травня 2014 року, але його вихідний код досі доступний для використання. TrueCrypt – це безкоштовне програмне забезпечення для шифрування дисків з відкритим вихідним кодом, доступне для

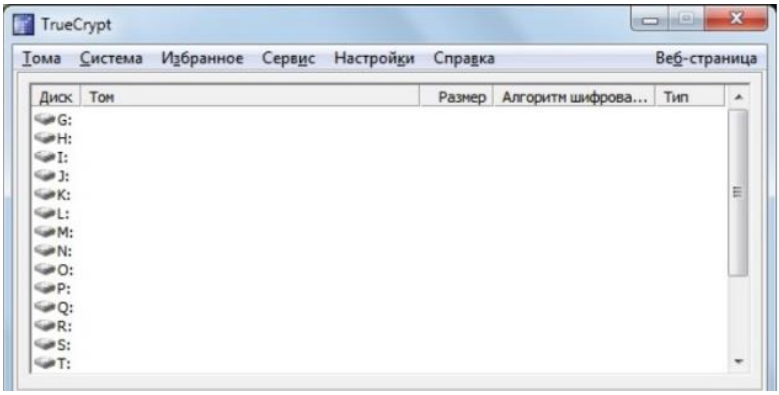
багатьох операційних систем. TrueCrypt надає користувачам шифрування/дешифрування в реальному часі, розпаралелювання та конвеєрну обробку для читання/запису до розділів так само швидко, як незашифровані розділи, а також правдоподібне заперечення через приховані томи та приховані операційні системи, щоб приховати дані користувача, навіть якщо він/вона змушений розкрити свій пароль. Іншими словами, це безкоштовна утиліта для OTFE (шифрування на льоту). Використовується для створення віртуально зашифрованого диска всередині файлу, шифрування частини диска або навіть усього.

На додаток до створення зашифрованих віртуальних дисків, TrueCrypt також дозволяв користувачам шифрувати цілі системні розділи або навіть цілі жорсткі диски. Це означало, що користувачі могли захистити всю свою систему, включаючи операційну систему та всі файли, за допомогою одного пароля. TrueCrypt здобув репутацію високонадійного інструменту шифрування, і він широко використовувався окремими особами, компаніями та навіть урядами в усьому світі. Однак у 2014 році розробники раптово закрили проект, пославшись на проблеми безпеки та попередивши користувачів перейти на альтернативне програмне забезпечення для шифрування.

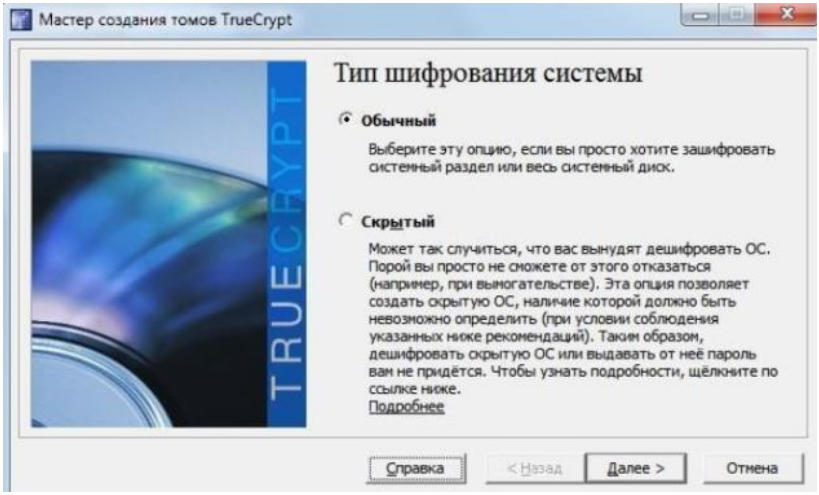
Незважаючи на припинення роботи, TrueCrypt залишається популярним інструментом серед багатьох користувачів, які продовжують використовувати його для розширених функцій шифрування.

Інструкція по встановленню

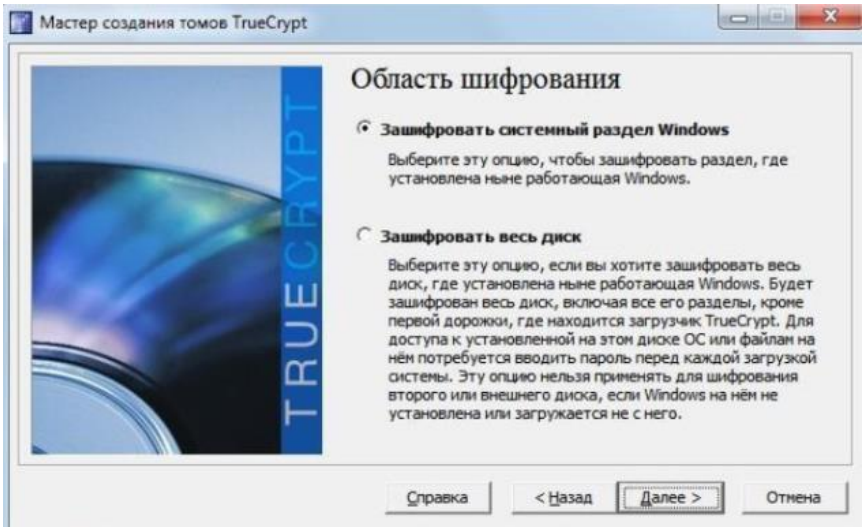
1) Запустити TrueCrypt. Рекомендується використовувати версію 7.1a як найбільш стабільну та безпечну.



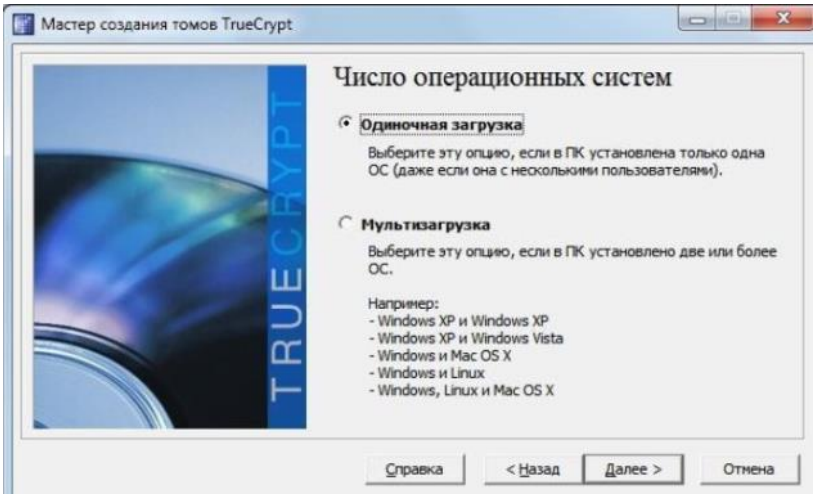
2) Зайти у вкладку Система головного вікна TrueCrypt і вибрати підпункт зашифрувати системний розділ. Вибираємо пункт Звичайний.



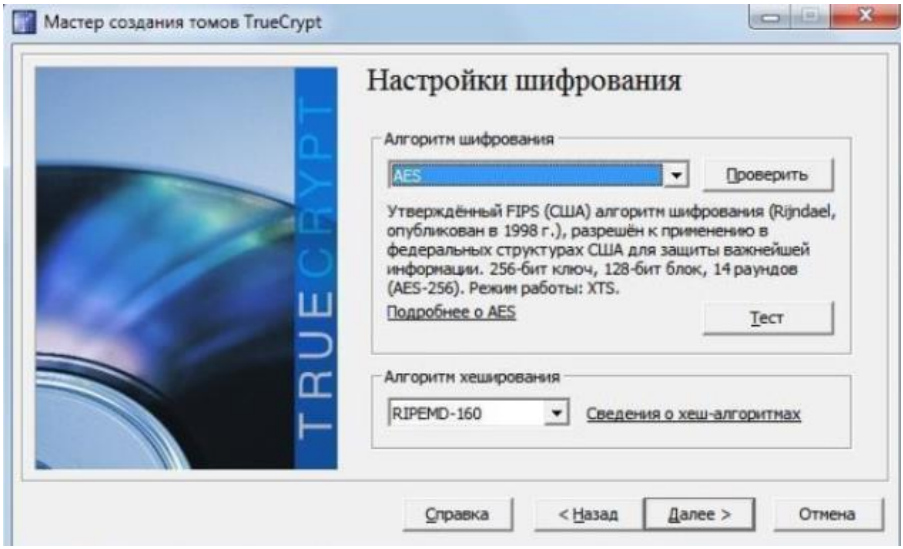
3) У наступному вікні бачимо два пункти. Зашифрувати системний розділ – зашифрує лише системний розділ. Зашифрувати весь диск – зашифрує всі розділи Вашого жорсткого диску. За будь-якого з пунктів буде створено спеціальну завантажувальну область TrueCrypt. Який пункт вам більше підходить, той і вибирайте.



