**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

# ПОЯСНЮВАЛЬНА ЗАПИСКА

**Дипломної роботи**

***магістра***
(назва освітньо-кваліфікаційного рівня)

**галузь знань** *12 Інформаційні технології*
(шифр і назва галузі знань)

**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)

**освітній рівень** ***магістр***
(назва освітнього рівня)

**кваліфікація**
(код і назва кваліфікації)

**на тему:** Методи підвищення ефективності захисту зовнішніх носіїв інформації від несанкціонованого доступу та модифікації

**Виконавець:** студент ІІ курсу, групи Кбм - 21

**Захарченко Євгеній Олександрович**
(підпис) (прізвище ім'я по-батькові)

| | **Прізвище, ініціали** | **Оцінка** | **Підпис** |
|---|---|---|---|
| **Керівник** | Наконечний В.С. | | |
| **Рецензент** | Сайко В. Г. | | |
| **Нормоконтроль** | Даков С.Ю | | |

**Київ 2022**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
“ ” 2022 р.

**ЗАВДАННЯ**
**на виконання дипломної роботи**

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**студенту** **КБм-21** **Захарченко Євгенія Олесандровича**
(група) (прізвище ім’я по-батькові)

**Тема дипломної роботи** Методи підвищення ефективності захисту зовнішніх носіїв інформації від несанкціонованого доступу та модифікації

## 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол № 5 від 29.10.2021р.

## 2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

| | |
|---|---|
| **Об’єкт дослідження** | Процес зберігання, обробки інформації на зовнішньому носії інформації та збереження властивостей інформації |
| **Предмет дослідження** | Методи забезпечення високого рівня властивостей безпеки інформації на компактному носії інформації |
| **Мета** | Розробка та опис принципу роботи зовнішнього носія інформації з можливістю забезпечення виконання основних властивостей інформації |
| **Вихідні дані для проведення роботи** | Аналітичні дані про засоби захисту від несанкціонованого доступу, характеристики сучасних накопичувачів. |

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

**Наукова новизна** створення методів роботи зовнішнього носія із захищеним віртуальним диском та можливістю забезпечення високого рівня безпеки.

**Практична цінність** розробка принципу роботи зовнішнього носія інформації

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

## 5. ЕТАПИ ПРОВЕДЕННЯ РОБОТИ

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.10.2021 – 05.11.2021 | *виконано* |
| 2 | Аналіз виконаної роботи дипломної роботи бакалаврату | 06.11.2021 – 17.02.2022 | *виконано* |
| 4 | Аналіз основних інструментів захисту даних на накопичвачі | 18.02.2022 - 14.03.2022 | *виконано* |
| 5 | Розгляд актуальних програмних засобів захисту | 15.03.2022 – 30.03.2022 | *виконано* |
| 6 | Розробка алгоритму роботи носія з віртуальним розділом | 31.03.2022 – 01.04.2022 | *виконано* |
| 7 | Розширення описаного методу до декількох варіантів використання | 02.04.2022 – 20.04.2022 | *виконано* |
| 8 | Аналіз розробленого методу | 21.04.2022 – 04.05.2022 | *виконано* |
| 9 | Оформлення пояснювальної записки | 05.05.2022 – 15.05.2022 | *виконано* |
| 10 | Підготовка до захисту дипломної роботи | 15.05.2022 – 19.05.2022 | *виконано* |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економіний ефект** Зниження збитків через викрадення конфіденційної інформації з зовнішніх носіїв

**Соціальний ефект** Покращення технологій забезпечення захисту зовнішніх носіїв інформації

## 7. ДОДАТКОВІ ВИМОГИ

_____

_____

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв
до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____
Термін подання дипломної роботи до ЕК _____

**УДК 004.056.5**

# РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Методи підвищення ефективності захисту зовнішніх носіїв інформації від несанкціонованого доступу та модифікації» складається зі вступу, основної частини, що містить 5 розділів, висновків і списку використаних джерел. Загальний обсяг роботи – 67 сторінок. Робота містить 12 рисунків, 4 таблиці. Список використаних джерел включає 31 джерело.

*Об'єкт дослідження* – процес зберігання, обробки інформації на зовнішньому носії інформації та збереження властивостей інформації.

*Мета роботи* – розробка та опис принципу роботи зовнішнього носія інформації з можливістю забезпечення виконання основних властивостей інформації.

*Предмет дослідження* – методи забезпечення високого рівня властивостей безпеки інформації на компактному носії інформації.

*Метод дослідження* – аналіз програмних засобів захисту інформації, порівння актуальних способів збереження інформації, моделювання роботи пристрою з віртуальним захищеним розділом.

В роботі проведено аналіз актуальних способів збереження інформації та програмні засоби її захисту, сучасні підходи розробки сукупності заходів для забезпечення безпеки інформації.

Розроблено принцип роботи зовнішнього носія інформації з захищеним віртуальним розділом та можливістю перевірки прав доступу до нього.

*Практичне значення роботи* полягає у створенні методу роботи зовнішнього носія з захищеним віртуальним диском та можливістю забезпечення виского рівня безпеки.

Результати здійснених у дипломній роботі досліджень можуть бути використані для зберігання та перенесення конфіденційної інформації.

*Ключові слова:* зовнішні носії інформації, віртуальний диск, конфіденційна інформація, розподілення доступу, непримітність, психологічна непривабливість.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ACE – Apacer Compression Explorer
AES – Advanced Encryption Standard
CD – Compact Disc
CD-R – Compact Disc-Recordable
CD-ROM – Compact Disc Read-Only Memory
CD-RW – Compact Disc-ReWritable
DVD – Digital Versatile Disc
EFS – Encrypting File System
exFAT – Extended FAT
FAT – File Allocation Table
HDD – Hard Disk Drive
MFT – Master File Table
NTFS – New Technology File System
SD – Secure Digital Memory Card
SSD – Solid-State Drive
TPM – Trusted Platform Module
Wi-fi – Wireless Fidelity
ВЗД – Віртуальний Захищений Диск
Гб – Гігабайт
Еб – Ексібібіт
ЗД – Загальний Диск
Кб – Кілобайт
ОС – Операційна Система

# ЗМІСТ

# ВСТУП

На сьогоднішній день Інтернет технології розвиваються дуже швидко. Ми використовуємо соціальні мережі для спілкування та передачі файлів. Все більше даних передаються за допомогою мережі Інтернет. Тому з’являється все більше методів злому, велика імовірність несанкціонованого використання персональних даних, інформації заради вигоди зловмисника. Через ресурси мережі інтернет, соціальні мережі зловмисники можуть підключитися до мобільного пристрою та викрасти персональні дані. Один телефон, залишений без паролю надає зловмиснику можливості здійснити придбання на значну суму, форматувати всі дані, включно з хмарного сховища і навіть знищити соціальне життя людини. Також все більше з'являються віруси та програми-шпигуни, що можуть приховано встановлюватися на комп’ютерах, збирати та модифікувати дані, а також використовувати ресурси персонального пристрою.

Таким чином, питання передачі та зберігання інформації становить одне з найголовніших актуальних питань безпеки людини та її персональних даних.

Метою дипломної роботи «Методи підвищення ефективності захисту зовнішніх носіїв інформації від несанкціонованого доступу та модифікації» є розробка та опис принципу роботи зовнішнього носія інформації з можливістю забезпечення виконання всіх властивостей інформації.

Задачі, що потребують вирішення:

- Провести аналітичний огляд актуальних способів збереження інформації (хмарні інструменти, зовнішні носії, їх види).
- Визначити найбезпечніший, найзручніший зовнішні носій інформації для розробки методу, способу, принципу захисту інформації.
- Проаналізувати актуальні способи, програми захисту інформації.
- На основі проаналізованих програм сформувати набір/складових для забезпечення захисту інформації на зовнішніх носіях.

● Розробити та описати систему заходів забезпечення високого рівня властивостей безпеки інформації на зовнішньому портативному носії.

● Проаналізувати результат розробки, знайти можливі недоліки.

Це процес зберігання, обробки інформації на зовнішньому носії інформації та збереження властивостей інформації

Методи забезпечення високого рівня властивостей безпеки інформації на компактному носії інформації.

У дипломній роботі використовувались такі методи дослідження як:

● Спостереження.

● Порівняння.

● Аналіз.

● Історичний метод.

● Абстрагування.

У дипломній роботі одержані наступні рішення та досягення:

● Удосконалено способи зберігання інформації на компактному пристрої.

● Розроблені методи забезпечення конфіденційності, цілісності та доступності на зовнішньому носії, який базується на віртуальному розподіленні пам’яті.

● Узагальнено засоби захисту інформації на носії даних.

● Розроблені правила надання доступу до прихованої області пам’яті з чутливою інформацією.

Практична цінність кваліфікаційної роботи полягає в:

Розробці методів, що базуються на використанні технології віртуального розподілення пам’яті на зовнішньому носії інформації.

Розробці способу забезпечення високого рівня конфіденційності, доступності та цілісності інформації на носії.

Розробці правил отримання доступу до віртуальної області пам’яті.

Матеріали дослідження даної роботи були апробовані на VIII Міжнародній науково-практичній конференції «Information Technology and Implementation

(Satellite)» 1 грудня 2021 року, її назва «Methods to increase the effectiveness of protection of external media from unauthorized access and modification».

# РОЗДІЛ 1
# ІНФОРМАЦІЯ. ВИБІР ЗОВНІШНЬОГО НОСІЯ ІНФОРМАЦІЇ

## *1.1 Терміни та визначення*

Ми живемо в епоху інформаційного суспільства, коли комп'ютери та телекомунікаційні системи використовуються у всіх сферах життєдіяльності людини та держави - від вирішення проблем національної безпеки, охорони здоров'я та управління транспортом до торгівлі і фінансів. Інформація відіграє важливу роль у кожному аспекті життя. Зараз як ніколи актуальне твердження «Хто володіє інформацією, той володіє світом». У кваліфікаційній магістерській роботі автор пропонує нові методи захисту інформації на зовнішньому носії та визначити основні складові зовнішнього носія з високим рівнем захищеності інорфмації на ньому. Проте спочатку потрібно чітко встановити поняття та їх визначення.

У законі України «Про інформацію» наведене таке тлумачення поняття інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1. Розділ 1, стаття 1]. Відомо, що інформація має властивості. Найважливішими, з практичної точки зору, властивостями інформації є цілісність, конфіденційність та доступність. Тому, метою кваліфікаційної роботи є — збереження цих властивостей. Пригадаємо їх визначення.

Конфіденційність інформації – властивість інформації, що характеризується унеможливленням її несанкціонованого розповсюдження, одержання чи ознайомлення з нею [1].

Цілісність інформації - це властивість інформації, яка характеризує захищеність інформації від несанкціонованого спотворення, руйнування або знищення [2].

Доступність інформації – властивість інформації, що характеризується унеможливленням несанкціонованого блокування (заборони) дій з інформацією фізичної або юридичної особи, яка має відповідне право [3].

Інформація з обмеженим доступом – інформація, право доступу до якої обмежене встановленими правовими нормами та (або) правилами. Така інформація потребує захисту [3].

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [3].

Метод захисту (protection method) – система принципів і прийомів, спрямованих на реалізацію функції захисту. Метод захисту може бути реалізований програмним, програмно-апаратним або апаратним способом [4].

Інформаційна безпека - стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [5].

Безпека інформації – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації [6].

### *1.2 Зовнішні носії інформації:*

Для передачі та зберігання інформації використовуються носії інформації. В якості носія може використовуватися аркуш паперу, фотоплівка, клітини мозку, диски, карти пам'яті різного типу, хмарне сховище, телефон тощо.

У наш час найрозповсюдженішими носіями даних являються засоби призначені для роботи з комп’ютером. Серед них найбільшою популярністю користуються жорсткі диски, оптичні диски, флеш-носії та хмарні середовища [7].

### *1.2.1 Інтернет. Хмарні сховища*

Хмара здається чудовим та легким рішенням, але потрібно пам'ятати про деякі нюанси доступу:

- Постійний доступ – чи завжди наявний доступ до Інтернету?

- Надійний/захищений доступ – чи можливо довіряти “вільному” Wi-Fi під час входу до системи?

Маючи накопичувач із шифруванням можна бути впевненим, що дані захищені, доступні і в разі їх втрати ніхто не отримає доступу до зашифрованих файлів.

Цей метод не вважається надійним засобом передачі інформації. У цьому випадку важко забезпечити конфіденційність інформації, оскільки доступ до неї не потребує прямого доступу до системи. Можливо зробити це будь-де за допомогою Wi-Fi, мобільної точки доступу чи іншої бездротової мережі. Навіть найкращий захист можна оминути. Необхідно пам'ятати, ідеального захисту не існує. Це займе лише додатковий час із найнадійнішою системою захисту хмарних сховищ проти шпигунського програмного забезпечення, вірусів, тощо. Можливо необхідні роки але з часом такі системи з'являться. Крім того, місце злодія може бути навіть на іншому континенті [8].

