МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"

УДК 681.3.06

«До захисту допущено»

Завідувач кафедри

_____ Шуклін Г.В.

(підпис) (ініціали, прізвище)

“____” _____ 2022р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

на тему: **МЕТОД НАДІЙНОГО ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ, ЯКА ЗБЕРІГАЄТЬСЯ НА МАГНІТНИХ НОСІЯХ**

Студентка групи СЗЗМ – 71 Самсоненко Світлана Дмитрівна

(підпис)

Керівник д.т.н., доц. Ахрамович Володимир Миколайович

(підпис)

Нормоконтроль: ст. викладач Гребенніков Асаді Болдгоягович (підпис)

Київ – 2022

ЗАТВЕРДЖУЮ
Завідувач кафедри СІТКЗ
_____ Г.В. Шуклін
“___” _____ 2022 року

З А В Д А Н Н Я

НА АТЕСТАЦІЙНУ РОБОТУ СТУДЕНТУ

САМСОНЕНКО Світлані Дмитрівні
(прізвище, ім’я, по батькові)

1. Тема магістерської роботи: «Метод надійного захисту цифрової інформації, яка зберігається на магнітних носіях»
керівник магістерської роботи _Ахрамович Володимир Миколайович, д.т.н., доцент
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від « 16 » лютого 2022 року № 22

2. Строк подання студентом атестаційної роботи 30 травня 2022 року.

3.Вихідні дані до атестаційної роботи накопичувач на жорсткому магнітному диску (НЖМД).

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1) Проаналізувати роль та місце накопичувачів на жорсткому магнітному диску у загальній класифікації цифрових носіїв інформації, їх призначення та об. застосування;
2) Дослідити архітектуру побудови накопичувачів на жорсткому магнітному диску;
3) Дослідити методи безпечного зберігання та надійного знищення інформації з обмеженим доступом на магнітних носіях цифрової інформації.
4) Проаналізувати роль та місце накопичувачів на жорсткому магнітному диску у загальній класифікації цифрових носіїв інформації, їх призначення та об. застосування;
5) Дослідити архітектуру побудови накопичувачів на жорсткому магнітному диску;

5. Перелік графічного матеріалу
1. Загальна класифікація носіїв інформації.
2. Характеристики та властивості цифрових носіїв інформації

3. Структурно-модульна схема НЖМД.
4. Методи атак на жорсткі диски
5. Методи захисту
6. Методи знищення інформації
7. Налаштування BitLocker та шифрування диску.

6. Дата видачі завдання_____02.03.2022р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів роботи	Примітка
1	Підготовка і вивчення літератури	10.03.2022	виконано
2	Написання та оформлення 1 розділу	До 04.04.2022	виконано
3	Написання та оформлення 2 розділу	До 25.04.2022	виконано
4	Написання та оформлення 3 розділу	До 06.05.2022	виконано
5	Перевірка роботи на плпгіат + попередній захист	До 01.06.2022	виконано
6	Захист роботи	13.06.2022	
7	Випуск	30.06.2022	

Студент _____ Самсоненко С.Д.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Ахрамович В.М.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина дипломної роботи: 84 сторінки, 15 рисунків, 7 таблиць, 19 джерел.

Об’єкт дослідження: Сучасні магнітні носії цифрової інформації.

Предмет дослідження: Методи безпечного зберігання та надійного знищення інформації з обмеженим доступом на магнітних носіях цифрової інформації.

Мета роботи: Дослідження впливу акустичного сигналу на цілісність інформації на жорстких дисках, пошук ефективних методів безпечного зберігання та надійного знищення інформації з обмеженим доступом на магнітних носіях цифрової інформації.

Для досягнення означеної мети необхідно вирішити такі окремі завдання:

1) Проаналізувати роль та місце накопичувачів на жорсткому магнітному диску у загальній класифікації цифрових носіїв інформації, їх призначення та область застосування;

2) Дослідити архітектуру побудови накопичувачів на жорсткому магнітному диску;

3) Дослідити методи безпечного зберігання та надійного знищення інформації з обмеженим доступом на магнітних носіях цифрової інформації.