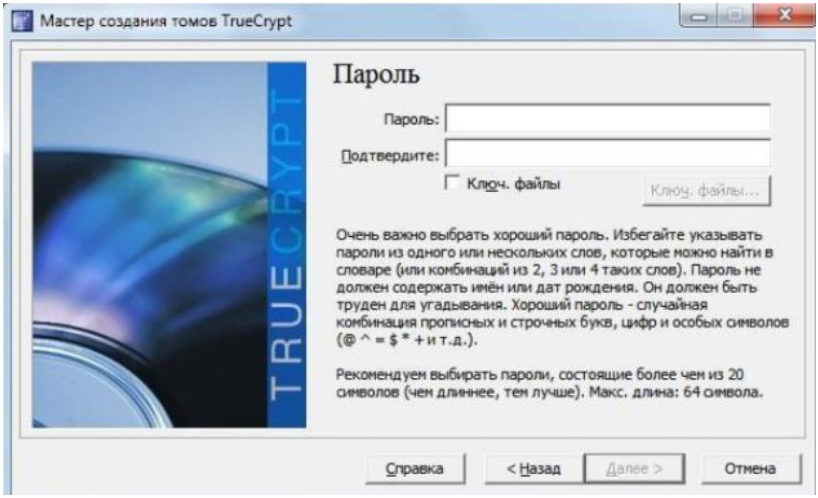
4) Якщо у Вас на комп'ютері лише одна операційна система, вибирайте перший пункт. Якщо у Вас їх декілька, вибирайте другий пункт.



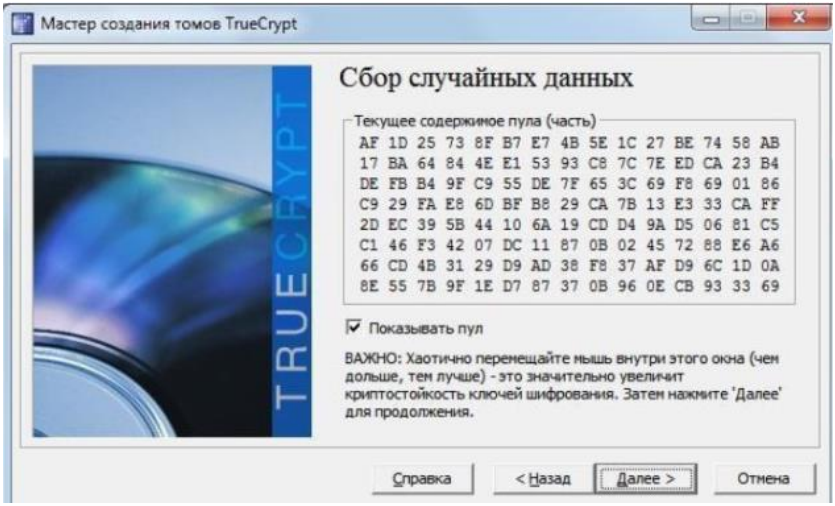
5) На цьому етапі можна вибрати алгоритм шифрування. Рекомендується вибрати AES-Twofish-Serpent і натиснути Далі.



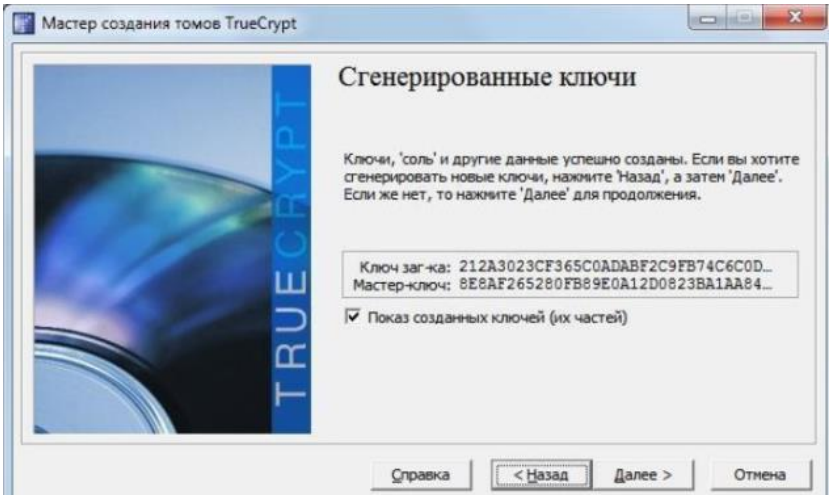
6) Тепер потрібно вигадати складний пароль, що задовольняє вимогам програми, інакше надійний рівень захисту не гарантується. Найкраще скористатися генераторами паролів, і згенерувати пароль відповідно до вимог, зокрема вкрай важлива кількість символів.



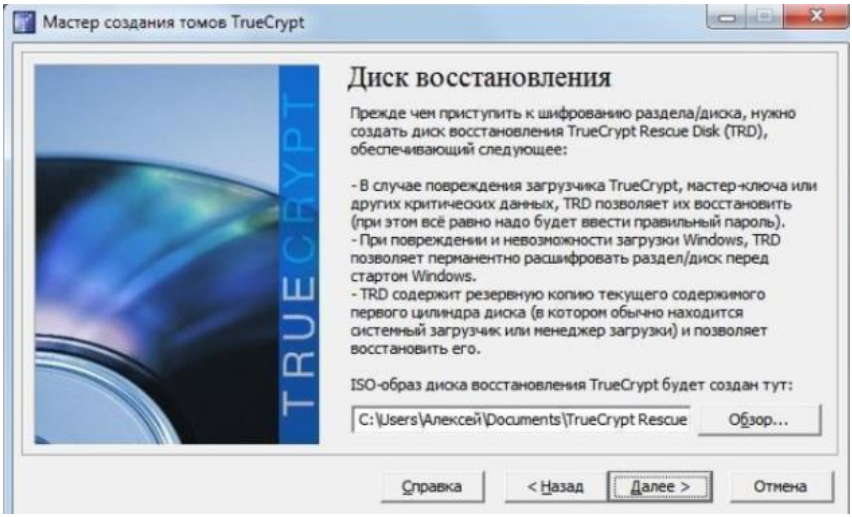
7) Далі слід рухати мишею в квадраті, чим довше, тим краще, щоб рандомізувати значення, що генеруються. Потім натискаємо Далі.



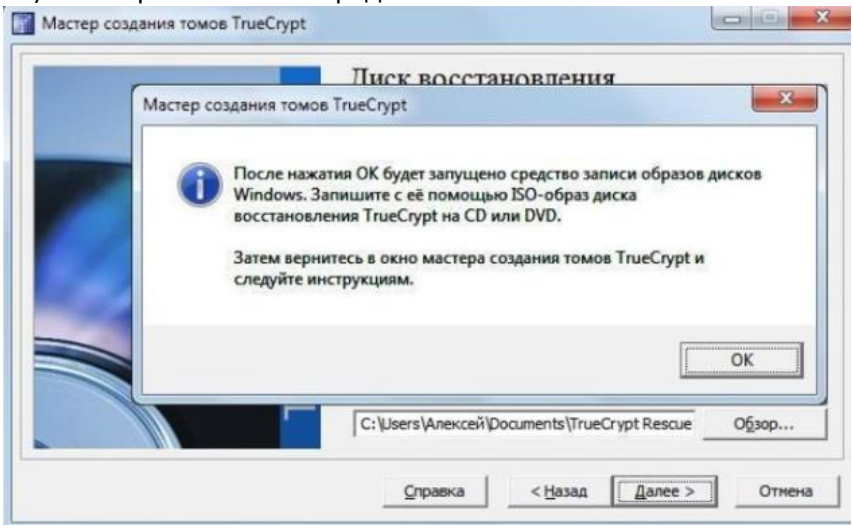
8) Далі слід рухати мишею в квадраті, чим довше, тим краще, щоб рандомізувати значення, що генеруються. Потім натискаємо Далі.