### *1.2.2 Магнітна стрічка, дискети, компакт(оптичні) диски*

На сьогоднішній час деяка вибірка носіїв інформації стає неактуальною. Об’єм пам’яті збільшується, все більше персональних комп’ютерів втрачають

дисководи, апаратне та програмне забезпечення для зчитування з неактуальних пристроїв збереження даних.

Магнітні стрічки користувалися великою популярність у кінці минулого 20 століття. Вони використовувалися для створення аудіо- та відеозаписів, зображення, та збереження цифрової інформації електронними обчислювальними машинами. Магнітна стрічка надала можливість багаторазового відтворення великих обсягів інформації. На той час це було дійсно актуально. В наш час магнітні стрічку практично не використовують для запису інформації, до того ж у такому випадку складно редагувати інформацію [9].

Дискети. Дискети або гнучкий диск - портативний носій інформації з об’ємом 80-512 Кбайт. В свій час вони мали велике розповсюдження. Дискети надавали можливість переносити файли та інформацію з комп’ютера на комп’ютер у порівняно зручному та компактному девайсі. На сьогоднішній час цей гнучкий магнітний диск має занадто малий обсяг пам’яті та більшість комп’ютерів не оснащені пристроями зчитування дискет. Дискети були відправною точкою у створенні майбутніх флеш-носіїв, що перевершують флоппі-диск у всьому [9].

Компакт-диски. Компакт диски мали більший об’єм пам’яті - близько 700 Мбайт. Навіть у наш час компакт-диски використовують для обміну інформацією, переносу даних, але не дуже великих розмірів та незалежними від електромагнітних полів. Вони були не дуже дорогі та згодом майже всі комп’ютери мали дисководи для читання компакт-дисків. Компакт-диски міцно зайняли свою нішу [10].

Накопичувачі поділялися за можливість запису та кількістю перезаписів на диск:

- CD-ROM - тільки для читання;
- CD-R - однократний запис інформації;
- CD-RW - багаторазовий перезапис.

Згодом з’явилися DVD-диски. Вони подібні до CD, але мали значний обсяг пам’яті - приблизно до 5 Гб у перших моделях. З часом об’єм пам’яті тільки збільшувався.

У 2006 році з’явився новий вид оптичних носіїв- BD. Завдяки новій технології запису вони могли зберігати інформацію до 50 Гб, що є значним обсягом навіть у наш час. Проте їх недоліком є те, що диски схильні до механічних пошкоджень під час використання та від впливу довкілля. Сам диск міг пошкодитися від лазерного променя під час зчитування інформації, легкі подряпини могли спричинити порушення цілісності, пристрій міг просто не реагувати на диск [11].

Описані вище носії інформації були проривом кожний у свій час. Вони були частиною еволюції накопичувача даних. Кожен наступний був кращий за попередній в якійсь мірі: збільшувався обсяг можливої інформації, зчитування та запис потребували менше зусиль та часу, користування та передача інформації становилися все комфортніше та швидше. Тож з часом з’явилися більш надійні та компактні носії, але кожен з них займає важливе місце в історії розвитку засобів зберігання інформації.

На сьогодні для зберігання та передачі даних найбільш актуальні наступні пристрої: USB-флеш-накопичувач, жорсткий диск та карта пам’яті. Кожен з них має як свої переваги, так і недоліки. Вони мають дещо різний напрям застосування, тож мають різні характеристики.

### *1.2.3 Флеш пам’ять*

Перед переходом розгляду флеш-носів необхідно зупинитися на роботі флеш-пам’яті. Флеш-пам’ять - тип комп’ютерної пам’яті, яка може на довгий час зберігати певну інформацію, при чому не використовуючи довгий час живлення. Дані можна видалити чи редагувати електричним методом.

У сучасних пристроях весь об’єм пам’яті розподілений на блоки. При необхідності інформація перезаписується цими блоками. Пам’ять має порівняно високу швидкість доступу до записаних даних та значну стійкіть до вібрацій. Одна з найголовніших переваг - дуже низька кількість споживаної енергії під час роботи. Серед найпомітніших обмежень варто виділити скінченну кількість циклів перезапису даних. Але більшість виробників гарантують, що такі носії здатні

витримати 1 млн перезаписів, що повинно вистачити звичайному користувачеві. Пристроям з флеш-пам’яттю притаманна чутливість до електростатичного розряду, як будь-якій електроніці. Наразі флеш-пам’ять має найрізноманітніше застосування: карти пам’яті, USB-пристрої, камери, аудіоплеєри, мобільні телефони, тощо [12].

### *1.2.4 Зовнішній портативний диск*

Зовнішній портативний диск призначений для зберігання та транспортування файлів великого об’єму. Це можуть бути фотографії, фільми, ігри, різноманітні програми та операційні системи, тощо. Їх часто використовують під час подорожі, переїзду або просто для резервного зберігання даних. З часом максимальний обсяг пам’яті тільки збільшується. Велика ємність портативного диску стає причиною достатньо великих габаритів. Звісно й ціна має не останнє значення.

Наразі існує два основних види портативного диску: HDD та SSD. Узагальнено, зовнішній жорсткий диск представляє собою набір (від 1 до 5) алюмінієвих, скляних або композитних пластини, що рухаються. Саме на них записується інформація шляхом намагнічування матеріалу на цих пластинах. Об’єм таких носіїв починається приблизно з 120 гіга-байтів, а максимум доходить до декількох терабайтів. Такі носії можна використовувати поза домом, проте нерідко вони можуть вимагати живлення від мережі, що зменшує комфортність. Швидкість передачі даних у такому випадку вища, але не всі пристрої мають подібні порти. Під час роботи такі носії шумлять, проте вони мають меншу вартість. Такі зовнішні диску уразливі перед сильним теплом, магнітом або механічними пошкодженнями. Це потрібно враховувати під час домашнього користування. HDD краще підходять для роботи вдома, ніж для подорожей [13].

SSD-диски з’явилися порівняно недавно. Такі носії складаються з набору мікросхем і керуючого контролера. Більшість сучасних моделей використовують для зберігання інформації флеш пам’ять. Вони монолітні, у них відсутні пластини та немає рухомих частин в основній конструкції. Такі особливості будови дозволяють їм бути більш стійкими до механічних пошкоджень, менше споживати

електроенергію та не виробляти шум під час роботи. Крім того, швидкість зчитування на багато більша (різниця може бути більше, ніж в 100 разів). Ці переваги надають можливість конкурувати з HDD-носіями. SSD-накопичувачі мають декілька значних недоліків, порівняно з HDD-носіями. По перше, об’єм SSD-дисків значно менше: від 120 гігабайтів до декількох терабайтів. Проте для звичайного користувача цього достатньо. Ціна на такі накопичувачі значно вищі. Одним з головних недоліків можна вважати обмежену кількість перезаписів даних: від 10 до 100 тисяч разів. Для середньостатистичного користувача це рідко має критичне значення [14].

Для виявлення кращого носія серед зовнішніх портативних дисків підведемо короткі та узагальнені результати для HDD- та SSD-дисків (Таблиця 1.1):

*Таблиця 1.1*

Порівняння характеристик HDD та SSD накопичувачів

| **Характеристики** | **HDD** | **SSD** |
|---|---|---|
| Об’єм пам’яті | До декількох десятків терабайтів | До декількох терабайтів |
| Узагальнена будова | Сукупність декількох пластин та зчитувальної ігли | Монолітний блок з мікросхем та контролера |
| Читання;запис | 0.68 МБ/с; 0.78 МБ/с | 63.6 МБ/с; 139 МБ/с |
| Чутливість до механічних пошкоджень | Дуже чутливі | Так як немає рухомих елементів в будові, менш чутливі. |
| Шум при роботі | Наявний | Відсутній |
| Вага | Існує величезна варіативність розмірів та об’єму пам’яті. можна знайти відносно легкі накопичувачі в обох варіантах | |
| Кількість можливих записів-зчитувань | Не обмежено | 10-100 тисяч. |

Однозначно визначити найкращий вибір накопичувача на даний момент не являється можливим. У різних умовах кожен з них має свої переваги та недоліки. Можливо обрати накопичувач залежно від типу інформації, потреб, коштів, тощо. HDD гарно підходить для довготривалого зберігання даних. Він значно дешевший та має достатньо об’єму зберігати величезні файли, але щоб швидко зчитувати їх він не призначений. При роботі з ним потрібно бути обережним.

Для поточної роботи кращим вибором серед цих носіїв буде SSD. Він краще підходить для швидкої повсякденної роботи з файлами та не так боїться механічних пошкоджень, а захист відіграє чи не найголовнішу роль.

### *1.2.5 Карта пам’яті*

Карта пам‘яті - портативний електронний носій інформації. Іноді називають флеш-карта, так як сучасні карти виготовляються на основі флеш- пам’яті [15].

Головна особливість цього носія це його розмір. Він надзвичайно маленький, порівняно з іншими носіями. Розмір карти пам'яті починається з 12 × 14 × 1,1 мм та більше. Як бачимо це дуже гарна перевага, але іноді перетворюється в недолік. Карту дуже важко знайти, якщо десь загубив, але це ціна за компактність. Не зважаючи на розмір, флеш-карти можуть зберігати величезні обсяги даних: від декількох МБ до десятки терабайтів інформації. Обсяг пам’яті різних стандартів флеш-карт (таблиця 1.2):

*Таблиця* 1.2

Об'єм пам'яті різних стандартів карт пам'яті

| **Стандарт** | **Об’єм пам’яті** |
|---|---|
| SD 1.0 | 8 МБ до 2 Г |
| SD 1.1 | 4 ГБ |
| SDHC | до 2 ТБ |

| | |
|---|---|
| SDXC | до 2 ТБ |
| SDUC | до 128 ТБ |

Спочатку вони використовувалися для підключення пристроїв введення-виводу. Пізніше з’явилися карти меншого формату, що допомогло знайти застосування для мобільних телефонів, цифрових фотоапаратів. З кожним наступним покоління розмір зменшувався, а попит зростав. Вони були найзручнішим об’єктом зберігання даних для професійних цифрових відеокамер. Вони впевенно себе відчувають у роботі з мобільним пристроєм, музикальним плеєром чи відеокамерою, проте для роботи з комп’ютером чи ноутбуком часто виникають труднощі. З часом на панелі можливих портів зникають роз’єми для карт пам’яті. Карти пам'яті неможливо підключити без спеціального пристрою. Вони передають інформацію за допомогою адаптера або кардрідера. Доводиться використовувати спеціальні кардрідери або адаптери карт пам’яті, що не зовсім зручно. Карти пам’яті добре підходять для роботи компактних, порівняно маленьких пристроїв. такі як телефони, плеєри, відеокамери, але не для комп’ютерів. На сьогодні USB-пристрої мають значно більше застосування при роботі з файлами, документами між різними персональними комп’ютерами.

### *1.2.6 USB-накопичувач*

USB-накопичувач - це зовнішній носій інформації, основа роботи якого базується на флеш-пам'яті з інтерфейсом підключення USB-порт [16]. USB-порт дозволяє працювати з ОС, що дає можливість швидко передавати, записувати файли. Крім того, флеш-пам'ять (флешка) здатна підключатися до різних пристроїв, наприклад DVD-програвач, телевізор, музичне обладнання, якщо вони оснащення USB-роз'ємом. Флеш-пам'ять найчастіше використовується для зберігання, обробки та передачі інформації між комп’ютерами та ноутбуками. USB-флеш-накопичувачі

дуже компактні, легкі і можуть зберігати великі розміри інформації. Наразі можна знайти флешку, що може містити терабайти інформації. Основна частина пристрою займає приблизно 5 сантиметрів, а вага - менше 60 г. Звичайна флешка легко поміщається в кишені та має низьку привабливу ціну.

USB-накопичувач без корпусу (Рисунок 1.1):

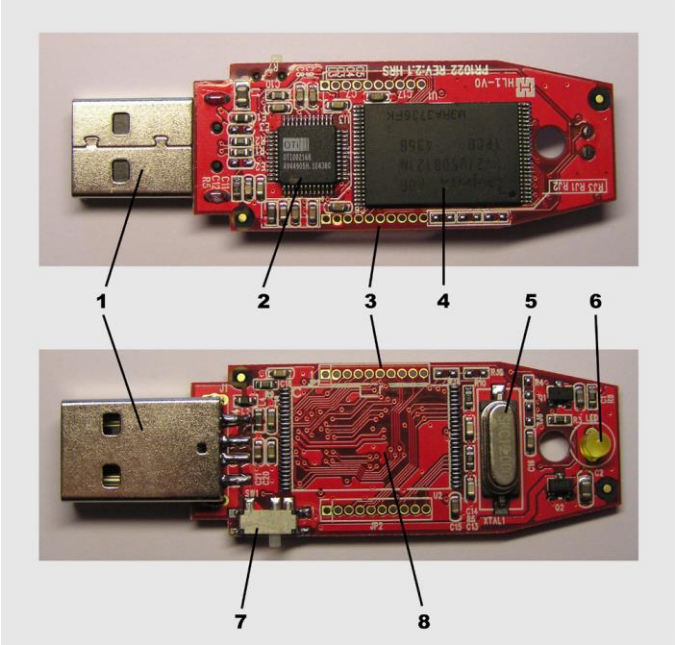


Рисунок 1.1 – Внутрішня будова флеш-носія

Стандартний пристрій USB Flash накопичувача складається з наступних електронних компонентів:

1 — USB-роз'єм;

2 — мікроконтролер;

3 — контрольні точки;

4 — мікросхема флеш-пам'яті;

5 — кварцовий резонатор;

6 — світлодіод;

7 — перемикач «захист від запису»;

8 — місце для додаткової мікросхеми пам'яті

Деякі сучасні накопичувачі (Рисунок 1.2) можуть мати мізерні розмір, основна частина якої USB:

Рисунок 1.2 – Накопичувач компактного розміру

На більшості флешок повсюдно використовуються файлові системи сімейства FAT. Залежно від розміру накопичувача застосовуються FAT16, FAT32 або exFAT. Для флешок розміром 64Гб і більше використовуються NTFS або exFAT [17].