Методи дослідження: З метою досягнення мети та розв’язання поставлених задач були застосовані загальнонаукові методи дослідження: емпіричні (*спостереження та експеримент*), теоретичні (*аналіз, класифікація та узагальнення*).

В роботі проаналізовано архітектуру побудови, методи запису інформації на НЖМД, актуальні методи атак на ЖД. Надано рекомендації щодо використання датчиків реагування, повного шифрування даних. Розглянуто методи знищення інформації на ЖД. Сформована та реалізована методика шифрування ЖД

Сфера застосування: Результати виконання окремих завдань можуть бути використані для розроблення програмних та програмно-апаратних рішень покращення захисту інформації на жорстких дисках.

Ключові слова: ІНФОРМАЦІЯ, ЦИФРОВІ НОСІЇ, БЕЗПЕЧНЕ ЗБЕРІГАННЯ.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1 ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ 9
1.1. Основні поняття та визначення 9
1.2. Класифікація цифрових носіїв інформації, їх призначення та область застосування 11
1.3 Роль та місце накопичувачів на жорсткому магнітному диску у загальній класифікації цифрових носіїв інформації 22
Висновки до розділу 1 24
РОЗДІЛ 2 ПОБУДОВА ТА ВЛАСТИВОСТІ НАКОПИЧУВАЧІВ НА ЖОРСТКОМУ МАГНІТНОМУ ДИСКУ 25
2.1. Архітектура НЖМД 25
2.1.1. Технічні характеристики НЖМД 27
2.1.2. Різновиди жорстких дисків 33
2.1.3. Технології запису та зберігання інформації 39
Висновки до розділу 2: 45
РОЗДІЛ 3 НАДІЙНЕ ЗБЕРІГАННЯ ТА ЗНИЩЕННЯ ІНФОРМАЦІЇ НА МАГНІТНИХ НОСІЯХ ЦИФРОВОЇ ІНФОРМАЦІЇ 46
3.1. Методи атак на жорсткі диски 46
3.2. Методи захисту жорстких дисків 48
3.2.1. Метод шифрування для захисту ЖД 51
3.2.2 Практична реалізація методу шифрування 54
3.3. Методи знищення інформації на жорстких дисках 60
3.3.1 Програмні методи стирання інформації 62
3.3.2 Руйнуючі методи знищення інформації 64
Висновки до розділу 3: 69
ВИСНОВКИ 70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 72

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

КД- компакт-диски

МіБ- мебібайт

НЖМД – накопичувач на жорстких магнітних дисках

ЖД – жорсткий диск

ПЕОМ – периферійна електро-обчислювальна машина

ПЗ – програмне забезпечення

КК – кредитні картки

ПК – персональний комп’ютер

ROM – постійна пам’ять

PROM – постійна програмована пам’ять

EEPROM – електрично-перепрограмувальна постійна пам'ять

RAM – оперативна пам'ять

ВСТУП

На сьогоднішній день рішення проблеми інформаційної безпеки вже розглядаються на державному рівні, що підтверджується нормативно-правовими і організаційними документами. В Україні на цей час діє три Закони України: «Про електронні документи і електронний документообіг» , який встановлює основні організаційно-правові принципи електронного документообігу і використання електронних документів; «Про електронний цифровий підпис», який визначає правовий статус електронного цифрового підпису та регулює взаємовідносини, які виникають при використанні електронного цифрового підпису та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює взаємовідносини в області захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Одним із важливих аспектів сучасного інформаційного простору є спеціальні цифрові носії інформації, що широко використовуються в наш час.