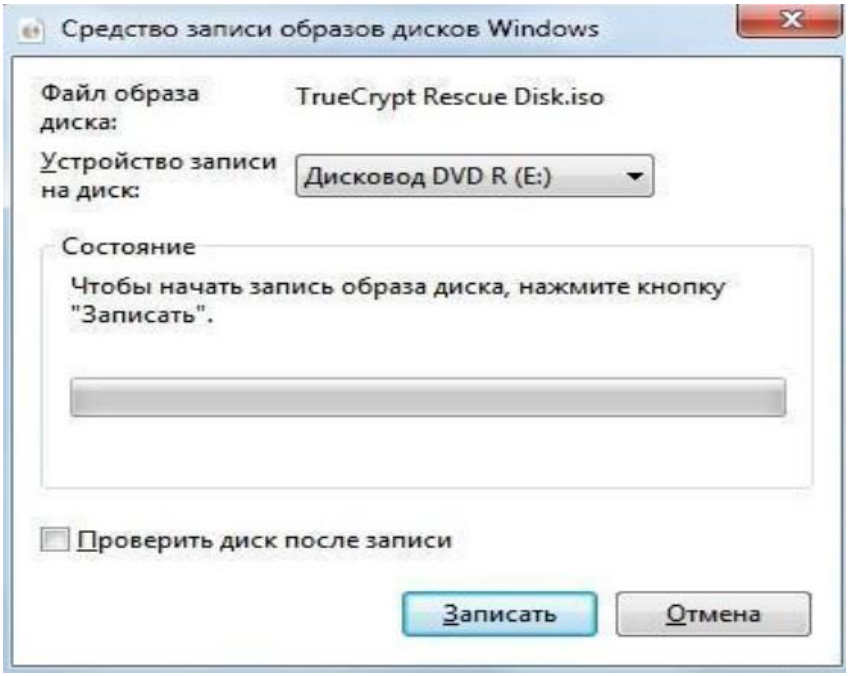
9) Далі створюється образ диска відновлення TrueCrypt. Необхідно вказати, де він зберігатиметься. Створити і далі записати його на диск необхідно, тому що інакше Ви не зможете перейти безпосередньо до процесу шифрування даних.



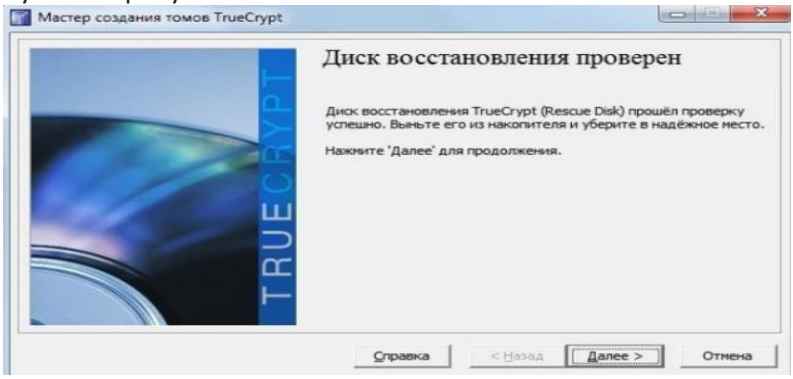
10) Після прочитання попередження натискаємо ОК.



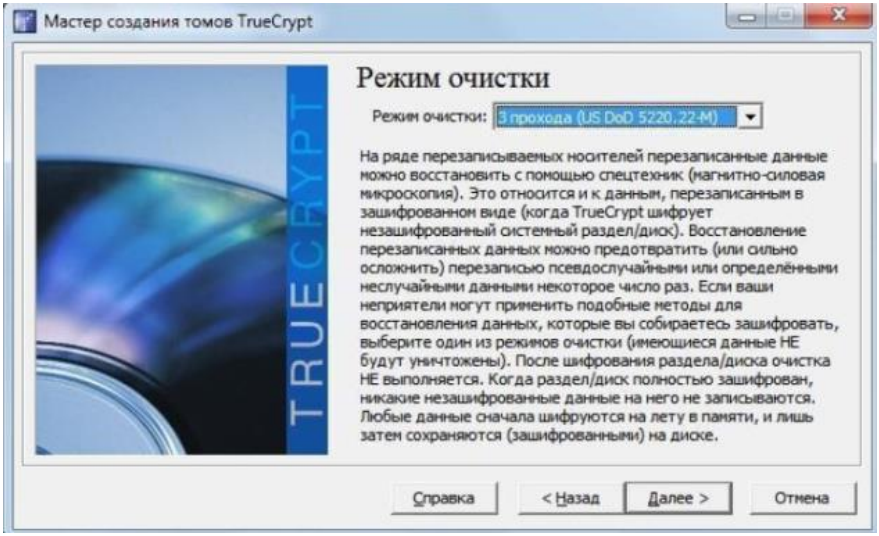
11) Далі, як і було сказано, відкриється засіб запису образів дисків. Обов'язково запишіть цей образ на диск – у разі помилки у завантажувальному записі, він врятує ситуацію. Відповідно для запису достатньо вставити CD-диск і натиснути «записати».



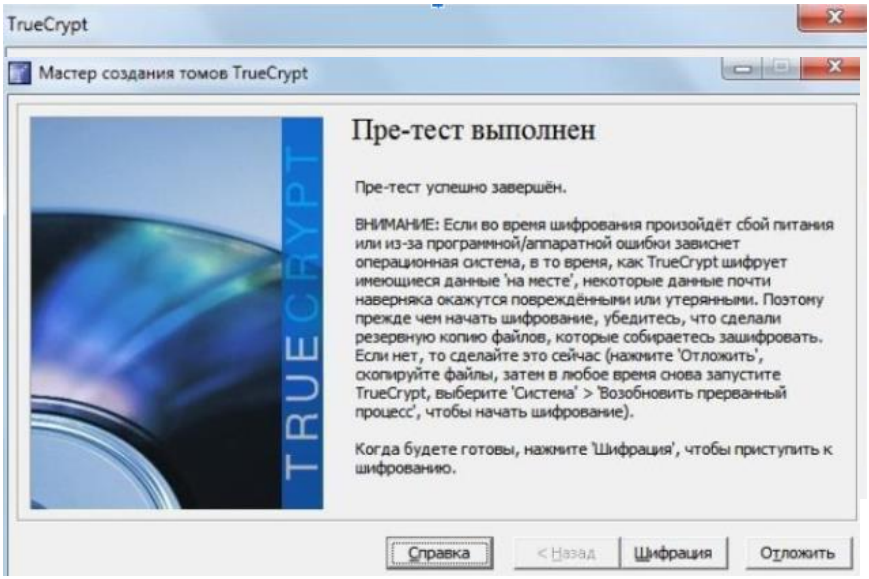
12. Якщо ви вже записали диск, вставте його в дисковод і натисніть. Диск буде перевірено на наявність помилок. Якщо диск записаний без помилок, ви побачите таке вікно. Натисніть «Записать». Якщо диск був записаний з помилками, його потрібно записувати знову і знову, щоб перевірити диск, оскільки без цього ви не зможете перейти до наступного кроку.



13) Далі потрібно вибрати режим очищення. Якщо у Вас є інформація, яка може скласти хоч якусь цінність, то вибираємо, як мінімум, 3 проходи, але слід врахувати, що процес шифрування триватиме в кілька разів довше. Після того, як Ви зробили вибір, натискаємо Далі.

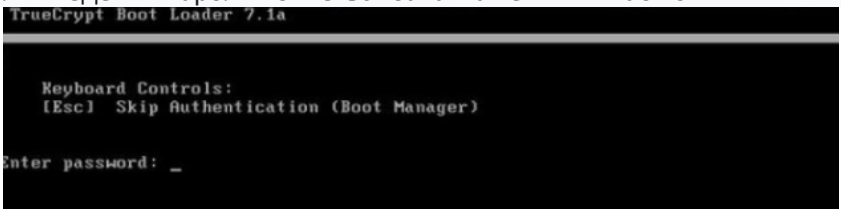


14) Далі програма пропонує перевірити, чи завантажувач працює коректно. Головне не забути пароль, тому що його зараз доведеться ввести. Натискаємо Тест.



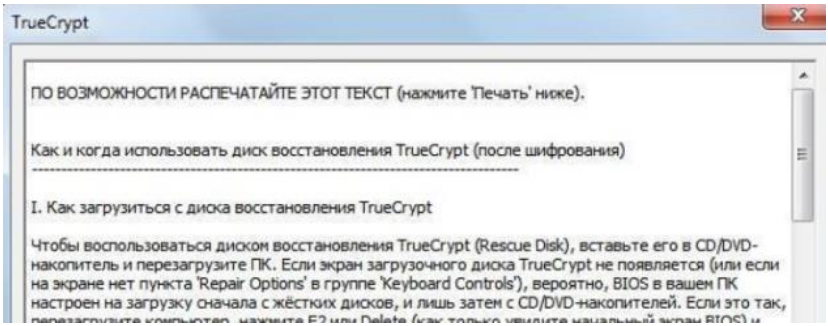
15) Далі пропонується надрукувати текстову довідку на тему проблем, які можуть виникнути під час тестування. Важливо пам’ятати пароль, і у разі чого скористатися диском відновлення TrueCrypt. Натискаємо Ок.

16) Завантажувач виглядатиме так, як показано на малюнку нижче. Після введення пароля почнеться завантаження Windows.