До основних переваг використання USB-накопичувачів можна віднести [18]:

- Компактність.
- Можливість підключитися до великої кількості техніки, що обладнані USB-портами.
- Великий допустимий об’єм інформації.
- Низька вартість.
- Стійкі до механіх пошкоджень.
- Відсутність рухливих частин.
- Низьке енергоспоживання.
- Не чутливі до пилу.

До значних недоліків варто віднести [19]:

- Обмежена кількість циклів перезапису даних.
- Можливо зберігати інформацію на носії без підключення до пристрою протягом лише 5 років.
- Швидкість обробки інформації обмежена швидкістю роботи USB-порту.
- Вразливість до радіації та електростатичного розряду.

- Несиметричність порту підключення до пристрою. Під’єднати флешку вдається не з першого разу.

Даний носій інформації має не мало переваг, але в той же час вони стають джерелом потенційного порушення користування інформацією.

Накопичувач може використовуватися на будь-якому або майже будь-якому ПК за рахунок стандартного інтерфейсу підключення та відсутності необхідності встановлення додаткового програмного забезпечення. Власник інформації стає мобільнішим, маючи можливість працювати з необхідними даними не тільки на своєму робочому місці.

Може застосовуватися як для читання, так і для багаторазового запису та видалення файлів. Не потрібно великої кількості витратних носіїв інформації, робота користувача зручніша, ніж у випадку з CD. Файли на носії USB можуть бути несанкціоновано видалені або змінені [20].

Недорого коштує. Застосування в організації не вимагає значних витрат, часто працівники компаній застосовують самостійно придбані пристрої. Користувачі ставляться до пристрою легковажно, використовують не лише з службовою метою і часто втрачають.

Невеликого розміру та ваги. Зручно у застосуванні та перенесенні. Пристрій може бути легко викрадений у легального користувача зловмисником.

Щоб захищеність флешки відповідала рівню захищеності звичайного домашнього комп'ютера, не захищеного нічим, крім антивірусу, ця флешка повинна:
а) перебувати у квартирі та ніде крім,
б) бути якимось містичним чином захищено від можливого впливу вірусів.

Теоретично це можна досягти за допомогою організаційних заходів. Власник флешки, яка використовується лише всередині захищеного приміщення для перенесення інформації між кількома захищеними від вірусів комп'ютерами, може бути спокійним.

На жаль, така ідеальна з точки зору безпеки ситуація навіть якщо і виникає, то зазвичай триває недовго: флешку знадобиться винести кудись.

***Висновки за розділом 1***

Кожен з вище описаних флеш-носіїв наразі актуальний. Вони використовуються у різних сферах та мають свої переваги та недоліки. Карту пам’яті доцільно використовувати у компактних малих пристроях для зберігання фото- та відео матеріалів. Вона гарно підходить для роботи з такими файлами та обміну ними між різними носіями. SSD-накопичувач добре використовувати для зберігання порівняно великої кількості інформації на довгий проміжок часу та роботи з об’ємними файлами під час подорожі або просто резервного зберігання. Значні габарити не дозволяють носити носій кожного дня та комфортно з ним працювати. USB-флеш-накопичувач має найкращі характеристики для щоденної роботи з документами. Він надзвичайно компактний, більшість комп’ютерів підтримують цей формат. Даний вид накопичувача маж якщо не найкращі, то вище середнього показники.

# РОЗДІЛ 2
# ЗАГАЛЬНА ХАРАКТЕРИСТИКА НОСІЯ

## *2.1 Загальні терміни та визначення*

Розділ/том - це частина довготривалої пам’яті носія інформації (жорсткого диска, SSD, USB-накопичувача, тощо), логічно виокремлена для зручності роботи. Частина пам’яті, який має свою одну конкретну файлову систему [21].

Каталог (директорія, тека, папка) - це елемент файлової системи, призначений для групування та структурування файлів за певною ознакою. Сукупність каталогів утворюють ієрархію [22].

Сектор - це фізично найменша одиниця зберігання пам’яті. Розмір одного сектора дорівнює 512 байтів. Сукупність секторів- кластер. Кількість секторів в одному кластері завжди є кратним піднесення якогось числа до степеня 2 [22].

Кластер - це мінімальна одиниця адресації до даних, структурна одиниця електронної таблиці. Всі кластери на одному розділі однакові за розміром та мають свій порядковий номер. Розмір не фіксований, залежить від ємності диску [22].

## *2.2 Вибір файлової системи*

Після того, як визначено об’єкт, розглянемо методи та засоби для забезпечення його захисто. Для початку потрібно знати як зберігається інформація на носії. Базова структура, що відповідає за розміщення файлів на пристрої, їх упорядкування та доступ до них, називається файлова система. Вона забезпечуєте те, що файли будуть корректно зчитані операційною системою та з ними можна буде виконувати основні операції: пошук, запис, читання, редагування файлу, тощо.

Визначаємо яку файлову систему краще використовувати для захисту інформації. Наразі існує 2 найпопулярніші файлові системи: FAT та NTFS.

### *2.2.1 Огляд файлової системи FAT*

Однією з найрозповсюдженіших файлових систем являється таблиця розміщення файлів FAT. Загальна структура файлової системи FAT складається з наступних елементів [23]:

- Завантажувальний сектор.
- Таблица FAT (дві копії).
- Кореневий каталог.
- Область розміщення даних.

Завантажувальний сектор - розташований на початку файлової системи. Він необхідний для початкового завантаження системи. Також в ньому зберігається інформація про параметри розділа, логічного диску [24].

Таблица FAT (Таблиця розміщення файлів) - міні-образ диска/увесь об'єм пам'яті розподілений на кластери.

Кожен файл займає один або ланцюжок кластерів в таблиці FAT. Кожен кластер має подібну будову. Перші два елементи містять інформацію про саму систему FAT. Третій і наступні елементи призначені для файла, який знаходиться на дисковому просторі. Один з елементів має спеціальну мітку, що вказує на стан кластера. Існує три типи цих міток [25]:

- Вільний кластер - кластер, який доступний для запису файла, даних (для FAT16 цей набір символів- "0000H").
- Зайнятий кластер - в мітці вказується наступний номер кластера, що містить той самий файл. Якщо це останній кластер ланцюжка, то кластер має спеціальний код-позначення цього (для FAT16 цей - "FFF8 FFFFH").
- BAD-блок - кластер з помилкою доступу. В цьому випадку наявне пошкодження кластеру (для FAT16 цей набір символів - "FFF7H"). Ця мітка присвоюється при форматуванні диску для того щоб, наступного разу обмежити доступ до нього.

Таким чином утворюються ланцюжки кластерів, які є частинами одного великого файлу. В такий спосіб створюється повна таблиця розміщення файла на

носії. Пошкодження таблиці розміщення файлів повністю знищує структуру файлової системи, тому на диску завжди зберігається дві копії таблиці. Ідентичність цих таблиць регулярно перевіряються засобами операційної системи [25].

Кореневий каталог -це основна система папок в яку вкладено всі інші папки та інші каталоги, що забезпечують роботу файлової системи. Каталог, чи він кореневий чи підкаталог, являє собою базу даних, що містить інформацію про кожен зареєстрований в ньому файл. Для кожного файлу існує запис в каталозі. Всього на запис виділено 32 байти (Таблиця 2.1).

*Таблиця 2.1*

Розташування полів в кластері файлової таблиці FAT.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | | | | | | | | **2** | | | **3** | **4** | | | | | | | | | | **5** | | **6** | | **7** | | **8** | | | |

Інформація в каталозі записується послідовно. Він складається з восьми полів, які містять основну інформацію про файл, каталог:

1. Ім’я
2. Розширене ім’я
3. Атрибути
4. Створення
5. Час останнього редагування
6. Дата останнього редагування
7. Номер першого кластеру
8. Розмір файла

Ім’я. Якщо в перший байт має значення “00”, це означає, що цей елемент раніше не використовували, тобто не має сенсу зчитувати код далі, зберігаються ресурси системи. При видаленні файла перший байт змінює своє значення на E5 (1110 0101), решта байтів запису залишається незмінною. Саме це дозволяє відновити файл після видалення, якщо це місце не використовувалося для іншого файла.

Розширення імені. При описі файлу може бути пустим. Містить інформацію про те, коли зберігається інформація про каталог або том.

Атрибути файла. Кожен біт цього поля відповідає за певний атрибут файла, що вказаний в таблиці 2.2. Останні два біта резервні та повинні дорівнювати “0”.

*Таблиця 2.2*

Типи атрибутів файла

| **№ біта** | **Призначення** |
|---|---|
| 0 | Захищений |
| 1 | Прихований |
| 2 | Системний |
| 3 | Мітка тому |
| 4 | Каталог |
| 5 | Архівний |
| 6 | Не використовується |
| 7 | Не використовується |

Створення. Містить інформацію про дату і час створення, останньої роботи (читання запис) з документом.

Час останнього редагування. Ціле число, що отримується з формули години*2048+хвилини*32+секунд\2.

Дата останнього редагування. Ціле число, що отримується з формули (рік-1980) *512+місяць*32+день. Обмеження дати в такому випадку становить з 1980 по 2108 рік.

Номер першого кластеру. Вказує на перший кластер файлу в таблиці FAT. Якщо на диску ще не виділено місце для даних, то це поле має код “0000”.

Під час роботи програма робить запит до операційної системи з метою отримання доступу до вмісту якого-небудь файла. Операційна система читає записи каталога про цей файл, щоб знайти перший кластер документа. Потім вона звертається до елементу таблиці FAT, щоб знайти наступний кластер ланцюжка.

Система повторює запит, поки не знайде останній кластер потрібного файла. Таким чином вона повністю визначає в яких кластерах міститься інформація про файл та в якій послідовності. Тепер вона може надати програмі інформацію про будь-яку частину файла, до якого був запит.

В загальній логічній структурі файлової системи каталог розташований відразу після таблиці FAT. Має фіксовану кількість секторів в FAT12/FAT16. В FAT32 має змінний розмір.

Область даних - увесь інший об’єм пам’яті системи, який містить вміст файлів і каталогів.

Наразі існують наступні версії файлової системи FAT: FAT12, FAT16 (FAT), FAT32, exFAT (FAT64). Основна різниця полягає в розмірі кластера в таблиці. Число в даному випадку вказує на розрядність адресаціїї кластерів в таблиці. В файловій системі FAT для кожного файла виокремлено ціла кількість кластерів. Це означає один кластер не може містити інформацію про декількох файлів, навіть якщо вони займають надзвичайно мало місця. Це стає причиною того, що текстовий файл, що містить текст “Привіт” завжди мінімально займає об’єм кластеру, для системи з 32-кілобайтними кластерами, розмір файла буде 32 Кбайт, хоча реальний об’єм документу може становити 12 байтів. В такому випадку з’являється невикористана частина пам’яті, яка називається втраченим місцем. Вибір мінімального значення кластера здається найкращим варіантом, проте в такому разі збільшується кількість кластерів, а отже об’єм адресної інформації. Це призводить до зменшення швидкості виконання файлових операцій. Доводиться йти на компроміс та обирати щось середнє.

Сенс декількох файлових операцій в таблиці FAT, на які потрібно звернути увагу. Форматування - таблиці значень індексних вказівників, крім перших трьох записів (2 системні та 3 містить необхідні мітки тома, дані про пошкоджені сектори) та записи кореневого каталогу обнуляються. Область розміщення даних при цьому не змінюється.

Видалення файлу - перший символ файлового поля та всіх кластерів, що належать файлу змінюється на код “E5”. Область розміщення даних при цьому

також не змінюється.

Версії файлової системи FAT:

FAT 12 - використовувалася в основному для дискет. Вона не підтримувала ієрархічну систему каталогів. Всі файли розташовувалися в одному місці. Тобто не можливо було створити папки взагалі. Це було в якійсь мірі логічно, так як ця система для дискет, а вони були ємністю 160-180 Кбайт. Не було сенсу в розподіленні документів по різним текам. Зі збільшенням об'ємом допустимої інформації на дискетах та появі нових носіїв це обмеження стало значно незручним. З часом з'явилася нова версія, де це обмеження було вирішено.