Важко перелічити всі відомі на сьогоднішній день області застосування жорстких дисків. В основі технології таких носіїв інформації лежать сучасні розробки мікроелектроніки, фізики, прикладної математики, криптографії та суміжних галузей, однак механізми захисту не досконалі і потребують розроблення рекомендацій щодо механізмів захисту інформації.

РОЗДІЛ 1 ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ

1.1. Основні поняття та визначення

Для точного введення визначень «цифрові носії інформації», назв типів цифрових носіїв та інших понять, які стосуються технологій їх побудови та методик застосування доцільно навести терміни, які встановлені діючим в Україні законодавством та нормативними актами Ради Євросоюзу. Історично першими були європейські тлумачення понять, які спочатку використовувались в електронному документообігу та інших сферах застосування інформаційних технологій сучасності. У подальшому, із стрімким розвитком та впровадженням інформаційних технологій в нашій державі, прагненням України до інтеграції у єдиний європейський інформаційний простір, Директивою Ради Європи та українським законодавством були встановлені для використання єдині поняття та визначення у цій сфері діяльності.

Наведемо та з’ясуємо суть цих понять та визначень.

Цифровий носій інформації **–** це будь-який носій, який закодований в машиночитаючому форматі. Цифрові носії можна створювати, переглядати, розповсюджувати, змінювати та зберігати інформацію на пристроях цифрової електроніки. Цифрова інформація може бути визначена як будь-які дані, що представлені послідовністю цифр.

Гнучкий магнітний носій інформації – це пристрій для зберігання невеликих обсягів інформації, що являє собою гнучку пластикову пластину із нанесеним на неї шаром речовини, що реагує на зовнішнє магнітне поле, в захисній оболонці. Використовується для перенесення даних з одного комп'ютера на інший та для розповсюдження програмного забезпечення.

Жорсткий магнітний носій інформації - енергонезалежний комп'ютерний пристрій, що перезаписується. Є основним накопичувачем даних у всіх сучасних комп'ютерах.

Оптичний диск - оптичний носій інформації у вигляді пластикового диска з отвором у центрі, процес запису та зчитування інформації з якого здійснюється за допомогою лазера**.**

Смарт-картка - пластикові картки із вбудованою мікросхемою. У більшості випадків смарт-карти містять мікропроцесор та операційну систему, що керує пристроєм, та контролює доступ до об'єктів у його пам'яті.

Флеш-носій - електронний запам'ятовуючий пристрій, що використовується як носій (накопичувач) інформації. Флеш-носій підключається до комп'ютера або іншого зчитувального пристрою за інтерфейсом USB.

Електронний документ - документ, інформація в якому зафіксована у вигляді електронних (цифрових) даних, включаючи обов'язкові реквізити документа.

Електронний цифровий підпис - унікальна цифрова інформація у вигляді комбінації символів. За допомогою цієї інформації можна дізнатися, хто саме та коли підписав документ. Таким чином, *електронний цифровий підпис* – це офіційний затверджений законом аналог власноручного підпису, який застосовується для підписання електронних та засвідчення паперових документів, перетворених на електронний формат.

Електронний підпис - це особливий реквізит документа, що дозволяє встановити відсутність у ньому спотворення інформації з формування ЕП і підтвердити приналежність ЕП власнику. Значення реквізиту виходить у результаті криптографічного перетворення інформації.

Механізм перевірки підпису - пристосоване програмне чи апаратне забезпечення, яке використовується для введення в дію даних для перевірки підпису.

Сертифікат - електронна атестація, яка пов'язує дані для перевірки підпису з особою і підтверджує ідентичність цієї особи. Наведемо терміни, які встановлені чинним законодавством України, зокрема Законом України «Про електронний документообіг» та Законом України «Про електронний цифровий підпис».