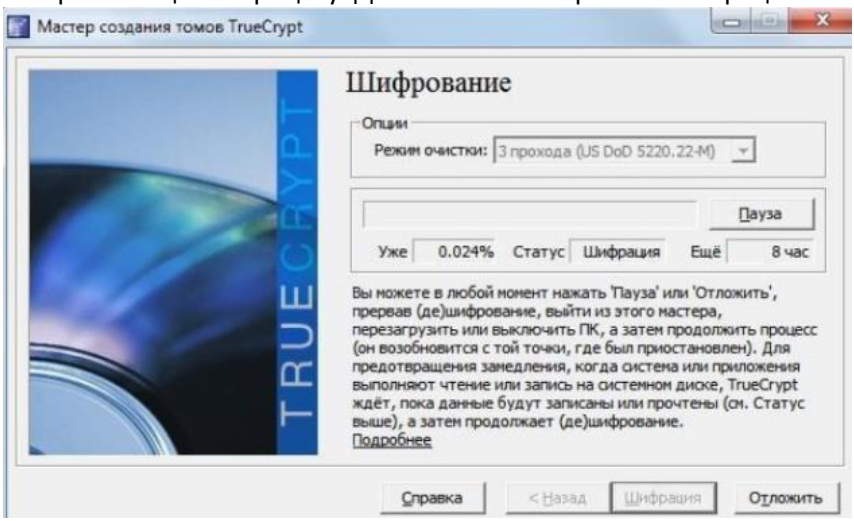


17) Тест пройдено успішно, можна розпочинати безпосередньо шифрування. Натискаємо кнопку “Шифрація”.

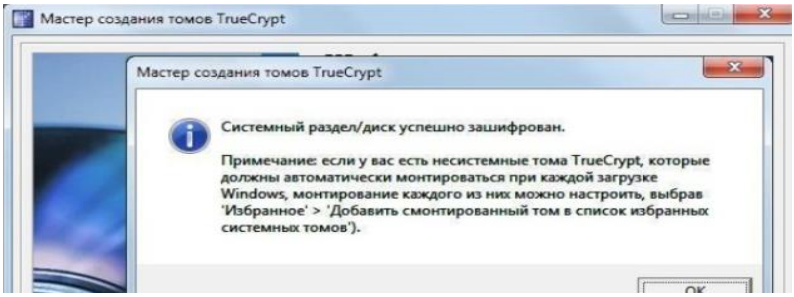
18) Далі знову пропонується роздрукувати довідку. Головне не відключати комп’ютер та не переривати роботу програми. Якщо ви шифруєте ноутбук, рекомендується підключити його до розетки, а також відключити перехід у режим сну при простої. Натискаємо ОК.



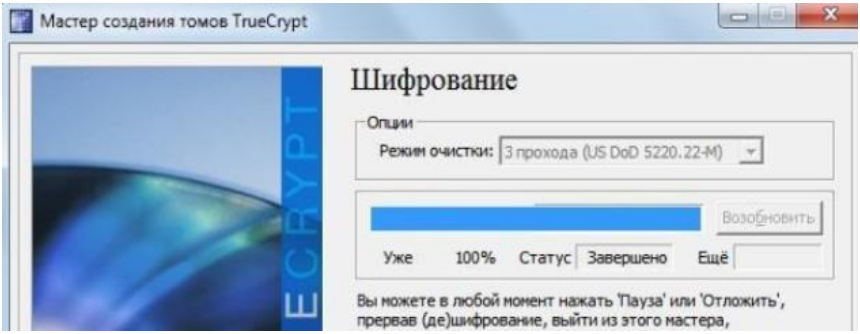
19) Безпосередньо процес шифрування. Будьте готові довго чекати на завершення цього процесу. Дочекайтеся завершення операції.



20) Після завершення процесу шифрування з’явиться таке повідомлення. Натискаємо ОК.



21) Натискаємо «готово».



Тепер щоразу під час завантаження системи Вам необхідно буде вводити пароль. Це убезпечить Вас від несанкціонованого доступу до інформації, що зберігається на вашому комп'ютері.

Порядок виконання роботи

1. Скачати програму truecrypt з наведеного нижче сайту.
2. Встановити програму у відповідності до рекомендацій.
3. Вибрати розділ, або каталог для проведення експериментів з шифрування даних.
4. Виконати рекомендований процес шифрування. Пересвідчитись в працездатності програмного забезпечення.
5. Зробити та оформити звіт.

Вміст звіту

1. Тема та мета роботи.
2. Порядок виконання роботи.
3. Висновки про доцільність використання програми і тривалість шифрування.

Лабораторна робота №15

Тема: Захист даних за допомогою VeraCrypt

Мета. Набуття здатності досліджувати, проектувати та реалізовувати апаратне та програмне забезпечення, оптимізовувати обчислювальні алгоритми та принципові електронні схеми спеціалізованих інформаційних систем.

VeraCrypt – це програмне забезпечен6ня, що використовується для шифрування «на льоту». VeraCrypt безоплатний і відкритий проект, що

починається з 2013 року в якості ворка True Cript. Запущений і по даний час підтримується Mounir Idrassi, засновницею компанії IDRIX після того, як 28 травня 2014 року було оголошено про припинення підтримки програми TrueCrypt.

За твердженнями розробників, у VeraCrypt реалізовано ряд вдосконалень в області безпеки порівняно з True Cript.

В той час, як True Cript використовує 1000 ітерацій при генерації ключа, яким шифрується системний розділ при використанні алгоритма PBKDF2-RIPEMD-160, VeraCrypt використровує 327 661 ітерацію. Для стандартних розділів на диску, що шифруються і файлових контейнерів VeraCrypt використовує 655 331 ітерацію для хеш-функції RIPEMD-160 та 500 000 ітерацій для SHA-2 и Whirlpool. Це суттєво сповільнює VeraCrypt при відкриванні зашифрованих розділів диску при їх монтуванні, але робить його не менше, чим в 10 і не більше, чим в 300 раз більш стійким до атак прямим перебором.

У VeraCrypt виправлений недолік початкового завантажувача для Windows. Для режима завантаження із зашифрованого розділу добавлена підтримка алгоритму SHA-256 та виправлені проблеми з нестабільністю ShellExecute для Windows.

Для Linux і macOS добавлена підтримка дисків з секторами більше 512 байт. Для Linux реалізована підтримка розділів, що відформатовані під NTFS.

Вказані вдосконалення привели до несумісності з форматом розділів TrueCrypt. Розробники VeraCrypt вважають старий формат TrueCrypt занадто уразливим для потенціальної атаки АНБ і відмовились від нього. Це головна відмінність між VeraCrypt і конкуруючим проектом TrueCrypt — CipherShed, який продовжує підтримувати старий формат. Починаючи з з версії 1.0f, VeraCrypt може відкривати і перетворювати в свій формат розділи, що відформатовані у форматі TrueCrypt [6], [7].

17 серпня 2016 року у версію 1.18a добавлена можливість шифрування дискових розділів, шо форматовані у форматі GPT[8].

VeraCrypt – безкоштовна крос-платформена програма з відкритим кодом. Можна завантажити версиії VeraCrypt для Windows, macOS та Linux з [офіційного сайта розробника](). В якості прикладу

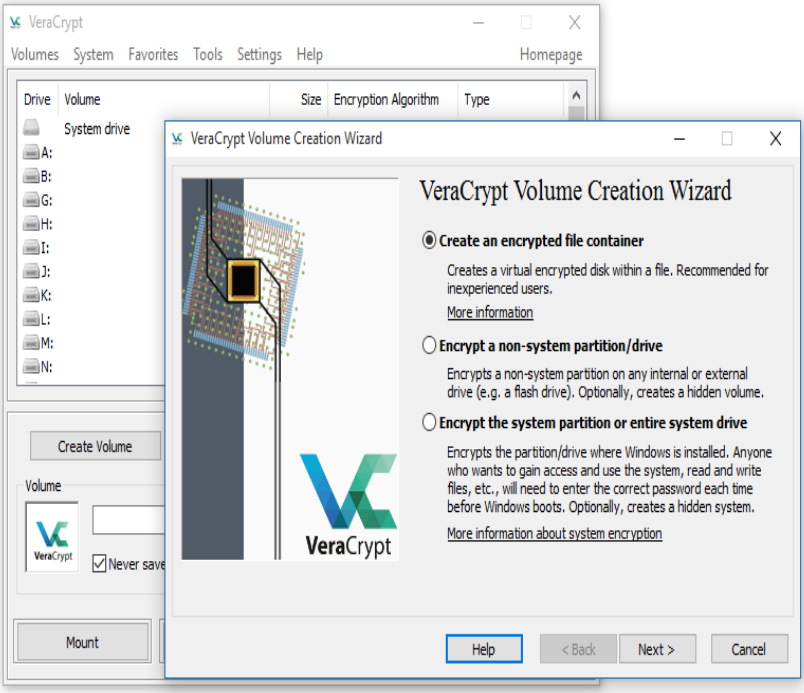


Рис.1. Головне вікно програми VeraCrypt.

використовується версія для Windows.