FAT/FAT 16 - використовується на вінчестерах. На даний час також не актуальна через максимальний допустимий об'єм диску до 2 Гб. Має кореневий каталог фіксованого розміру (512 записів). Тобто всього можна мати на носії обмежену кількість файлів. Система має розмір кластера диску від 512 байтів до 32 Кбайтів, кількість - до 65524. Через це нераціонально використовується простір на розділі, фактично зникає велика кількість пам'яті через неповне заповнення кластеру. Не підтримується останніми версіями операційної системи Windows.

FAT 32 - теоретично підтримується на дисках з об'ємом пам'яті до 2 Тб, а файл може мати важити до 4 Гб. Логічно, Наразі, одна з найпопулярніших файлових систем. Практично всі прилади та операційні системи повність здатні працювати з таким форматом файлової системи. FAT 32 використовує 32-розрядяну адресацію кластерів. Його розмір може бути в межах від 512 байтів до 16 Кб. Цей допустимий розмір менше в порівнянні з попередньою версією, проте це підвищує ефективність використання дискового простору в середньому на 15 %. Не зважаючи на те, що розмір кластера може бути фактично будь-яким, традиційно він складає 512 байтів. Для деяких операційних системи це свого роду константа. Основний недолік - це обмеження файлу в 4 Гбайти, що не дозволяє зберігати величезні за пам'яттю дані. В операційних системах Windows 2000, Windows XP, Windows Vista та Windows 7 неможливо створити розділ більше 32 Гб, проте можна працювати, якщо вони створені в інших ОС. Ще одним обмеженням являєть кількість символів, що виділяється на ім'я файлу - 256. Це не так мало, але для тих, хто любить давати довгі

змістовні назви, це значний недолік. В наступній версії ця проблема вирішена.

exFAT/FAT 64 - Ця система спеціально створювалася для флеш-носіїв. Головні особливості полягають в більшому можливому об’ємі пам’яті як для окремого файла, так і для розділу. Другим головним плюсом стає швидкість оброблення даних, порівняно з попередніми версіями. FAT 64 збільшує максимальний об’єм розділу диску - більше 32 Гб, окремого файлу - більше 16 Еб та надає краще управління простором. Розмір кластера від 4 Кб до 128 Кб. В цій версії зменшено кількість перезаписів одного й того ж сектору, що надзвичайно важливо для флеш-носіїв, так як багаторазовий перезапис призводить до зношування (виведення з ладу) цих секторів.

Основним недоліком можна вважати в певному сенсі новизну цієї версії. FAT 32 набула широкого використання. Її підтримують майже всі носії, побутова техніка, телефони, телевізори, ОС. Оскільки exFAT порівняно нова система, існує велика кількість моделей пристроїв, які не здатні працювати з таким форматом: DVD-програвачі, сучасні телевізори, відеокамери. Linux-подібним ОС необхідно встановлювати спеціальне програмного забезпечення, а Android - це різновидність Linux! Це значно зменшує коло використання. Більш того, старі версії Windows не можуть працювати з ним. Звичайно, існують спеціальні драйвери, програми та оновлення для систем, щоб підтримувати цей формат. Навіть з цим фактом нерідкість пристрій, що не підтримує даний формат. Джерело проблеми полягає в ліцензуванні цього формату на пристроях зі сторони Microsoft. В цій сфері дуже багато правових суперечок. Підтримка exFAT повноцінно і легально реалізована тільки в Windows, при чому не у всіх старих версіях. Іншим недоліком являється, більш складна структура, що призводить до більшого використання обчислювальних ресурсів.

### *2.2.2 Огляд файлової системи NTFS*

NTFS - файлова система з підвищеним рівнем безпеки та максимального допустимого об’єму даних, розроблена для заміни системи FAT. Однією з головних переваг являється максимальний розмір: для розділу - це 16 Тб та немає обмежень на розмір файлу. Тобто єдине обмеження - це 16 Тб на всю систему. Висока швидкість роботи через малий розмір файлових кластерів від 512 байтів до 64 Кб, але оптимальним вважається розмір до 4 Кб [20].

NTFS має високий рівень захищеності та складну ієрархічну структуру. В ній немає атрибутів, але є можливість розмежовувати доступ до файлів для різних користувачів і груп користувачів. Крім того можна надавати їм квоти, тобто обмежувати максимальний розмір використання простору різним користувачам. Користувач при створенні файлу становиться фактичним її власником. Він може встановити різний рівень доступу для інших користувачів до нього. Проте, дозволи, квоти та розмежування доступу не захищають від програм-зломщиків. Це не абсолютний захист. Система використовує журнулювання дій для підвищення надійності. Вона характеризується високою продуктивністю і ефективність використання дискового простору. Покращений рівень безпеки завдяки використанню методів шифрування даних за допомогою EFS. EFS дозволяє шифрувати файли і папки, але тільки на локальних комп’ютерах. Вона не може шифрувати стиснуті або системні дані.

В файловій системі NTFS диск складається з наступних частин [17]:

- MFT - загальна таблиця файлів, де міститься інформація про файли та каталоги.
- Дані користувача.
- Метафайли - файли, що містять службову інформацію.

Кожен мета-файл відповідальний за певну дію/функцію системи. Наприклад, LogFile - файл запису історії всіх операцій в системі в спеціальний журнал; Boot - завантажувальний сектор; Bitmap - контролює вільне місце в томі, тощо. Така система захищає документи при електричних збоїв або при проблемах роботи

операційної системи. В таких випадках існує можливість відновлювати файли після збою за допомогою System Restore. У разі відновлення даних в такій ситуації система орієнтується на записи в журналі/історії змін та відновлює останню стабільну версію даних. Але в разі серйозного збою, відновити інформацію надзвичайно складно, майже неможливо. Однією з головних причин цьому так само як і з exFAT є відсутність офіційної документації файлової системи від Microsoft у вільному доступі.

До переваг можна віднести швидку роботу з великими файлами та можливість використання довгих імен для файлів. На жаль, системі притаманні схожі проблеми, що й у exFAT. Система не сумісна в роботі з операційним системами нижче Windows NT та має обмеження в сумісності з іншими ОС, такими як Mac OS та Linux. Також, популярні ігрові консолі Playstation та Xbox 360 також не працюють з таким форматом, тільки Xbox One здатна читати файли в NTFS. Крім того, система має високі вимоги до об’єму оперативної пам’яті.

***Висновки за розділом 2***

У свою чергу, NTFS має додаткові засоби для забезпечення підвищеного рівня захищеності даних від несанкціонованого доступу. Вона відмінно підходить для внутрішніх жорстких, системних дисків та SSD для роботи з останніми версіями ОС Windows, починаючи з NT [20].

exFAT - переймає принцип роботи файлової системи FAT разом з більшістю переваг та недоліків. Має більш шире коло пристроїв, що можуть працювати з цим форматом та спеціальні додаткові програми для роботи з більшість ОС ніж NTFS. Ця система підходить для флеш-носіїв, зовнішніх накопичувачів з великим об’ємом пам’яті для зберігання необробленого відео, 3D-проекта, тощо та інші величезні файли [20].

FAT 32 - одна з найрозповсюдженіших, простих та старих файлових систем. Це забезпечує сумісність роботи майже з будь-яким приладом та ОС. Існує велика кількість документації для роботи з нею. Система має обмеження на розмір файлу

до 4 Гб та розділу до 8Тб. Вона має менше вбудованих інструментів для захисту даних, проте наразі існує безліч сторонніх програм для вирішення цієї задачі. До недоліків можна віднести зменшення швидкості роботи з файлами при великій їх кількості в одному каталозі. Відмінно підходить для зовнішніх носіїв з порівняно невеликим об’єм пам’яті для роботи з текстовими документами, презентаціями, файлами до 4 Гб [20].

# РОЗДІЛ 3
# ІНСТРУМЕНТИ ЗАХИСТУ ІНФОРМАЦІЇ НА НАКОПИЧУВАЧІ

## *3.1 Основні способи захисту*

Втратити маленький пристрій дуже просто, тим більше, якщо користувач за характером не дуже уважний і зібраний. Втративши флешку, неможливо бути впевненим ні в тому, втрачена вона або вкрадена, ні в тому, що людина, яка випадково знайшла її, не скористається записаними даними.

Існують певні інструменти для захисту даних на зовнішньому носії. Додатковий захист файлів вбудований не на кожному USB-накопичувачі та файловій системі, проте сьогодні існує велика варіативність захисту даних на флешці. Лише в деяких моделях USB-носія вже передбачений додатковий захист інформації. Він може виявлятися в шифруванні даних, спеціальних програмних методів чи просто в особливості будови корпуса флеш-носія. Можна виділити три основних способи обмеження доступу до вмісту диска USB-flash:

- Механічних засіб;
- Апаратний спосіб;
- Програмне шифрування.

Розглянемо кожен з них детальніше.

Механічний спосіб:

До механічних засобів відносяться всілякі пристосування, безпосередньо перешкоджають підключенню флешки до USB-роз'єму комп'ютера. Одним з цікавих варіантів такого захисту є кодовий замок-ковпачок для флешки (Рисунок 3.1). Часто можна побачити флешки з вбудованим кодовим замком. Механізм такого замка блокує висувний язичок пристрої всередині корпусу, діючи за принципом кодового замка на валізі.

Рисунок 3.1 – Флеш-носій з кодовим замком-ковпачком

Одним з найбільш оригінальних рішень є приховування флешки в криптекс - міцної трубці, оснащеної кільцевим кодовим замком (Рисунок 3.2). Сама ідея такого захисту інформації належить Леонардо да Вінчі. Але в дизайні USB-flash-накопичувачів це досить ново та незвично.

Рисунок 3.2 – Криптекс для приховування флешки

Механічні засоби захисту інформації на дисках USB-flash виглядають дуже ефектно, але фактично не володіють високою надійністю. З механічними перешкодами, при наявності часу і бажання, впоратися досить легко. На загальнодоступному сегменті ринку механічних замків для флешок, рідко можна знайти пристрої, виконані з надміцних матеріалів і гарантовано руйнуючих носія при спробі несанкціонованого доступу до нього. Більшість кодових замків для флешок мають статус сувенірної продукції. Вони використовуються в більшій мірі

для краси, для виділення, привабливості флешки як такої [22].

Апаратний спосіб

Більш надійним засобом захисту даних на флешках та інших накопичувачах інформації вважається апаратне шифрування даних. У випадку з дисками USB-flash основним елементом шифрування такого пристрою являється спеціальний чіп. При зчитуванні інформації з флешки дані проходять через цей чіп разом зі спеціальним ключем шифрування. Без цього ключа прочитати дані неможливо. Такі пристрої можуть мати різні методи аутентифікації. Цей захист зазвичай реалізований у вигляді введення пароля, встановленого користувачем, але іноді може застосовуватися біометричний захист.

Наскільки може заспокоїти PIN-код – питання філософське. Приблизно на стільки ж, наскільки заспокійлива думка, що, швидше за все, ніхто не стане піднімати флешку, що валяється, і скоро її просто роздавлять. Добре, якщо так, а якщо ні, то PIN-код підберуть і дуже легко. Призначені для цього програми сьогодні є у кожного студента.

Теоретично можна боротися із цим, збільшуючи довжину PIN-коду. Але чим довше PIN-код, тим вища ймовірність того, що він записаний на корпусі флешки.

Іноді альтернативою паролю може служити відбиток пальця. Для цього в корпус флешки вбудовується біометричний датчик. Слід зазначити, що вбудований в флешку сенсор для зняття відбитків пальців є більше іміджевим аспектом, ніж нагальною потребою. На практиці такий метод аутентифікації має серйозні недоліки. У більшості випадків, для коректної роботи датчика палець слід притискати з невеликим зусиллям. При цьому неминуче відхилення флешки від своєї осі і створення зайвого навантаження на USB-порт комп'ютера. Накопичувачі з біометричним датчиком зручно використовувати для авторизації при підключенні флешки до горизонтально орієнтованим бічним USB-портів ноутбуків і вертикально орієнтованим портам на передній панелі стаціонарних комп'ютерів. В інших випадках користуватися сканером відбитка пальця просто не комфортно. Біометричний сканер є хорошою опцією в двох випадках: коли потрібно зробити на когось враження і коли існує реальна загроза того, що пароль, введений з

клавіатури, стане доступним третім особам.

В якості альтернативи біометричного датчика може виступати справжній електронний кодовий замок (Рисунок 3.3). Щоб отримати доступ до даних на флешці, власник повинен ввести послідовність з чотирьох або більше цифр за допомогою кнопок, розташованих на корпусі пристрою. Головною перевагою цього рішення полягає в тому, що розблокування флешки проводиться до її підключення до комп'ютера. Працездатність замку забезпечується за рахунок вбудованого в корпус флешки акумулятора [23].


Рисунок 3.3 – Флешка з електронним кодовим замком

Програмне шифрування:

Третій спосіб шифрування даних на флешці є найбільш доступним і в той же час найменш зручним. Існує велика кількість програм, які дозволяють шифрувати дані. В основі роботи всіх цих програм лежить створення закритого паролем файлу-контейнера, всередині якого зберігаються «секретні» дані. Щоб прочитати інформацію в такому цифровому контейнері, необхідно ввести пароль. Після цього в системі з'явиться віртуальний знімний диск, на якому будуть доступні раніше приховані дані.