Однозначне розуміння суті базових понять, термінів та визначень надає можливість дослідження видів носіїв цифрової інформації, з’ясування технологій їх побудови, збереження даних та удосконалення методів захисту інформації, яка міститься на цих носіях. [1]

1.2. Класифікація цифрових носіїв інформації, їх призначення та область застосування

Носії інформації за методом зберігання та передачі інформації поділяються на аналогові та цифрові. До аналогових можна віднести: папір, магнітні стрічки, мікрофільми та металеві носії. В свою чергу цифрові носії інформації поділяються на: магнітні, оптичні та Flash-накопичувачі (рис. 1.1).

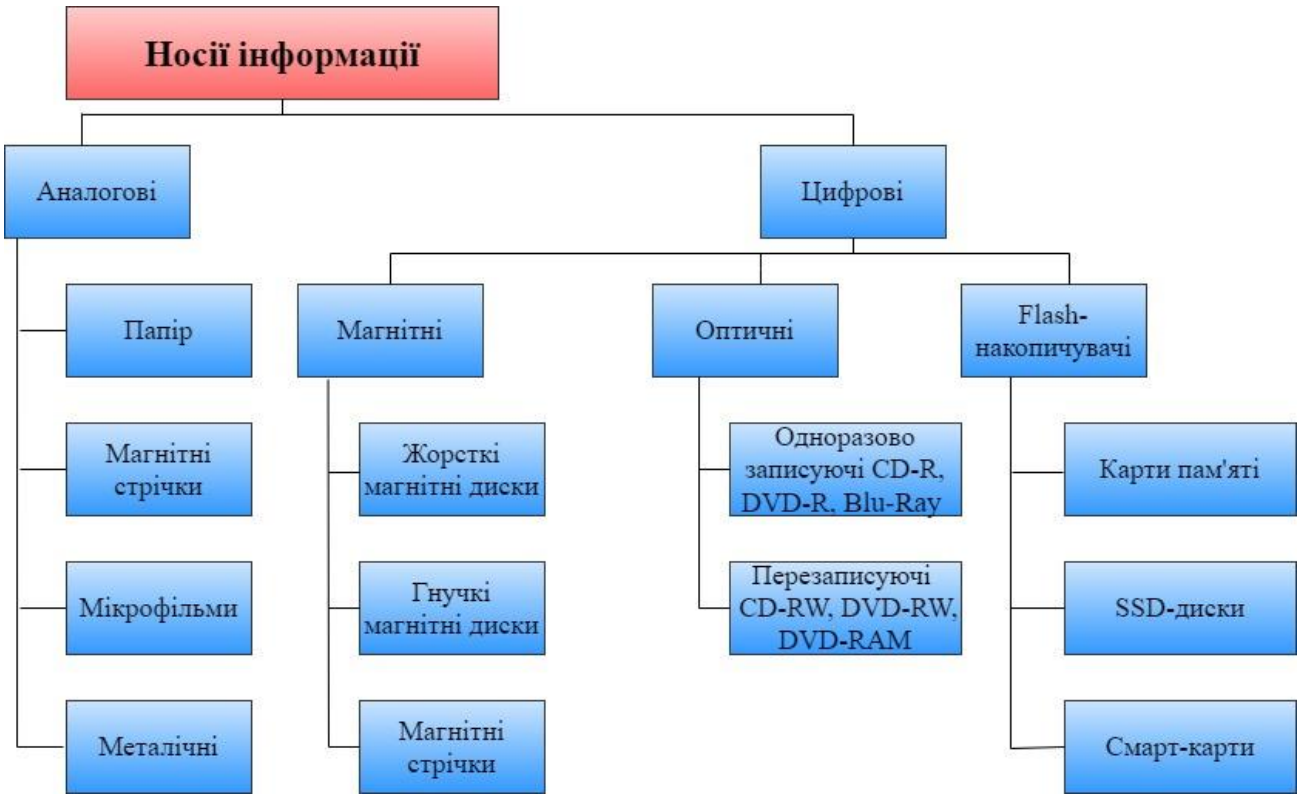


Рис. 1.1 – Загальна класифікація носіїв інформації

1.2.1. Магнітні диски

Гнучкі магнітні диски

Спосіб запису двійкової інформації на магнітному середовищі називається магнітним кодуванням. Метод полягає у вишиковуванні магнітних доменів в середовищі вздовж доріжок у напрямку прикладеного магнітного поля своїми північними та південними полюсами. Двійкова інформація встановлюється у однозначну відповідність до орієнтації доменів.