1. Завантажити дистрибутив VeraCrypt (файл .exe) с офіційного сайта на свій ПК [8]. Якщо бажаєте встановити VeraCrypt на комп'ютер як звичайну програму, вибирайте самий перший рядок в розділі «Windows». Посилання починається зі слів «VeraCrypt Setup» .

2. Запустити установку. Спочатку пропонується вибрати мову (Рис.2).

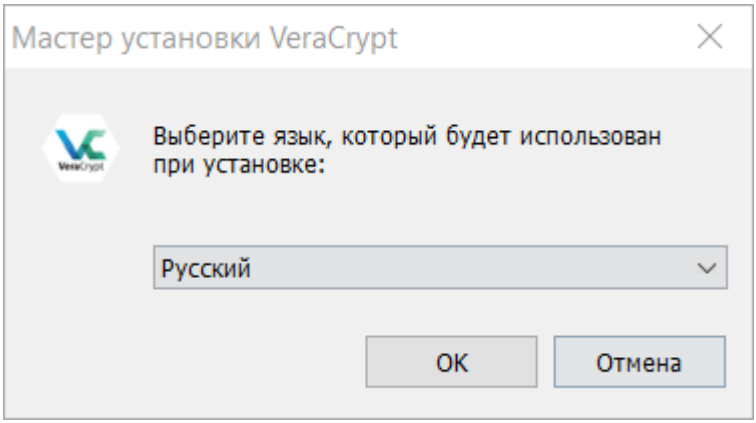


Рис.2. Вікно вибору мови інтерфейсу.

Вибирайте та натискайте «ОК».

3. Вікно з ліцензійною згодою [9].

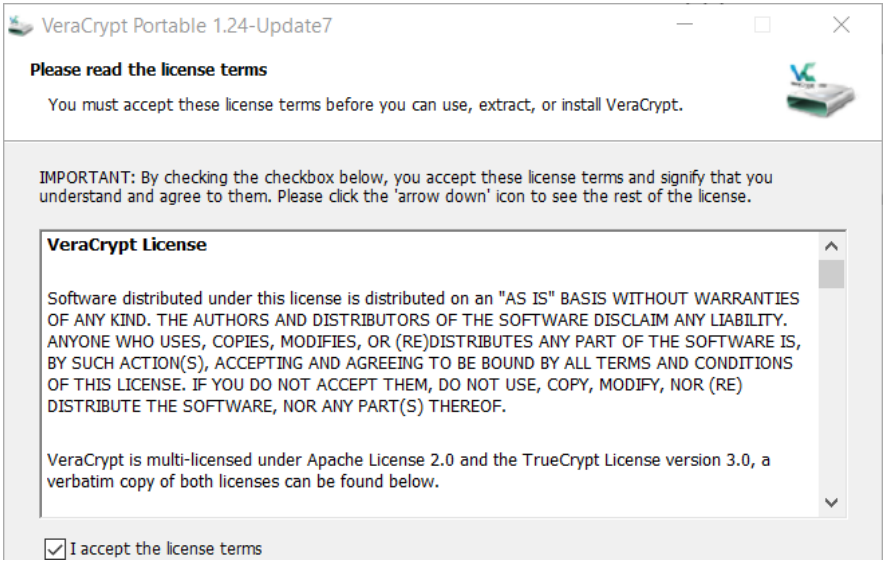


Рис.3. Погодження ліцензійної угоди

Поставити галочку в полі «I accept the license terms» і натиснути кнопку «Далее».

4. Куди розпакувати файли?

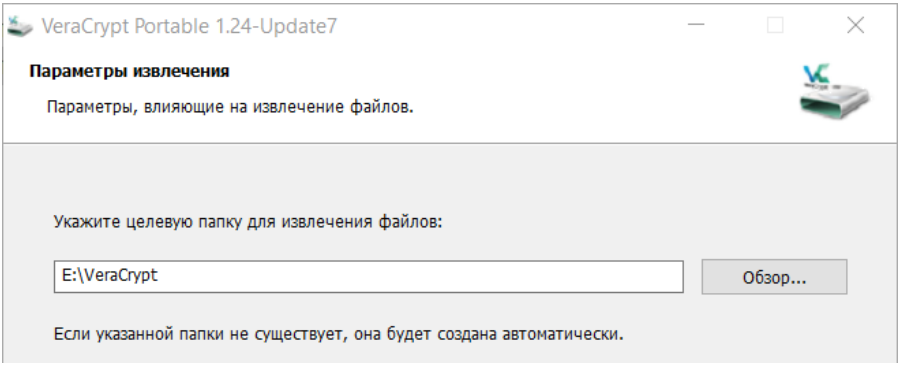


Рис.4. Вказати місце розташування програми.

Виберіть папку і натиснути «Извлечь». Коли все завершиться, VeraCrypt повідомить «Все файлы успешно извлечены в указанное целевое место». Натиснути кнопку «ОК».

6. Щоб стартувати программу, запустіть файл VeraCrypt.exe:

Цю нескладну процедуру доведеться робити щоразу для підключення вашого зашифрованого контейнера (тома). Щоб у вас у системі з'явився віртуальний шифрований диск. На практиці монтування зазвичай роблять щоранку на початку роботи. Набивши руку, ви досягнете автоматизму.

1. Запустіть VeraCrypt, якщо ви цього ще не зробили.

2. Виберіть у вікні букву для майбутнього віртуального диску– будь-яку, яка більше подобається.

3. Натисніть кнопку «Вибрати файл» у правій частині вікна.

4. Знайдіть файл-контейнер, створений вами раніше, на своєму комп'ютері. (Див. попередній розділ).

5. Натисніть кнопку «Змонтувати» у нижньому лівому куті вікна.

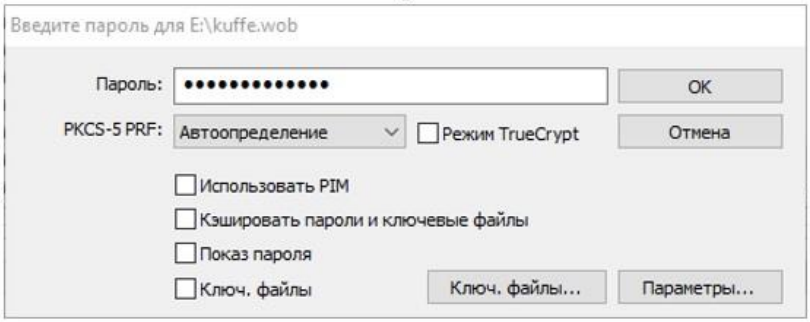


Рис.5.·Увести·пароль·до·шифрованого·диску.¶

6. У маленькому віконці, що відкрилося, введіть пароль. (Той, який вигадали у попередньому розділі, п.8). VeraCrypt може попросити трохи почекати.

Змонтований том в програмі VeraCrypt має такий вигляд:

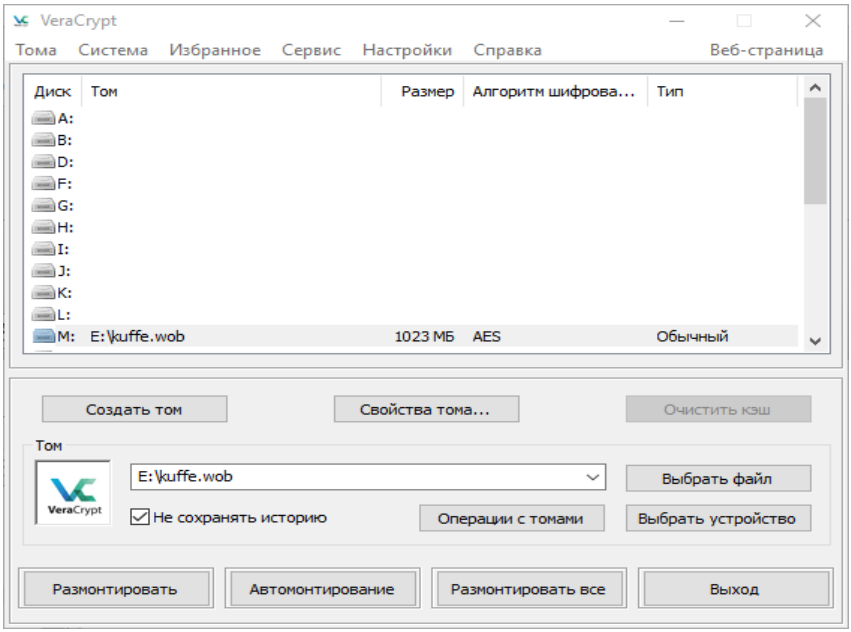


Рис.6. Вигляд змонтованого тому.

Якщо ви скористаєтеся файловим менеджером, можете переконатися: у системі з'явився новий диск (у нашому прикладі диск M:). Це віртуальний диск, з яким можна працювати так само, як із будь-яким іншим диском. При записі на цей диск файли автоматично шифруватимуться. При прочитанні або копіюванні з віртуального диска VeraCrypt на звичайний диск файли автоматично розшифровуватимуться.