Різниця між програмами лише в нюансах. Одні програми повністю приховують невелику ділянку дискового простору, інші - створюють файл, видимий в системі. Багато програм дозволяють користувачеві самостійно вибрати, який алгоритм шифрування буде використаний для кодування даних.

Програмні заходи використовуються для шифрування даних на накопичувачах для забезпечення конфіденційності та цілісності даних. Шифрування може бути

проведено як для окремого файла, так і для всього накопичувача. В залежності від об’єму та типу даних виділяють наступні різновиди шифрування [24]:

- Шифрування всього носія.
- Створення додаткового зашифрованого розділу/папки.
- «Точкове» шифрування окремих файлів.

Шифрування окремих файлів:

Використання засобів шифрування USB-носія вирішує завдання контролю доступу до інформації, що зберігається на ньому. Адже якщо інформація записується тільки в зашифрованому вигляді, то прочитати її можна, тільки знаючи справжній ключ. Головним недоліком цих засобів є складність управління засобом криптографічного захисту інформації (СКЗІ), зокрема ключами шифрування. У найпростіших випадках ключі вираховуються на основі пароля користувача. Але при цьому USB-носій може використовуватися тим самим користувачем і поза підприємством. На наш погляд, правильнішим має бути використання системи управління ключами, яка працювала б тільки в корпоративному середовищі і не дозволяла б користувачеві правильним чином згенерувати ключ шифрування поза цим середовищем. Проте, як повноцінний СКЗІ, такий засіб складно в управлінні. У цьому слід пам'ятати, що СЗИ НСД теж може бути обов'язковим задля забезпечення безпечної програмного середовища використання СКЗІ.

Створення віртуального жорсткого диска (криптоконтейнера):

Зручний засіб для роботи із зашифрованою інформацією на комп'ютері. На жорсткому диску або flash-носії створюється файл або область диска, яка зашифрована. Перед початком роботи диск монтується в систему, і вся подальша робота з ним відбувається як зі звичайним носієм.

Інформація шифрується на льоту, непомітно для користувача. Для монтування диска необхідно ввести пароль або надати електронний ключ і пін-код доступу до нього. Як правило, переважна більшість програмних продуктів цього типу пропонує на вибір кілька алгоритмів шифрування або їх комбінаторики.

До мінусів програмного шифрування даних можна віднести необхідність установки програми на кожен комп'ютер, де необхідно прочитати зашифровані дані

на флешці. Навіть ті програми, які встановлюються безпосередньо на диск USB-flash, вимагають для роботи права адміністратора, щоб встановити в системі спеціальний драйвер.

### *3.2 Захист від несанкціонованого копіювання*

Довгий час вважалося, що захист цифрової інформації від копіювання неможливий. Всі методи, що створювали такий захист зводилися до заплутування алгоритму і створення пристроїв, стійких до вторгнення і сканування. Виділення ж її в самостійний вид захисту обумовлено, головним чином, прагненням захистити авторські і комерційні інтереси розробників та власників програм для ПК. Виробникам, що випускають свою продукцію на зовнішніх носіях доводиться робити захист від копіювання. Для цього використовуються різні методи та способи захисту.

У світовій практиці існують наступні способи поширення програм [25]:

- FreeWare (вільно зі збереженням прав за автором);
- ShareWare (2-4 тижні випробувати, потім або не використовувати або оплатити);
- CriptWare (дві версії: демо + зашифрована робоча).

В якості ключового елемента можуть виступати флеш-накопичувач, певна частина апаратури ПК або спеціальний пристрій, що підключається до ПК.

Основні функції, які виконують системи захисту програми від копіювання, полягають в наступному [25]:

1) Ідентифікація середовища, з якої буде запускатися захищається програма. Воно полягає в створенні індивідуальної важко відтворюваної особливої ознаки.

2) Аутентифікація середовища, з якого надходить запит на копіювання інформації, що знаходиться під захистом програми.

3) Реєстрація санкціонованого копіювання.

4) Реагування на спроби несанкціонованого копіювання.

5) Забезпечення недоступності вивченню алгоритмів роботи системи захисту.

На сьогоднішній день під засобами захисту інформації на флеш-накопичувачах розуміють сукупність різних технічних і програмних систем і пристроїв, що використовуються для вирішення різних завдань із захисту інформації, в тому числі попередження витоку, захисту даних на флешці (флеш-накопичувачі) від запису і забезпечення повного комплексу заходів для безпеки інформації, що захищається. Реакція на спроби несанкціонованого копіювання може бути різна. Наприклад, відмова у виконанні запиту, попередження зловмисника, знищення програми або документів, що підлягають нерозголошенню (після першої спроби або після декількох спроб і т. д).

Протидія вивченню алгоритмів роботи системи захисту передбачена для того, щоб перешкодити зловмиснику в вивченні структури і змісту реалізованої на носії системи захисту, алгоритму роботи системи з метою її нейтралізації. Важливість цієї функції визначається тим, що кваліфікований системний програміст, в загальному випадку, може визначити логіку роботи будь-якого модуля всієї системи захисту і знайти способи її подолання.

З технічної точки зору дозвіл відтворення інформації, що захищається і в той же час заборона її копіювання являє собою вкрай складну задачу, тому що відтворення передбачає читання інформації, її обробку та запис на пристрій виведення, а копіювання - читання і запис інформації на пристрій зберігання. Ефективний технічний захист інформації від несанкціонованого копіювання при дозволеному її відтворенні може бути досягнута, тільки коли пристрій відтворення знаходиться цілком під контролем правовласника.

У загальному вигляді методи захисту інформації від несанкціонованого копіювання можна розбити на три групи [25]:

- Методи, що перешкоджають безпосередньому копіюванню.
- Методи, що ускладнюють зчитування скопійованої інформації.
- Методи, що перешкоджають використанню скопійованої інформації.

Незалежно від ознаки класифікації найефективнішими методами захисту інформації від несанкціонованого копіювання є криптографічні. Однак в цьому випадку типовою є ситуація, коли для використання захищеної інформації

правомірний власник повинен мати крім самої інформації ще й ключ до неї, що зменшує рівень захисту від несанкціонованого копіювання. Тому криптографічні методи захисту інформації від несанкціонованого копіювання припускають приховування від користувача використання ключа шифрування.

Системи захисту від копіювання можна розділити на наступні групи:

Захист програми з використанням «нестандартного» носія або способу запису інформації. Метод передбачає використання нестандартних протоколів запису даних на носій. Як приклад, можуть бути використані “биті” сектори, що не дозволяють зчитувати файли стандартними засобами. Недоліком цього методу являється потенційна можливість отримати інформацію. Існує дуже багато програмних інструментів для зчитування інформації різного типу запису на носій.

Використання підходу SaaS. Перенесення коду самих програм в хмару і надання функціоналу цих програм, як сервісу. При цьому код програми розташований і виповнюється на сервері, доступному в глобальній мережі. Доступ до нього здійснюється з використанням алгоритмів перевірки наявності ліцензії у клієнта.

Спеціальні засоби, що ускладнюють копіювання інформації. Прикладом методу являється обфускатор. Він виконує обфускацію - «заплутування» коду, на рівні алгоритму, вихідного тексту.Текст або код у такому разі приводиться до виду, який зберігає свою функціональність, але ускладнює аналіз алгоритмів роботи і модифікацію при декомпіляції. Як правило, вона застосовується в критичних до безпеки, але не критичних до швидкості місцях програми, так як це зменшує швидкість виконання коду і відповідно збільшує час виконання програми. Хоча обфускація допомагає зробити розподілену систему безпечнішою, не варто обмежуватися тільки нею. Обфускація - це безпека через неясність. Вона не гарантує складності декомпіляції і не забезпечує безпеки на рівні сучасних криптографічних схем [25].

Використання механізмів активації програмного забезпечення. Програма «прив'язується» до заліза комп'ютера (підраховується контрольне значення, однозначно відповідає встановленим комплектуючих комп'ютера, його системним

характеристикам). Це значення передається розробнику програми. На основі нього розробник генерує код активації, відповідний для активації програми лише на зазначеній машині (копіювання встановлених виконуваних файлів на інший комп'ютер призведе до непрацездатності програми). З огляду на те, що скопіювати встановлене захищене додаток все-таки можна, то захист в цьому випадку відбувається в більшій мірі «від використання». Основним недоліком є ситуація, якщо користувач проводить модернізацію комп'ютера (в разі прив'язки до заліза), захист відмовляє. Автори багатьох програм в подібних випадках готові дати новий реєстраційний код. Як прив'язки використовуються, в основному, серійний номер BIOS материнської плати, серійний номер вінчестера. З метою приховування від користувача дані про захист можуть розташовуватися у прихованій області пам’яті. Іншим недоліком є потенційна можливість емуляції «універсального» апаратного оточення (навіть якщо розробник реалізував захист від використання програми під віртуальною машиною).

На теперішній час розроблено значна кількість програмних додатків для захисту флеш-накопичувача від несанкціонованого копіювання. Кожна програма має свій набір інструментів, алгоритмів і методів для запобігання копіювання інформації. Деякі з них працюють дуже надійно, деякі з них на задовільному рівні. Згодом з'являються нові версії та аналоги програм. Розглянемо деякі з них.

### *3.3 Дослідження способу захисту «Folder Lock»*

Програма Folder Lock пропонує швидкий спосіб шифрування і захисту паролем файлів і папок. Після шифрування папки, її розташування (шлях до неї) буде прихований і доступний тільки через програмний інтерфейс [26].

Сейфи. Вона так само може створювати зашифроване сховище, зване «Locker» або «Сейф». «Locker (s)» захищені 256-бітовим шифруванням AES. У ньому можна зберігати безліч своїх особистих файлів / папок і захистити їх паролем одним натисканням кнопки. «Сейфи» є портативними, так що можна безпечно їх передавати, робити резервне копіювання, тримати на USB, CD / DVD, ноутбуці або

передавати по електронній пошті [26].

Повне видалення файлів. Просте видалення файлів не є гарантією того, що вони не можуть бути відновлені знову. Знищення файлів назавжди видаляє ваші файли з жорсткого диска таким чином, що навіть програма для відновлення файлів не зможе відновити їх знову. Блокування папок не тільки допомагає знищувати файли, але і дозволяє знищувати порожнє місце на диску, тому незалежно від того, які файли були видалені раніше, вони також знищуються.

Folder Lock має додаткові функції, такі як, блокування доступу, прихований режим, запобігання спробам злому, мобільність, очищення історій і багато іншого (всього понад 20 пунктів), що дозволяє зберегти конфіденційність і безпеку особистих даних користувача. Програма працює на 32-бітних і 64-бітних Windows 10, 8, 7, Vista, XP [26];

### *3.4 Опис програми захисту «USB Secure»*

Невелика і проста програма для захисту паролем USB і інших флеш-накопичувачів. Програма не вимагає прав адміністратора і працює з усіма типами портативних пристроїв (USB, флеш-диски, флеш-карти, карти пам'яті, зовнішні жорсткі диски і т.д.). При першому запуску необхідно задати пароль, який буде використовуватися для подальшого доступу до документів. Заблокувати відкриття можна як весь носій цілком, так і вибрати окремі папки та файли на свій розсуд. При використанні інструменту жоден користувач, якому не повідомляли пароль не зможе відкрити / відредагувати / скопіювати / видалити запаролених дані. Вона працює автоматично, як тільки диск USB підключений, просить ввести пароль [27].

### *3.5 Опис методу шифрування «EFS»*

Це швидкий метод шифрування в Windows. EFS є вбудованим інструментом, використовуваним файлової системою NTFS. Замість шифрування всього диска, EFS дозволяє захищати каталоги і окремі файли. Під час роботи Windows створює

ключ шифрування, який зберігається локально. Процес є простим, але не гарантує повну безпеку. Доступ до зашифрованої інформації можливий тільки з зазначенням пароля і логіна облікового запису. Слід записати ці дані, оскільки в разі їх втрати інформація залишиться заблокованою назавжди. EFS файл втрачає шифрування після його переміщення в файлову систему FAT 32 або exFAT, а також при передачі через мережу або по електронній пошті [28].

### *3.6 Дослідження роботи системи шифрування «BitLocker»*

BitLocker - це система шифрування диска, включена у версії Microsoft Windows Professional. Програма призначена для захисту даних методом шифрування цілих томів. Щоб розблокувати диск, захищений за допомогою BitLocker, потрібно ввести пароль або використовувати зовнішній USB-диск. Підтримуються наступні алгоритми шифрування [29]:

- AES 128.
- AES 128 с Elephant diffuser (використовується за умовчанням).
- AES 256.
- AES 256 с Elephant diffuser.

Сам ключ може зберігатися в TPM або на USB-пристрої, або ж на комп'ютері. TPM - назва реалізації криптопроцесора, в якому зберігаються криптографічні ключі для захисту інформації. BitLocker шифрує том, а не фізичний диск. Том може займати частину диска, а може включати в себе масив з декількох дисків. Для роботи BitLocker в разі шифрування системного диска буде потрібно два NTFS-томи, один для ОС і один для завантажувальної частини.