Кількість доріжок та секторів відповідна до типу та формату дискети. Сектор зберігає мінімальну кількість інформації, яка може бути записана/зчитана на/з диск(у). Місткість сектора постійна і становить 512 байт. На дискеті можна зберігати від 360 Кілобайт до 2,88 Мегабайт інформації

Найбільшого поширення набули дискети з такими характеристиками: діаметр - 3,5 дюйма (89 мм), ємність - 1,44 Мбайт, число доріжок - 80, кількість секторів на доріжках - 18.

Магнітні стрічки

Магнітна стрічка - це найпоширеніший знімний носій даних. Вони мають велику популярність. Є кілька переваг використання магнітних стрічок порівняно з іншими запам’ятовуючими пристроями.

У порівнянні з жорсткими дисками, магнітні стрічки економічні. Так само як ціни на жорсткі диски, ціни на магнітну стрічку постійно знижуються.

Організація зберігання магнітної стрічки в захищеному сховищі проста. Крім того, в цьому випадку дані будуть захищені від пошкодження комп'ютерними вірусами, стихійними лихами, некваліфікованими працівниками та іншими факторами такого роду.

Магнітні стрічки використовують також для резервного копіювання даних. Як тільки резервна копія втратить актуальність, магнітну стрічку можна використовувати повторно. Навіть якщо обсяг необхідних даних постійно збільшується, це не завжди вимагає закупівлі додаткових касет з магнітною стрічкою.

У той же час у магнітної стрічки є свої недоліки: магнітна стрічка допускає багаторазове використання, проте згодом потребує заміни. Якщо стрічка не буде замінена своєчасно, дані на ній можуть бути пошкоджені. Пошук конкретного об'єкта на стрічці може тривати тривалий час.

1.2.2. Оптичні диски

Історія походження та вдосконалення властивостей

Перший оптичний диск, розроблений наприкінці 1960-х Джеймсом Т. Расселом, зберігав дані у вигляді мікронних точок світла і темряви. Оптична система зберігання даних Рассела використовувала потужне підсвічування для зчитування точок через прозорий аркуш матеріалу, на якому були закодовані точки.

Хоча Расселу приписують розробку першого оптичного сховища, його творіння мало схоже на пізніші компакт-диски або DVD. Рассел використовував прозору фольгу як носій, а потім зчитував дані, просвічуючи через неї світло. Сучасні оптичні диски використовують лазер для зчитування світла, що відбивається від носія запису. Крім того, система Рассела не оберталася під час зчитування даних, тому вона могла мати будь-яку форму, а не просто диск.

Сучасні компакт-диски та DVD створені на основі технології, розробленої в 1969 році в Нідерландах фізиком Пітером Крамером під час роботи в Philips Research. Крамер розробив метод кодування даних на світловідбиваючій металевій фользі, яку можна було зчитувати за допомогою маленького малопотужного червоного лазера. Лазерна збірка зчитувала точки і перетворювала дані в електричний сигнал, який потім перетворювався на звуковий або візуальний вихід. Його робота стала основою всіх цифрових оптичних носіїв інформації, хоча спочатку вона використовувалася лише для аналогового відео на першому LaserDisc.

У 1970-х роках Philips об'єдналася з Sony у спільний консорціум, зосереджений на оптичному накопичувачі. У 1979 році вони розробили перший

аудіо компакт-диск, який ознаменував початок цифрового оптичного зберігання для комерційного використання. Однак ця технологія не отримала серйозного визнання, доки Philips і Sony не випустили перший комерційний програвач компакт-дисків у 1982 році. З тих пір існувала постійна послідовність форматів оптичних дисків, спочатку у форматах CD, а потім у ряді DVD. формати.