Спробуйте скопіювати на віртуальний диск кілька файлів і переконайтеся, що все працює як треба.

Коли роботу завершено, потрібно розмонтувати том. Для цього достатньо натиснути кнопку «Розмонтувати» у нижньому лівому кутку програми. Не забувайте робити це наприкінці роботи. Не залишайте змонтованим, коли перезавантажуєте або вимикаєте комп'ютер.

Створення прихованого тома

Припустимо, обставини склалися невдало: вас змушують здати пароль від зашифрованого контейнера. (У законодавстві деяких країн є така норма). VeraCrypt дозволяє одночасно виконати вимоги закону та зберегти конфіденційність даних.

В іноземній літературі цей принцип називається plausible deniability (приблизний переклад – «легальна відмова»).

Ви створюєте у своєму контейнері друге секретне відділення. У нього немає «випираючих частин» або додаткових входів. Уявіть собі сейф, на вигляд звичайний, але з двома кодами.

Перший код відкриває стандартне відділення. Другий – таємне. За потреби можна пожертвувати першим кодом. Програма влаштована так, що жодної технічної можливості довести існування прихованого відділення (тому) немає.

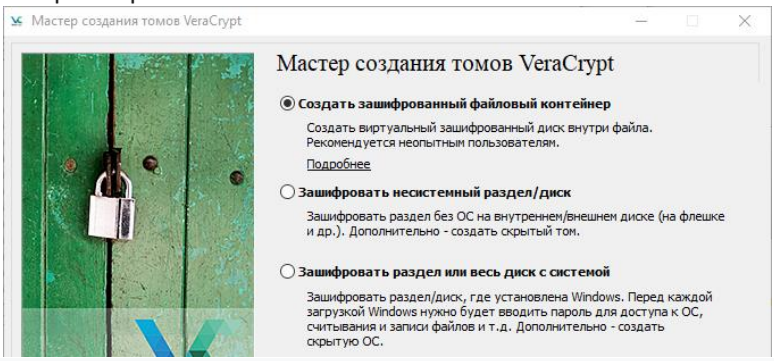
1. Запустіть VeraCrypt.

Користувачі Windows можут вибрати таку послідовність дій:

- створити прихований том у існуючому томі;
- створити новий звичайний том, та потім у середині нього приховане відділення.

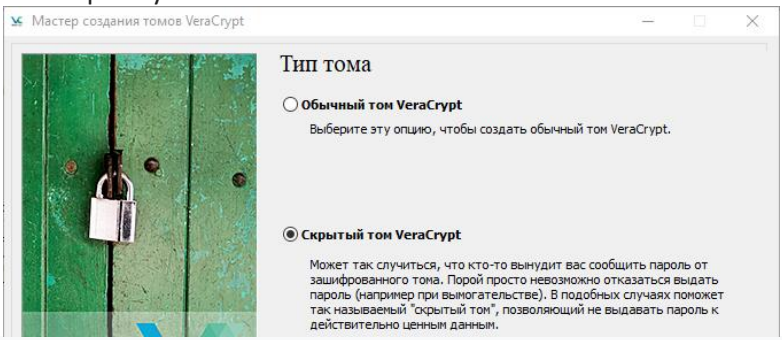
Для економії часу та місця показується перший варіант. Щоб його використати, спочатку потрібно розмонтувати відповідний том, якщо він у вас змонтований.

2. Натисніть кнопку «Створити том». Відкриється вже знайомий майстер створення томів.

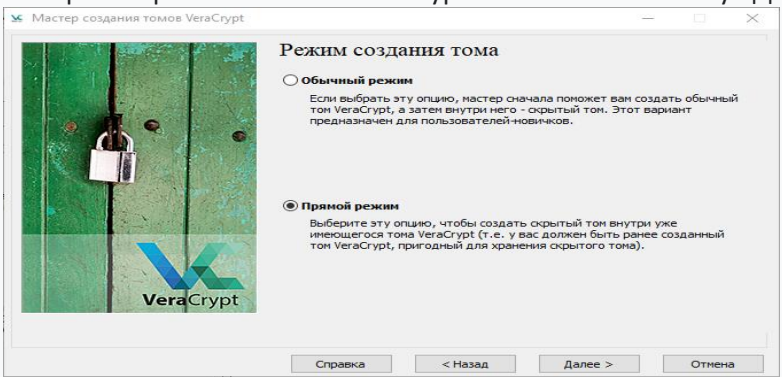


Виберіть «Створити зашифрований контейнер» (за замовчуванням) і натисніть кнопку «Далі».

3. Вибір типу тома.

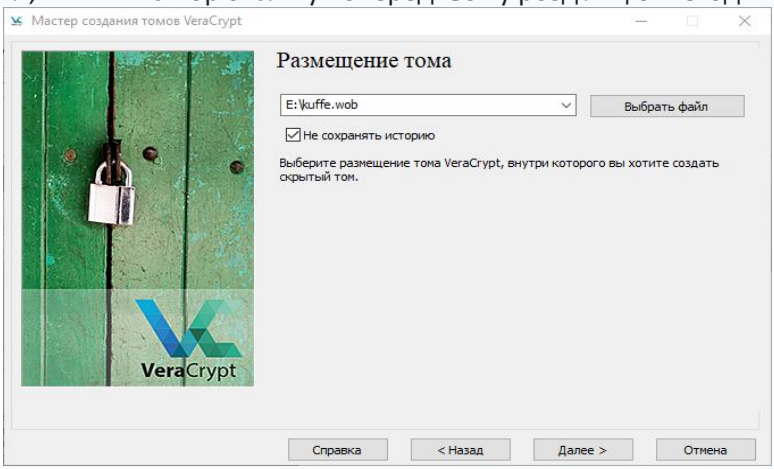


Виберіть «Прихований том VeraCrypt» та натисніть кнопку «Далі».



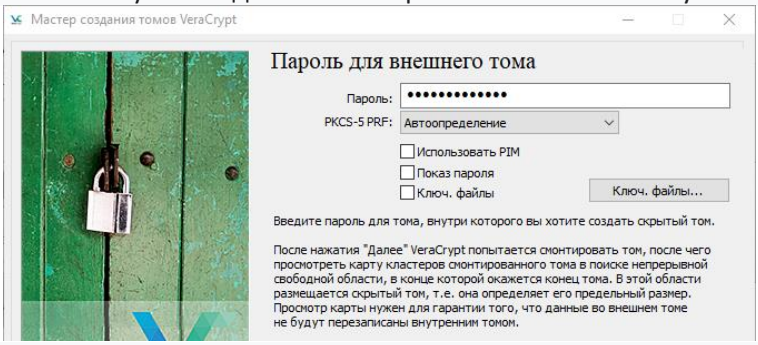
Ви вже маєте том VeraCrypt (Ви його створили в попередньому розділі). Тому вибираємо "Прямий режим". Натисніть кнопку "Далі".

5. Натисніть кнопку «Вибрати файл» і знайдіть на комп'ютері той файл, який ми створювали у попередньому розділі цієї методички.



Знайдіть на диску створений раніше файл-контейнер і натисніть кнопку «Далі».

6. Спочатку необхідно ввести пароль зовнішнього тому.



Введіть пароль зовнішнього тому та натисніть кнопку «Далі». VeraCrypt може попросити вас трохи почекати.

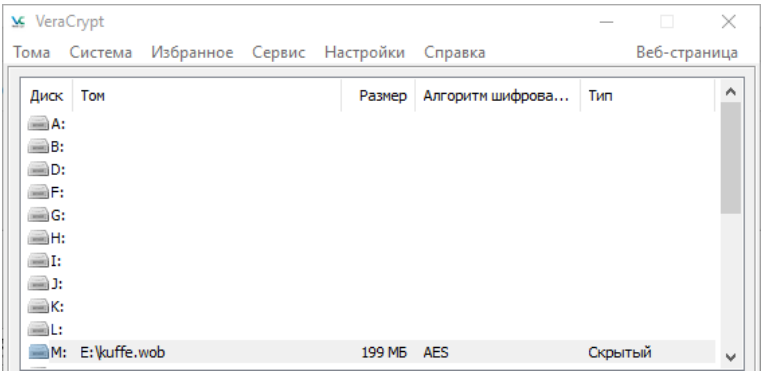
7. Пароль перевірений, VeraCrypt повідомляє, що все нормально можна продовжувати.

Натисніть «Далі».

8. Інші кроки повторюють відповідні кроки попереднього розділу. Єдина різниця в тому, що ви не можете встановити довільний об'єм для прихованого тому. Він буде обмежений обсягом зовнішнього тому.

Монтування схованого тому

Прихований том монтується так само, як зовнішній. Залежно від того, який пароль ви вкажете на вході, буде змонтовано зовнішній том або прихований том. Ось як виглядає змонтований прихований том в основному робочому вікні VeraCrypt:



Зверніть увагу на значення «Прихований» у стовпці «Тип».