### *3.7 Опис роботи програмного забезпечення «BestCrypt»*

BestCrypt - це пакет програм для створення на жорсткому диску комп'ютера віртуального зашифрованого диска. З зашифрованим контейнером можна працювати як зі звичайним жорстким диском - розміщувати на ньому файли і

виконувати з ними будь-які операції, інсталювати програми і т.д. BestCrypt створює і підтримує зашифровані віртуальні диски, причому ці диски позначено, як звичайні диски з відповідними літерами дисків. Будь-який тип фізичних носіїв даних можна використовувати для зберігання даних і доступу до них в контейнерах BestCrypt: жорсткі диски, змінні носії, магніто-оптичні пристрої і т.д [30].

### *3.8 Дослідження роботи програми «Apacer Compression Explorer»*

Apacer Compression Explorer - прикладне програмне забезпечення, яке забезпечує стиснення, декомпресію та захист паролем даних. ACE використовується на флеш-накопичувачах USB 2.0 серії Apacer Handy Steno. ACE забезпечує безпеку файлів на рівні пароля, щоб запобігти порушенням особистих чи критичних даних. Захист файлів, реалізований за допомогою запиту пароля, який активується під час підключення флеш-пам’яті та запуску плагіну Handy Steno [31].

Не маючи складного інтерфейсу, ACE сприяє зручному та швидкому автоматичному стисканні та збереженні файлів на флеш-диску. Оскільки ACE встановлений на флеш-носій, користувачам не потрібно встановлювати додаток на ПК, що чудово підходить для мобільності. Крім того, весь інсталяційний пакет ACE займає лише менше 1 Мб місця на флешці.

Apacer Compression Explorer складається з двох частин (Рисунок 3.4). Перша - це провідник ACE, який схожий на провідник Windows для управління файлами та всіх функцій ACE. Інша - значок ACE Express, який є ярликом для швидкого стиснення та зберігання файлів на накопичувачі.

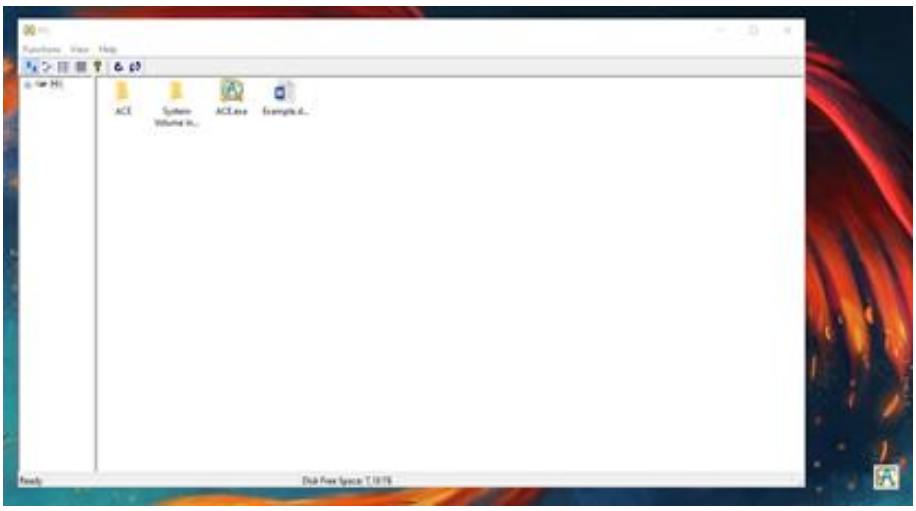

Рисунок 3.4 – Провідник та значок ACE Express після запуску програми

Значок ACE Express - це невеликий значок, який з’являється на робочому столі комп'ютера. Він дозволяє користувачам просто перетягувати файли на значок, щоб автоматично стискати та зберігати файли на флеш-пам’яті Apacer Handy Steno Series. Швидкий, простий і завжди доступний, він дозволяє користувачам стискати та зберігати файли у свою флешку, незалежно від того, що вони роблять на своєму ПК.

Вікно провідника ACE не тільки забезпечує повний перегляд всього вмісту флеш-накопичувача, воно також пропонує простий інтерфейс управління, щоб користувачі могли легко керувати всіма файлами на флешці. Окрім функції стиснення, ACE також забезпечує функцію захисту паролем, яку легко встановлює користувач.

Щоб отримати змогу використовувати функції цієї програми необхідно спочатку завантажити на флеш-носій та виконати файл ACE.exe. При першому запуску програми, з’явиться спливаюче вікно, що запросить встановити пароль. (Рисунок 3.5). Після встановлення паролю, його потрібно буде вводити кожен раз, якщо необхідно доступ до захищених файлів. Програмний засіб готовий до використання. Файл пароля також зберігається у /ACE/ACE.pwd на флеш-диску. У разі видалення цього файлу, ACE буде обробляти запит, як при першому запуску і попросить користувача встановити новий пароль.

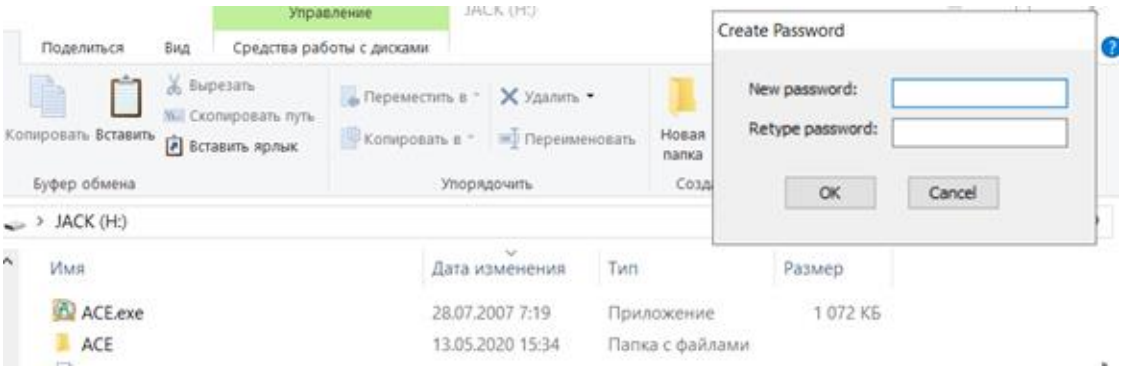


Рисунок 3.5 – Спливаюче вікно запиту введення паролю

Клікнувши на ліву клавішу мишки, відкривається провідник, у разі натискання правої - ми бачимо контекстне меню (Рисунок 3.6), що пропонує наступні функції:

- Показати/скрити теку ACE з файлами.
- Встановити шлях до папки, де будуть зберігатися документи.
- Зміна паролю.
- Інформація про дійсну версію програми.
- Вихід з програми.

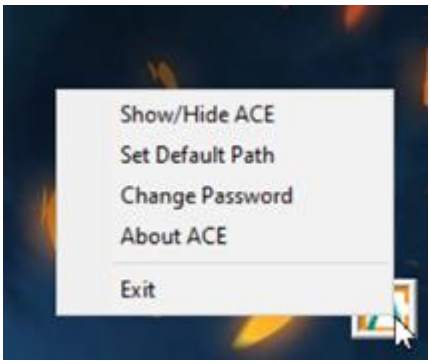


Рисунок 3.6 – Функції значка ACE Express:

Розглянемо алгоритм роботи програми. Для стиснення/шифрування файлу необхідно виконати:

1. У Windows Explorer виберіть файли або папку, яку потрібно скопіювати на флешку.

2. Перетягніть (натисніть і утримуйте лівою кнопкою миші) і перепустіть (відпустіть мишу) ці вибрані файли чи папки до вікна провідника ACE або до значка ACE Express.

3. Файли або папка будуть автоматично стискатися і зберігатися у вікні провідника ACE або зберігатися безпосередньо на флеш-накопичувачі в попередньо встановленій папці в значку ACE Express.

Приховування теки з файлами:

Для цього використовується значок ACE Explorer. У правому верхньому куті вікна ACE Explorer необхідно обрати "закрити" або "Сховати".

Можливо використовувати вікно ACE на панелі функцій, щоб його приховати або під час використання вікна значка ACE Express необхідно двічі клацнути лівою кнопкою миші, щоб відкрити вікно ACE, або правою кнопкою миші, щоб побачити спадне вікно, і обрати «Відкрити / Сховати вікно провідника ACE».

Специфічність паролю:

Пароль створюється при першому запуску плагіну. Він використовується для шифрування даних. При зміні чи втраті пароля, файли що були зашифровані першою версією пароля неможливо відкрити новим. Пароль зберігається в папці ACE. При видаленні цієї папки, пароль також видаляється. У цьому випадку програма при наступному запуску буде просити створити пароль, як при першому використанні. Файли, що були зашифровані видаленим паролем відповідно не можливо відкрити іншим новим. Їх можливо розшифрувати лише аналогічним паролем.

Варто зауважити, після виходу з програми документи залишаються на носії в форматі azf. Їх можна копіювати, видалити, змінити назву, проте відкрити лише за допомогою паролю, яким вони були зашифровані.

Розглянуто деякі можливості програмного забезпечення Apacer Compression Explorer. Ця програма не має широкого поширення, проте вона володіє деякими цікавими методами забезпечення конфіденційності інформації на носії.

***Висновки за розділом 3***

У загальному вигляді методи захисту інформації від несанкціонованого копіювання можна розбити на три групи:

- методи, що перешкоджають безпосередньому копіюванню;
- методи, що ускладнюють зчитування скопійованої інформації;
- методи, що перешкоджають використанню скопійованої інформації.

Незалежно від ознаки класифікації найефективнішими методами захисту інформації від несанкціонованого копіювання є криптографічні. Системи захисту від копіювання можна розділити на наступні групи:

Захист програми з використанням «нестандартного» носія або способу запису інформації.

Використання підходу SaaS. Перенесення коду самих програм в хмару і надання функціоналу цих програм, як сервісу.

Спеціальні засоби, що ускладнюють копіювання інформації. Прикладом методу являється Обфускатор.

Використання механізмів активації програмного забезпечення. Програма «прив'язується» до заліза комп'ютера.

У розділі також розглянуті методи захисту інформації, які відносяться не тільки до флеш-носіїв, але до інших видів носіїв, наприклад CD-диски, дискети, дані на розділах жорстких дисків. Такі методи і програми розглянуті для того, щоб розробити нові підходи захисту, які базуються на розглянутих. Неможливо повністю перенести метод на інший тип накопичувача, так як вони мають різну файлову структуру, алгоритм розміщення інформації, існує досить багато відмінностей. Метою їх розгляду було виділення, ідеї, суті в цих методах захисту і злому інформації на них. Деякі описані програми які надають захист від копіювання даних в той же час дозволяють повністю видаляти файли на носії. В основному програми переформатовують документи в спеціальний сторонній формат або / і переносять в окремий прихований розділ / папку.

На основі вище розглянутих програм, можливо підсумувати функції, які дуже

важливі в розробці методу захисту даних в поточній дипломній роботі:

- шифрування даних;
- віртуальний диск для збереження конфіденційної інформації (часто використовується як альтернатива шифрування);
- захист від копіювання;
- повне видалення даних;

# РОЗДІЛ 4
# ПРИНЦИП РОБОТИ ВІРТУАЛЬНОГО ЗАХИЩЕНОГО ДИСКУ

## *4.1 Загальний принцип роботи*

Метод захисту даних базується на віртуальному розподіленні всього розділу носія на дві частини: відкриту та приховану. На носії зберігаються всі документи. Вони можуть містити як відкриту інформацію, так і конфіденційну, яку потрібно захистити від несанкціонованого доступу.

В якості зразка в роботі використовується USB-флеш накопичувач, обраний на основі аналізу всіх, в тому числі актуальних, носіїв інформації розглянутих у 1 розділі дипломної роботи. Об’єм пам’яті становить 32 Гб. Вона включає 28 Гб для віртуального диску та 4 для загального. Цієї пам’яті достатньо для зберігання великої кількості документів. Не використовуються носії з великим об’ємом, щоб мінімізувати можливість викрадення флешки сторонньою людиною. Сам носій повинен мати не занадто визначні видимі характеристики для середньо-статистичного користувача.

Носій повинен бути захищений в різних аспектах. Зовні не будуть використані додаткові засоби захисту у вигляді перевірки відбитку, привабливого або надмірно захищеного корпусу. Ці засоби необхідні для підвищення шансів повернення накопичувача у разі випадкового залишку його у громадських місцях, наприклад в офісі або в ресторані.

Носій не повинен привертати уваги та викликати спокусу залишити його собі стороннім, незнайомим людям. Такий зовнішній вигляд та об’єм видимої пам’яті полегшує, збільшує імовірність повертання у разі загублення.

Розглянутий у 2 розділі програмний засіб ACE призначений для шифрування даних. У цьому методі зашифровані файли та ключ зберігаються в спеціально визначеній папці. ACE надає загальне представлення програми для захисту інформації на зовнішньому носії. На сьогоднішній час це вже застарілий,

неактуальний метод, що має занадто багато недоліків. У результаті використання плагіну на носії залишається файл, що неможливо відкрити після завершення роботи ACE. Проте наявність цього файлу можна побачити на носії, змінити його назву та навіть видалити цей документ. В ній представлено проблеми, які виправлені у запропонованій роботі. На думку автора цієї роботи, найголовніша проблема полягає в зовнішніх ознаках програми ACE на флешці.