Через п’ять років після випуску програвача компакт-дисків Sony об’єднала зусилля з Denon, щоб виготовити перший компакт-диск для зберігання всіх типів цифрових даних, а не лише аудіо. Компакт-диск міг містити приблизно 680 МБ даних, які пізніше збільшилися до 700 МБ. Майже через 10 років після цього Sony знову об'єдналася з Philips, а також Toshiba і Panasonic, щоб створити DVD, який збільшив ємність даних до 4,7 ГБ.

Минуло ще 10 років, перш ніж наступне покоління оптичних накопичувачів, дисків Blu-ray, вийшло на ринок. Замість використання червоного лазера, диск Blu-ray використовує синій лазер, що значно збільшує ємність і швидкість передачі даних. Маючи пам’ять до 25 ГБ, Blu-ray був розроблений консорціумом, який знову очолювала Sony.

Цього разу Toshiba не брала участі, оскільки розробила та спробувала продати свій власний формат HD-DVD . Після короткої війни форматів Blu-ray став галузевим стандартом.

Таблиця 1.1 - Типи ємності оптичних дисків

Тип	Тривалість, хвилини	Сектор	Макс. розмір CD-DA		Макс. Розмір даних	
			байт	МіБ	байт	Міб
	21	94 500	22 264 000	212,0	193 536 000	184,6
	63	283 500	666 792 000	635,9	580 608 000	553,7
«650MB»	74	333 000	783 216 000	746,9	681 984 000	650,3
«700MB»	80	360 000	846 720 000	807,4	737 280 000	703,1
800MB	90	405 000	952 560 000	908,4	829 440 000	791,0
900MB	99	445 500	1 047 816 000	999,3	912 384 000	870,1

Як створюється диск:

- Перший етап полягає у підготовці даних для запуску в серію;
- Фотолітографія - другий етап, це процес створення штампу диска.

Оптичні диски недорогі у виготовленні. Усі сучасні формати використовують однакову базову структуру матеріалів. Тверда пластикова підкладка формує основу, а потім для кодування цифрових даних використовується світловідбиваючий шар - зазвичай алюмінієва фольга для дисків масового виробництва. Далі шар прозорого полікарбонату захищає фольгу і дозволяє лазерному променю проходити до відбиваючого шару.

Виробники можуть створювати попередньо записані аудіо та відео оптичні диски оптом. Вони також можуть створювати диски для розповсюдження програмного забезпечення та комп'ютерних ігор, хоча потокова передача через Інтернет зменшила потребу в таких типах дисків.

При масовому виробництві попередньо записаних дисків виробники спочатку створюють скляний майстер, а з цього майстра створюють негативне зображення диска з нікелю. Потім вони використовують це нікелеве зображення для фізичного штампування цифрових ямок у шарі відбивної фольги. Це дає можливість масового виробництва в масштабах, неможливих за допомогою індивідуального кодування оптичних дисків за допомогою лазера, як це відбувається, коли диск записується або записується на комп'ютері.

Оптичні диски, призначені для зберігання цифрових даних, містять різні матеріали для відбиваючого шару, залежно від того, чи диск можна записувати одноразово чи повторно. Оптичний диск із одноразовим записом містить шар органічного барвника між ненаписаною світловідбиваючою фольгою та полікарбонатом. Перезаписувані оптичні диски замінюють алюмінієву фольгу на сплав, який є матеріалом із зміною фаз, щоб його можна було стирати та перезаписувати кілька разів.

CD(компакт диск)

Оптичні диски, які використовують ту ж технологію, що й музика компакт-диски. Вони зберігають до 700 МБдані. Диски можна використовувати для мультимедіа додатків наприклад, енциклопедії, і може зберігати зображення, звуки та відеокліпи чи будь-що інше, що підійде.