Працювати з новим віртуальним диском прихованого тому можна так само, як і з віртуальним диском відкритого тома.

Якщо ви вдаєтеся до створення прихованого тому і збираєтеся зберігати там важливі файли, радимо також записати у зовнішній том якісь файли – важливі, але не конфіденційні. Якщо лиходій отримає

доступ до зовнішнього, він побачить, що той має вміст. Порожній зовнішній том виглядав би підозрілим.

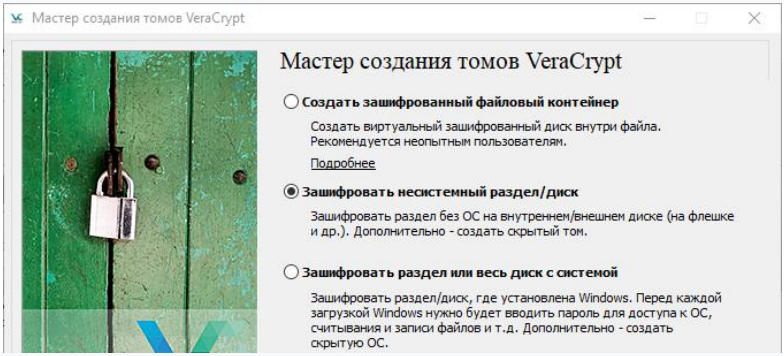
Шифрування диску

Іноді зручно зашифрувати цілий диск – наприклад, флешку. Зробити це не складніше, ніж файл-контейнер.

1 Підготуйте флешку. Якщо на флешці є важливі файли, зробіть резервну копію. Вставте флешку в порт USB комп'ютера. Операційна система розпізнає її як зовнішній носій і надасть їй букву.

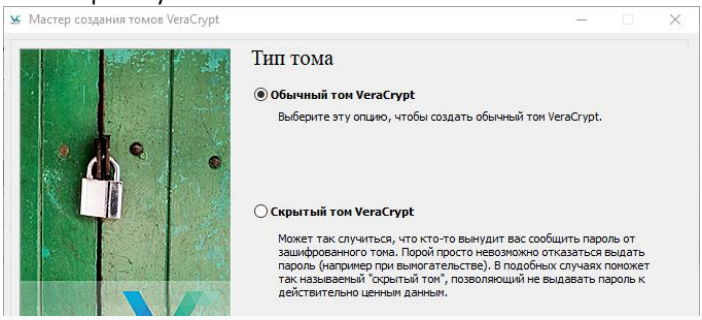
2. Запустіть VeraCrypt.

3. Натисніть кнопку «Створити том». З'явиться майстер створення томів.



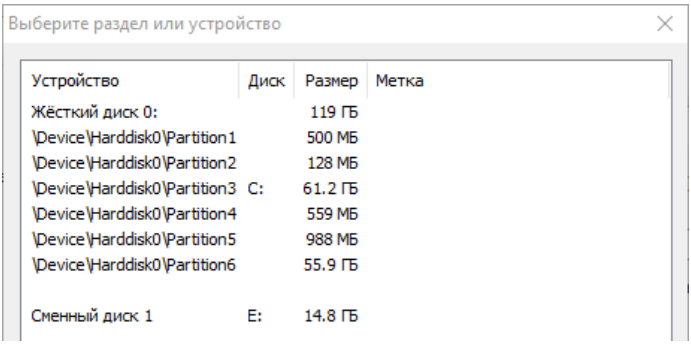
Виберіть «Зашифрувати несистемний розділ/диск». Натисніть кнопку "Далі"

4. Выбір типу тома.



Виберіть "Звичайний том VeraCrypt" і натисніть "Далі".

5. Тепер потрібно вибрати пристрій, який планується зашифрувати.



Натисніть кнопку «Вибрати пристрій». Відобразиться список доступних носіїв даних та розділів.

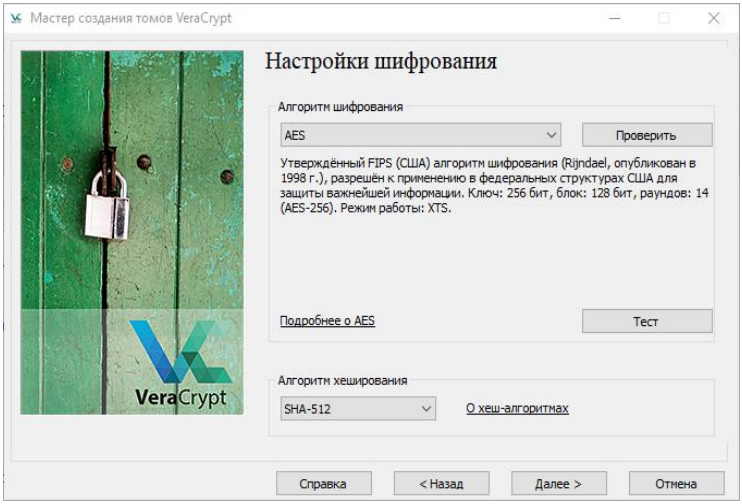
Виберіть розділ, який відповідає флешці. Будьте обережні, не переплутайте! Це особливо важливо, якщо на комп'ютері більше одного диска та/або до нього підключено два та більше зовнішніх носіїв. Переконайтеся, що це саме та флешка, яка потрібна. Натисніть кнопку "ОК", потім кнопку "Далі".

6. Виберіть режим створення тома.

• "Створити та відформатувати зашифрований том": флешка буде відформатована, а всі дані на ній втрачені. Швидкий спосіб.

• «Зашифрувати розділ на місці»: усі дані на флешці зберігаються. Повільний спосіб.

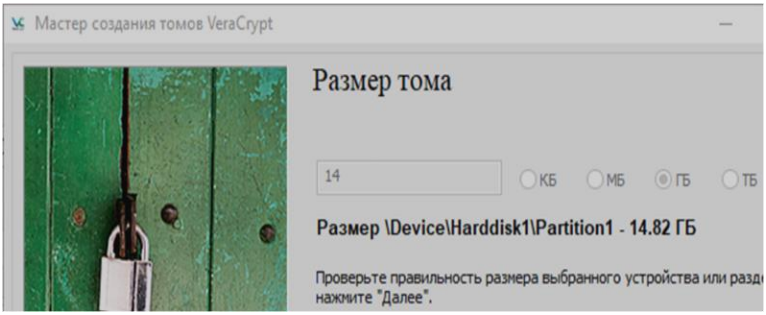
• Оскільки ми використовуємо чисту флешку (або принаймні зробили резервну копію - див. п.1), то вибираємо перший варіант. "Далі".



7. Знайомий етап – настроювання шифрування.

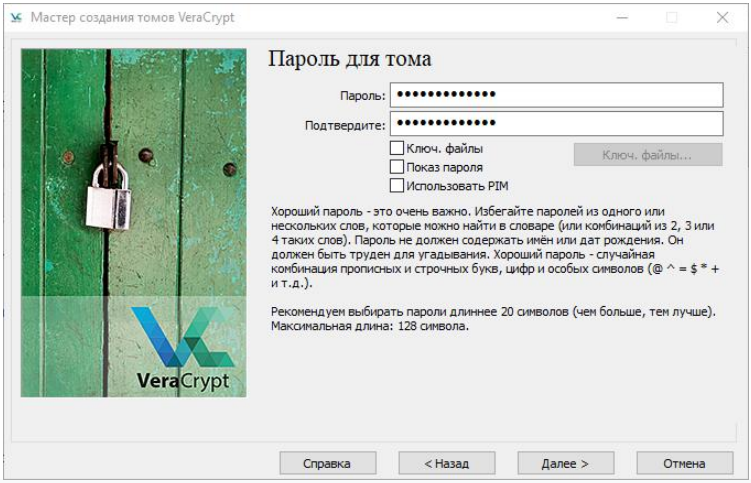
Можна залишити все як є і натиснути "Далі".

8. Розмір шифрованого диска



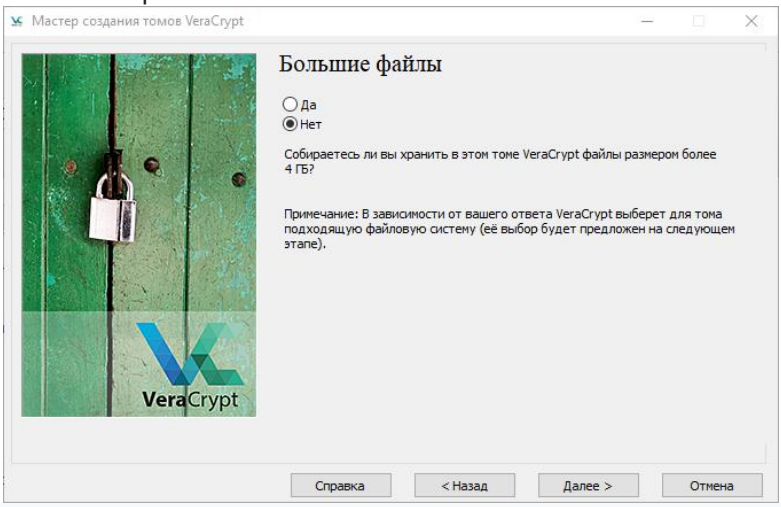
Тут нічого не вибрати та не змінити – вказаний обсяг флешки. Натисніть кнопку "Далі".