На носії існує папка ACE, для роботи необхідний файл запуску програми, а під час використання наявний ще один провідник (відмінний від стандартного) та ярлик управління. Метою створення методу являється уникнення(видалення) зовнішніх ознак наявності секретної інформації на накопичувачі для звичайного користувача, який нічого не знає про інформацію, що містить пристрій.

Складові системи контролю/управління доступу до віртуального захищеного диску (ВЗД):

- ВЗД
- Загальний розділ/диск
- Контролер управління доступу
- Алгоритм надання доступу системі до файлів на ВЗД

Контролер управління доступу - програмний код, що перевіряє відповідність ключів та на основі їх ідентичності визначає які права надані користувачеві або системі та з якими розділами можливо працювати.

Цей метод управління доступом до ВЗД складається з наступних етапів:

1) Розпізнавання зовнішнього накопичувача ОС
2) Запуск плагіну перевірки ключів
3) Перевірка умов виконання надання доступу до ВЗД
4) Визначення атрибуту ВЗД
5) Надається доступ, якщо умови виконані
6) Доступ заборонений, якщо умови не дотримані.

Під час роботи з накопичувачем можливі два стани системи контролю доступу о ВЗД: доступ авторизовано та не авторизовано

Правила надання доступу:

Процес доступу при авторизованому та не авторизованому стані відрізняється один від одного завдяки існуванню віртуального диску на носії (Рисунок 4.1).

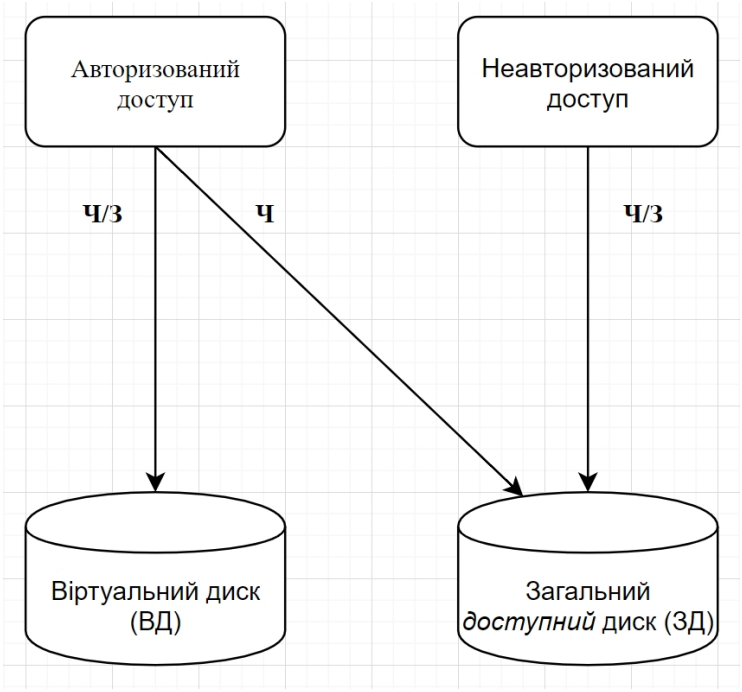


Рисунок 4.1 – Загальна блок-схема роботи системи надання доступу користувачеві до розділів диску

Система контролю доступу надає можливість читання/запису (Ч/З) при авторизованому стані користувачам з файлами на віртуальному диску. У цьому випадку користувач отримує доступ до віртуального диску, на якому зберігаються конфіденційні файли та може працювати з ними.

Під час неавторизованого доступу користувач взагалі не бачe віртуального диску в наявності, але може вільно працювати з документами на загальному диску.

Важливим обмеженням під час авторизованого стану являється на запис в загальному диску. Можливо читати файли та видаляти їх, але не виконувати запис. Це зроблено для того, щоб запобігти випадковому або навмисному перенесенню чутливої конфіденційної інформації з віртуального диску на загальний.

Для зручності можна розробити варіант, при якому наданий повний доступ на читання та запис до всіх розділів під час авторизованого режиму. У цьому випадку можна переносити файли з одного диску на інший, проте з’являється ймовірність збереження конфіденційної інформації у відкритому загальному розділі.

### *4.2 Алгоритм надання доступу*

Загальна система контролю доступу (Рисунок 4.2) згідно з даним методом включає: зовнішній носій інформації, процеси аутентифікації та авторизації користувача, віртуальний та загальнодоступний диск з їх файловими системами і даними та загальний інтерфейс роботи з накопичувачем.


Рисунок 4.2 – Логічна структура алгоритму роботи зовнішнього носія з ВЗД

*Аутентифікація.* При під’єднанні носія до пристрою відбувається перевірка прав доступу до віртуального захищеного диску. На цьому кроці перевіряється ідентичність ключів на віртуальному та загальному дисках.

*Авторизація.* В залежності від результату аутентифікації користувач отримує доступ або тільки до загального диску, або має змогу взаємодіяти з двома розділами флеш-носія.

*Файлова система ВЗД.* У 2 розділі проведений аналіз актуальних на сьогодні файлових систем. На основі цього аналізу можна зробити висновок, найдоцільнішою файловою системою в рамках дипломного проекту бажано використовувати FAT 32. Вона добре зарекомендувала себе за довгий час її використання. Наразі існує надзвичайно велика кількість документації щодо роботи з нею, що полегшує її модифікацію. FAT відмінно підходить для накопичувачів з порівняно невеликим об’ємом пам’яті.

*Інтерфейс.* Забезпечує взаємодію з інформацією на дисках. Працює відповідно до результатів ідентифікації.

На підставі проведеної аутентифікації користувач отримує різний рівень доступу до томів накопичувача. Якщо аутентифікацію не пройдено, користувач може бачити доступ лише до загального диску. У цьому випадку для нього флешка не має ніяких особливостей або ознак додаткового захисту.

У разі успішного проходження перевірки, користувач має доступ до загального диску (тільки читання та можливості видалення файлів) та віртуального захищеного з повним інструментом дій з конфіденційними файлами на розділі, крім можливості переносити або копіювати дані на загальний диск.

Даний метод забезпечує візуальний захист даних від несанкціонованого доступу. Тобто захист відмінно працює для середньостатистичного користувача, який не знає про наявність віртуального диску. Так як, технології все більше та більше розвиваються, існують програмні заходи, що можуть знайти цей ВЗД.

Етапи визначення надання прав доступу на читання та запис до розділу на носії інформації з ВЗД (Рисуноки 4.3 та 4.4):

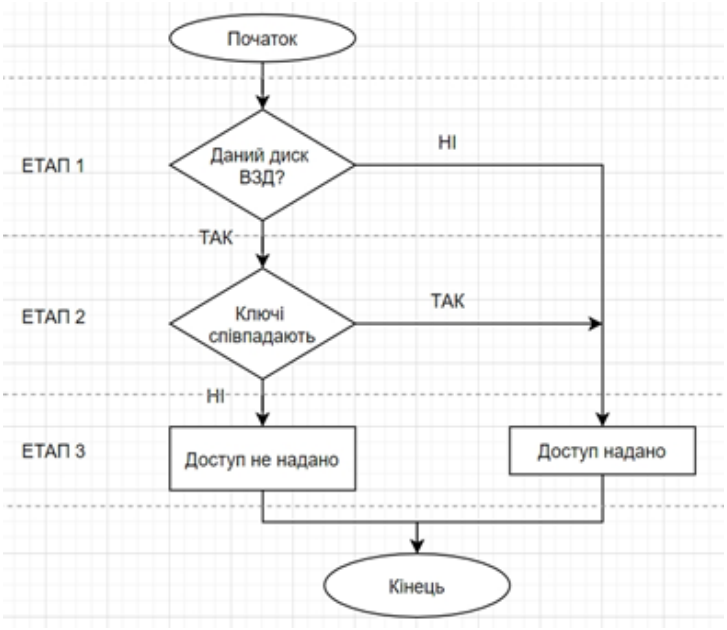


Рисунок 4.3 – Алгоритм визначення надання прав доступу на читання до розділу на накопичувачі інформації з ВЗД

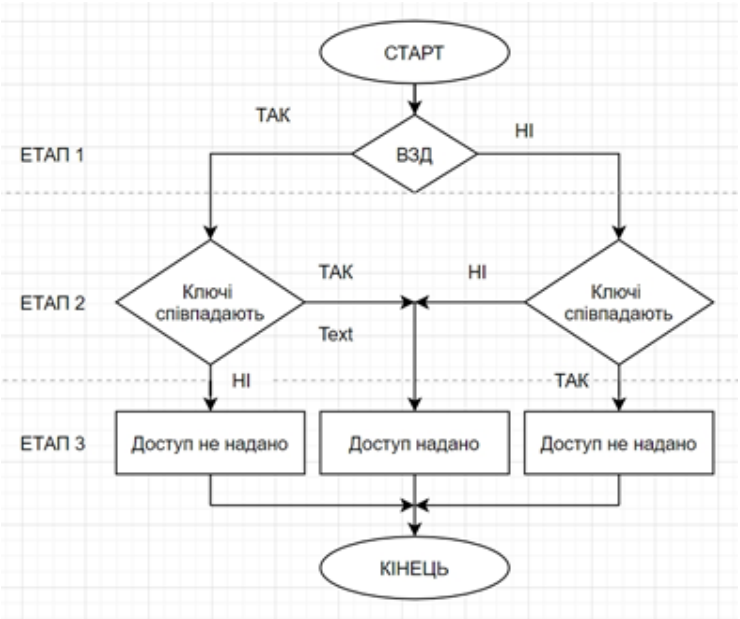


Рисунок 4.4 – Алгоритм визначення надання прав доступу на запис до розділу на накопичувачі інформації з ВЗД.

При визначенні прав доступу на читання на накопичувачі інформації з ВЗД напершому етапі визначається, до якого з розділів йде запит: до віртуального захищеного розділу, чи до загально-доступного простору. У разі, якщо користувач намагається прочитати інформацію на відкритому диску, йому будуть доступні файли на ньому. Під час роботи з ВЗД на другому етапі проводиться перевірка ідентичності ключів на диках. У випадку проходження перевірки ВЗД доступний користувачеві на читання, як і відкритий диск. Якщо ключі не співпадають користувач візуально спостерігає лише один доступний диск з відкритою інформацією. Користувач має права доступу на читання до явного диску завжди.

Визначення прав доступу на запис має додаткові нюанси для простору з відкритою інформацією. У цьому випадку так само відбувається перевірка до якого з розділів йде запит. Для отримання можливості створювати, видаляти, редагувати файли на ВЗД необхідно мати ідентичні ключі. При наданому доступі на запис на ВЗД можливі два принципи роботи відкритого доступу:

- відкритий диск не має обмежень та можливі всі функції, включаючи копіювання файлів;

- у режимі редагування ВЗД відкритий диск не доступний для редагування повністю або має ряд обмежень. У такому випадку можливо визначити сукупність функцій, що можу бути недостуні користувачеві від простого обмеження копіюваня з ВЗД до повної заборони будь-яких змін відкритого диску.

Другий режим роботи призначений для зниження імовірності збереження конфіденційної інформації на відкритому розділі.

У загальному принципи розподілення доступу до дисків можливо сформувати в наступні етапи:

Етап 1: надання доступу та вид доступу до файлів на розділі залежить перш за все від типу розділу, на якому вони зберігаються.

Етап 2: перевірка ідентичності ключів на ВЗД та звичайному диску.

Етап 3: в залежності від результатів другого етапу система надає доступ на читання до файлів на розділу диску.

### *4.3 Робота ключів*

При під’єднанні носія до комп’ютера, одним з перших плагінів запускається перевірка ключів на ВЗД та звичайному загально-доступному розділі. Цей процес відбувається до представлення інтерфейсу користувачеві.

Нехай ВЗД має ім’я “X”, а загальний - “F”. На ВЗД створена тека “KEY” за замовчуванням. Під час аутентифікації відбувається перевірка ідентичності вмісту папок “KEY” на ВЗД та на диску “F”. Вміст папки “KEY” може бути представлений у вигляді файлу з розширенням docx зі словом “Пароль” або сукупністю різних файлів. У такому разі збільшується варіативність ключа, адже це може бути текстовий документ, зображення або якийсь програмний файл. Варіативність наближається до нескінченності.

Якщо він різний (розмір, розширення, тип, тощо…), розділ “X” отримує атрибут системний/прихований і користувач взаємодіє лише з диском “F”. Він має доступ на читання та запис лишен на загально-доступний диск. ВЗД у цьому разі прихований та відсутні будь-які ознаки його існування.

Після вдалого проведення аутентифікації користувач може працювати з двома розділами. Проте, для загального диску він має лише право на читання, а для ВЗД - читання та запис. Це зроблено для зменшення ймовірності випадкового перенесення секретної інформації на загальний, не захищений розділ.

Для приховування ВЗД під час наступного підключення носія необхідно видалити теку “KEY” з розділу “F”. Перевірка ключів відбувається лише при під’єднанні носія до зчитувального пристрою.