9. Вигадати пароль і ввести його в обидва поля.



Натисніть "Далі". Якщо VeraCrypt висловить невдоволення щодо довжини пароля, можна повернутися та розглянути більш довгий варіант – або натиснути кнопку «Так».

10. Великі файли.



Чи плануєте працювати з файлами більше 4 Гб? Питання пов'язане з обмеженням файлової системи FAT. Якщо залишити вибір за

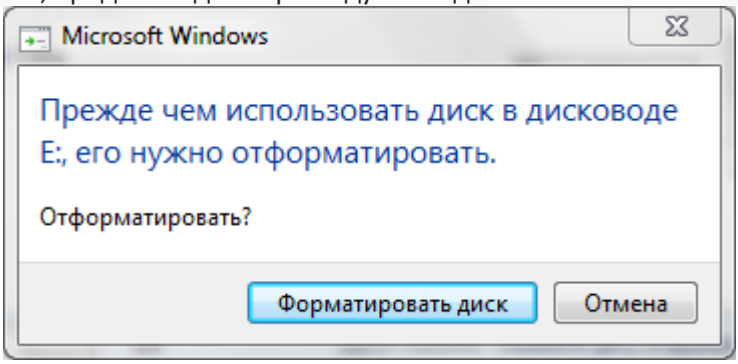
замовчуванням («Ні»), то під час підготовки флешки буде використана система FAT — з обмеженнями, але більш сумісна з різними пристроями. Якщо вибрати "Так", буде запропоновано систему exFAT. На наступному екрані можна скоригувати вибір. Натиснути "Далі".

11. Інші кроки аналогічні тим, які ви виконувались під час створення зашифрованого файлового контейнера

Робота з зашифрованим диском

Відкрити VeraCrypt. Підключити зашифровану флешку можна так само, як зашифрований файловий контейнер, див. вище. Єдина різниця: у головному вікні програми натиснути не кнопку "Вибрати файл", а кнопку "Вибрати пристрій".

Якщо вашу флешку придбає зловмисник і вставить її в USB-порт свого комп'ютера Windows, операційна система повідомить, що диск, ймовірно, не відформатовано. Навіть якщо на комп'ютері зловмисника встановлено VeraCrypt, зловмисник не дізнається, що флешка зашифрована. Він просто бачитиме «биту» флешку без будь-яких даних, придатних для перегляду або відновлення.

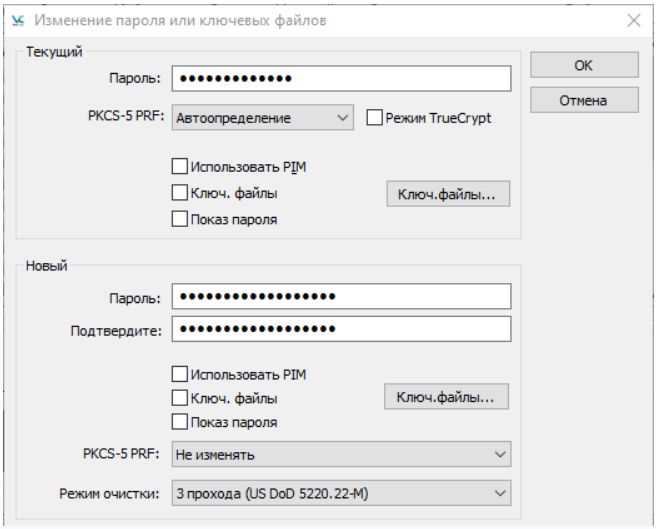


Заміна пароля

1. Запустіть VeraCrypt.

2. Натисніть кнопку «Вибрати файл» або «Вибрати пристрій» у правій частині вікна та виберіть файловий контейнер або зашифрований диск.

3. У меню «Тома» (перший пункт головного меню VeraCrypt) виберіть «Змінити пароль тома…».



У вікні «Зміна пароля або ключових файлів» введіть поточний пароль (вгорі) та двічі – новий пароль (нижче). Натисніть кнопку "ОК".

4. Завдання учбово-дослідних робіт.

Тема 11. Оцінити результати налаштування ОС засобами ***outbyte-pc-repair*.**

Тема 12. Оцінити результати перевірки ОЗП за допомогою **Memtest86.**

Тема 13. Дослідити процес відновлення даних за допомогою **recoverit.**

Тема 14. Оціінити результати відновлення даних засобами **hetman_partition_recovery.**

Тема 15. *Оцінити ефективність використання* ***Acronis Disk Director12.5.***

5. Питання та відповіді (Для самостійного опрацювання)

Питання. Якщо видалити програму VeraCrypt з комп'ютера, що станеться з зашифрованими файловими контейнерами?

Відповідь. З ними нічого не відбудеться. Всі папки та файли залишаться зашифрованими. Можете їх розшифрувати на любому комп'ютері, де встановлена VeraCrypt.

Питання. Чи всі типи файлів можна зашифрувати?

Відповідь. Так. Можете шифрувати будь-який файл: і текстовий документ, і електронну таблицю, і архів, і фотографію, і звуковий файл.

Питання. А програми?

Відповідь. Так, і програми. Ви можете тримати в зашифрованому контейнері цілий набір портативних програм, наприклад, текстовий редактор, переглядач фотографій, музикальний програвач, і т. п. Фактично, ви організовуєте власний захищений робочий простір.

Питання. Ящо комбінувати різні програми захисту даних, наприклад, VeraCrypt та KeePassXC?

Відповідь. Додатковий рівень захисту – непогана ідея. Базу паролей KeePassXC (як і саму програму KeePassXC) можна зберігати в захищеному контейнері VeraCrypt. Або, навпаки, пароль до контейнера або диску VeraCrypt – в базі KeePassXC.

Питання. Я забув пароль до файлового контейнера (диска). Чи можу як-небудь відновити пароль?

Відповідь. Ні.

Питання. Чи залишає VeraCrypt у файлі-контейнері свою «сигнатуру», яку-небудь інформацію, по якій можна здогадатись, що це – том VeraCrypt?

Відповідь. Ні, не залишає.

Питання. Якщо записати що-небудь в зашифрований контейнер, чи зміниться відповідним чином дата створення/зміни цього файлу-контейнера?

Відповідь. Дата залишається той, яка була при створенні файлу-контейнера.

Питання. Чому б не використовувати динамічні контейнери, котрі можуть змінювати розмір? Записав більше файлів – контейнер автоматично збільшився. Це так зручно?

Відповідь. Так, це зручно. Але якщо зловмисник має можливість спостерігати за змінами файлів на диску, він зможе помітити, що деякий файл постійно змінює свій розмір, і це здатне викликати додаткові підозри. Якщо вам потрібен більш ємкий контейнер, створіть новий, більшого об’єму, і перенесіть до нього дані звичайним копіюванням. Можна також скористатися утилітою VeraCrypt Expander, яка знаходиться в тій же папці, що і основні програмні компоненти VeraCrypt.

Використана література

1. Програмне забезпечення www.shadowdefender.com
2. Відеоогляд Shadow Defender https://www.youtube.com/watch?v=-PN2RmdIvoA
3. Безпечні експерименти над Windows! https://m.youtube.com/watch?v=pJTrzyUjnLo&pp=ygUvc2hhZG93IGRlZmVuZGVyINC60LDQuiDQv9C0LvRjNC30L7QstCw0YLRjNGB0Y8%3D
4. Огляд як користуватись програмою https://m.youtube.com/watch?v=TGjYWP92xB0&pp=ygUvc2hhZG93IGRlZmVuZGVyINC60LDQuiDQv9C-0LvRjNC30L7QstCw0YLRjNGB0Y8%3D
5. https://hackyourmom.com/pryvatnist/shyfruvannya-pk-iz-truecrypt/
6. Інструкція для початківців https://remontka.pro/truecrypt-manual-beginners/
7. TrueCrypt обзор программы или как пользоваться https://www.youtube.com/watch?v=HegsuuYmkvo
8. Встановлення та використання VeraCrypt https://www.youtube.com/watch?v=qm2Kmmksl_U
9. Встановлення та використання VeraCrypt https://www.youtube.com/watch?v=J0XrhT5fUbo
10. Як оптимізувати Widows 11 та прискорити роботу ПК у Windows 11 http://surl.li/nknqmd
11. Hetman Software: безпечне відновлення даних безкоштовно http://surl.li/azqujb