Виключення з правил (особливі випадки роботи ключів):

- Запуск носія відбувається вперше та відсутні будь-які файли на ВЗД та “F”, тоді доступ надається, так як вміст однаково пустий: немає файлів на загальному диску та папка “KEY” на ВЗД також абсолютно порожня. Користувач може створити будь-який файл-пароль для аутентифікації під час наступного використання носія.

- Відсутність теки “KEY” на розділі “F”, якщо на ВЗД вже існує файл-пароль також відноситься до випадків провалення аутентифікації.

- Власник флешки забув, втратив який файл був використаний у якості паролю. Для забезпечення доступу в цьому разі можна використати додаткову/запасну/резервну перевірку. Це може бути запам’ятовування системних характеристик комп’ютера. Створення білого списку носіїв, на яких ВЗД доступний завжди відкритий. Для цього необхідно мати окрему папку, де міститься інформація про дозволені пристрої. Розробка додаткових алгоритмів перевірки доступу, дозволених пристроїв вимагає більш детального опису, розробки, проте наразі це не є головною задачею кваліфікаційної роботи.

### *4.4 Повне видалення ключа*

Під час звичайного видалення зникає лише посилання на файл, перші біти, що вказують на наявність вмісту, проте сам зміст залишається незмінним. Повне видалення можливе при перезапису комірок накопичувача. Це стає причиною вагомої проблеми - можливість відновлення файлів сторонніми програмами.

На загальному диску користувач може задіяти програму такого типу та відновити теку “KEY”, таким чином отримати доступ до ВЗД під час наступного підключення. Постає питання повного видалення файлів на накопичувачі. Для вирішення цієї проблеми наразі автор цієї роботи пропоноує наступні варіанти дії для запобігання відновлення паролю:

1) Повне форматування носія кожного разу перед припиненням роботи. Так як, накопичувач призначений для забезпечення захисту інформації, майже всі документи зберігаються на ВЗД. Повне форматування забезпечує функцію видалення так званих “слідів” паролю. У такому разі на загальному диску незручно зберігати додатково файли та об’єм пам’яті з кожним форматуванням по-трішки скорочується. Проте, навіть з таким зменшенням носій можна буде використовувати достатньо довгий час. Для забезпечення сталості об’єму можна інколи використовувати перерозподіл пам’яті.

2) Використання сторонніх програм. На сьогоднішній час існує багато додатків як для відновлення, так і для повного видалення документів. Прикладом таких програм може бути алгоритм роботи Ccleaner, Eraser, File Shredder, тощо. Такі програми можна легко знайти в Інтернеті, задавши пошуковий запит “надійне видалення файлів”.

3) Логічне зміна/генерування паролю. Достатньо важко повністю видалити документ зі 100 відсотково впевненість неможливості відтворення. Вирішенням проблеми може бути створення алгоритму, що не дозволяє використовувати відновлені файли для проходження аутентифікації знову. Основна ідея полягає в наступному: назва папки, що містить пароль повинна бути загальна, непримітна, на приклад, “Todolist_day_month” або “Myplans_day_month”, тощо та замість “_day_month” використовувати генеровувану на поточний момент дату. Тобто, під час перевірки необхідно, щоб вміст папки “KEY” на ВЗД був ідентичним до вмісту папки “Myplans_23March”. У такому разі відновлений файл матиме стару недійсну дату та ключ буде не дійсним. Для стороннього користувача дана тека буде достатньо звична. Сумніви або домисли щодо існування ВЗД будуть відсутні. Це один з варіантів вирішення задачі. Він потребує більш детального опису та розробки, та поки що це другорядне завдання.

Одним з вагомих особливостей, інструментів забезпечення безпеки інформації являється непримітність носія.

По перше, немає ніяких додаткових вікон, запитів, що вимагають введення паролю та відсутні провідники з відмінного від системного, інтерфейсом. Якщо стороння людина відкриє флешку на своєму комп’ютері, то в нього не буде ніяких підозр, що він використовує спеціальний запам’ятовуючий пристрій з секретною інформацією.

По друге, зовні флешка не повинна мати якихось особливостей будови чи великого об’єму пам’яті на загальному диску. Вона не повинна мати якісь додаткові механічні засоби захисту, особливості будови чи дизайну. При підключенні спостерігається порівняно малий об’єм пам’яті в 4 Гб. Психологічно, флешка не надто приваблива та не надто цінна на перший погляд.

У першому розділі розглянуто загальні категорії користувачів комп’ютерною технікою. Метод захисту інформації даної дипломної роботи розрахований на захист даних від несанкціонованого доступу користувачів, рівень яких сягає впевненого користування. Технічна частина захищає від користувачів, які відносяться до впевненої категорії користування. Проте у деяких випадках психологічні методи захисту інформації можуть знизити ймовірність розкриття даних на ВЗД від користувачів високого рівня. Тобто, завдяки програмним заходам можливо віднайти документи, але лише у випадку, якщо несанкціонований користувач вирішить, що носій має цінність та захоче його перевірити. Звісно, це не захищає накопичувач у повну міру, проте зменшує шанси на розкриття конфіденційної інформації.

### *4.5 Людський фактор*

Надзвичайно важливу роль при захисті даних відіграє людський фактор. На жаль, дуже складно розробити метод, який повністю допоможе запобігти витоку інформації через людську помилку. У даній роботі автор пропонує деякі інструменти, щоб уникнути цього:

- віртуальний захищений диск, який доступний тільки при авторизації;
- відсутність візуальних ознак існування захищеного розділу при звичайному режимі використання;
- неможливість копіювання інформації на відкритий диск в захищеному режимі;
- мінливість ключа при відкритті носія (при додаткових заходів захисту від відновлення даних);
- непомітність носія і його характеристик (для підвищення шансу повернення носія в разі втрати).

***Висновки за розділом 4***

У результаті аналізу та розгляду різних інструментів захисту у цьому розділі детально розписано основні нюанси роботи методу захисту інформації на зовнішньому накопичувачі за допомогою зберігання даних на віртуальному захищеному розділі. Дані заходи забезпечують виконання властивостей:

Конфіденційності - так як інформація зберігається на ВЗД, доступ до неї має лише людина, яка точно знає про її наявність. Випадковий користувач при відкритті носія не побачить нічого незвичайного та не матиме підозр щодо існування секретної інформації. При використанні ВЗД документи неможливо скопіювати на загальний диск, що зменшує імовірність випадкового розкриття секретної інформації.

Доступності - таємна інформація зберігається на окремому віртуальному розділі, доступ до якого можливий лише при використанні ключа. Цей ключ має надзвичайну велику варіативність, адже це може бути файл або сукупність будь-якого формату. Підібрати ключ надзвичайно важко.

Цілісність - працювати з файлами на ВЗД можливо після проходження авторизації. Якщо доступ не надано, користувач не може взаємодіяти з ними, ні їх бачити, чи редагувати або знищувати. Під час форматування флеш-носія, процес відбувається лише із загальним розділом.

# ВИСНОВКИ

У дипломній роботі розроблений та описаний метод зберігання інформації на зовнішньому носії інформації з покращеним рівнем виконання властивостей безпеки інформації. В ході аналізу, розробки, розв’язанні поставлених задач були отримані наступні наукові та практичні результати:

1. Проведено аналітичний огляд різних типів зовнішніх накопичувачів. Виявлено та обрано найактуальніший та зручніший портативний носії для захисту інформації.

2. Запропонована узагальнена класифікація користувачів комп’ютерної техніки. Надані основні характеристики кожного типу користувача.

3. Розглянуто та проаналізовано найбільш поширені та актуальні файлові системи. Визначена найбільш придатна система для використання у розробці методу захисту даних.

4. Проаналізовано поширені на сьогоднішній час інструменти та програми забезпечення захисту інформації на носіях. На основі проаналізованих програм сформовано набір/складових для забезпечення захисту інформації на зовнішніх носіях.

5. Розроблено систему заходів забезпечення високого рівня властивостей безпеки інформації на зовнішньому портативному носії. Обґрунтовано актуальність та доцільність створення подібного пристрою з новим методом роботи носія.

6. Створено логічний алгоритм роботи носія з віртуальним захищеним диском. Описаний кожний етап роботи носія з віртуальним диском.

7. Визначені аспекти методу, які потребують доопрацювання. Запропоновано сценарії вирішення проблеми відновлення паролю на зовнішніх носіях.

У кваліфікаційній роботі всі поставлені завдання досягнено.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12

2. Закон України «Про технічний та криптографічний захист інформації»: [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

3. Проект Концепції інформаційної безпеки України [Електронний ресурс]. - Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15. pdf.

4. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99 [Електронний ресурс]. - Режим доступу: https://tzi.com.ua/downloads/1.1-003-99.pdf

5. Браіловський М.М., Ткаченко А.С. Захист та приховування інформації в графічних та мультимедійних об'єктах на базі стеганотехнологій. // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 05-06 квітня 2018 року; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова)та ін. К.: ВПЦ «Київський університет», 2018. – 510 с. С.444-447.

6. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей тез; м. Київ, 12 червня 2020 року; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2020. – 368 с. С. 69-72.

7. Воройский Ф. С. Інформатика. Новый систематизированный толковый словарь-справочник. - 3-е изд. - М .: ФИЗМАТЛИТ, 2005. - 760 с.

8. Ross Anderson. Security Engineering. Wiley, 2001. - 640 p.

9. Айков Д., Сейгер К., Фонсторх У. Компьютерні злодії: Пер. с англ. - М.: Мир, 1999. - 351 с.

10. Апін Б. Ю. Захист компьютерної інформації. - СПб.: БХВ - Київ, 2000. - 384 с.

11. Єфімов О.М. Інформаційний вибух: проблеми реальні та вигадані. - М .: Наука, 2004. - 159 с.

12. Алексеєнко В.М., Сокальський Б.В. Система захисту комерційних об'єктів. Технічні засоби захисту. М., 2010. - 94 с.

13. Барсуков В.С. Забезпеченні інформаційної безпеки. - М: ПЕК, 2005.

14. Безруков М.М. Компьютерная вірусологія. - М .: УРЕ, 2007.-416 с.

15. Герасименко В.А. Захист інформації в автоматизованих системах обробки інформації. 2 кн. М .: Вища школа, 2004

16. Грушо А.А, Тимонина Є.Є. Теоретичні основи захисту інформації . -М: Видавництво Агентства «Яхтсмен». 2006. – 192 с.

17. Мельников В.В. Защита информации в компьютерных системах. - М: Фінанси і статистика; Електронінформ, 2003. - 368 с.

18. Пілюгін П.Л. Общие вопросы зашиты вычислительных систем и особенности защиты персональных компьютеров: Курс лекцій. - М .: ІКСІ, 2003. - 84 с.

19. Спесивцев А.В., Вегнер В.А., Крутяк А.Ю. Защита информации в персональных ЭВМ. – М.: Радио и связь; МП «Веста», 2002. – 192 с

20. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. - М: Сов. радио, 1980.

21. Щербаков А.Ю. Защита от копирования. – М.: Эдэль, 2002

22. Варлатай С. Программно-аппаратная защита информации: учеб. пособие/ С. Варлатай, М. Шаханов. — Київ: ДВГТУ, 2007.

23. Белкин П. Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных/ П. Ю. Белкин, О. О. Михальський, А. С. Першаков. - М.: Радио и связь, 2005. - 168 с.

24. Гундарь К. Ю. Защита информации в компьютерных системах/ К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский. – К.: Корнійчук, 2008. – 152 с. 6. Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты/ В. В. Домарев. - К.: ООО ТИД ДС, 2001. - 688 с.

25. Антонюк А.О. Основи захисту інформації в автоматизованих системах/ А. О. Антонюк. – К.: КМ Академія, 2006. – 244 с.

26. Михайлов С. Ф. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. Основные концепции: учеб. пособие / С. Ф. Михайлов, В. А. Петров, Ю. А. Тимофеев. — М .: МИФИ, 2003. — 182 с.

27. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. — СПб. : Питер, 2008. — 320 с.

28. Петренко А. Б. Протидія витоку інформації через з'ємні носії в автоматизованих системах /А. Б. Петренко, Е. В. Бєтанов // Інформатика і комп'ютерні технології:VII міжнародна наук.-техн. конф.: зб. праць. — Донецьк : ДонНТУ, 2011. — С. 259—260.

29. Бетанов Е. В. Противодействие потере информации через USB носители: зб. тез VIII Міжнародно-технічної конференції студентства та молоді «Світ інформації та телекомунікацій-2010». — Київ, 27-28 квітня 2011 р. — 160 с.

30. Офіційний сайт підтримки програмного забезпечення ACE APACER [Електронний ресурс]. – Режим доступу: http://ace.apacer.com/index.asp.

31. Задирака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник. – Київ; Тернопіль: Підручники і посібники, 2007. – 272 с.

# ДОДАТОК А

## Тези наукових доповідей

1. Volodymyr Nakonechnyi, Yevgenii Zakharchenko. Methods to increase the effectiveness of protection of external media from unauthorized access and modification. VIII International conference «Information Technology and Implementation (Satellite)» (IT&I-2021)- Taras Shevchenko National University of Kyiv, December 1-2, 2021.