Існує кілька форматів, наприклад:

- CD-ROM - тільки для читання, дані записуються на них перед продажем.
- CD-R - це означає, що можна записувати дані на компакт-диск, користувач може записувати дані на компакт-диск один раз або заповнювати його з часом, використовуючи багатосесії (запис на один і той же диск в окремих випадках).
- CD-RW - означає перезапис CD-диску, на компакт-диск можна записувати та перезаписувати. На відміну від багатосесійних дисків, наявні дані можна перезаписати.

DVD (цифровий універсальний диск)

DVD-диски мають такий самий фізичний розмір, як і компакт-диски, але містять набагато більше даних - односторонній диск може вмістити до 4,7 ГБ. DVD-диски зазвичай використовуються для зберігання відео, тому ви часто бачите, як вони вимірюються в хвилинах, наприклад, 4,7 ГБ = 120 хвилин.

Існує кілька форматів, наприклад:

- DVD-ROM - тільки для читання, дані записуються на них перед продажем.
- DVD-R - тобто DVD-Recordable, користувач може записувати дані на DVD один раз або заповнювати його протягом тривалого часу за допомогою багатосесії.

- DVD-RW - означає DVD-Rewritable, DVD можна записувати та перезаписувати. На відміну від багатосесійних дисків, наявні дані можна перезаписати.

Blu-Ray - найсучасніший оптичний носій

Blu-ray - це формат оптичних дисків, наприклад CD і DVD. Диски Blu-ray можуть зберігати більше інформації, ніж інші оптичні носії, через блакитні лазери, які використовують дисководи. Один диск Blu-ray може вмістити до 25 ГБ даних. Двошарові диски Blu-ray зможуть зберігати 50 ГБ даних, що еквівалентно 4 годинам HD-контенту. У 2010 році Blu-ray Disc Association (BDA) оголосила офіційні специфікації для нового формату дисків Blu-ray XL (BDXL), максимальна ємність якого становить 128 ГБ. [3].

1.2.3. Флеш-накопичувачі

На даний момент є безліч варіантів зберігання інформації, які з них вимагають постійного підживлення електрикою (RAM), якісь назавжди «вшиті» в керуючі мікросхеми техніки, що оточує нас (ROM), а якісь поєднують у собі якості і тих, та інших (Hybrid). До останніх, зокрема, належить flash. Начебто і енергонезалежна пам'ять, але закони фізики скасувати складно, і періодично на флешках перезаписувати інформацію таки доводиться.

Карти пам’яті

Карта пам'яті - це невелика платівка, в яку вбудований модуль флеш-пам'яті. Цей модуль є незалежним, тобто інформація на карті пам'яті зберігається навіть у той час, коли вона витягнута з будь-якого пристрою.

Інформацію на картці пам'яті можна видаляти, перезаписувати тощо. Термін служби картки пам'яті дуже великий - десятки років.

Види карт пам’яті:

SD (Secure Digital) - найпопулярніший вид карт пам’яті, що використовується у багатьох фотоапаратах, відеокамерах, планшетах, старих

плеєрах, комунікаторах та кишенькових комп'ютерах. Відрізняється невисокою ціною. Максимальний об'єм – 4Гб.

MiniSD **–** це аналог SD, але значно меншого розміру. У наші дні вже фактично не вживається, на зміну miniSD прийшов формат microSD.

MicroSD (TransFlash) **-** зараз займає друге місце за популярністю після SD/SDHC, але найближчим часом має всі шанси стати найпопулярнішим форматом карт пам'яті. Відрізняється від SD дуже невеликими розмірами; microSD-карти навіть менше ніж miniSD. Це і плюс і мінус: з одного боку, з появою microSD стало можливим зменшити габарити пристроїв; з іншого - таку мініатюрну картку легко втратити.

SSD-диски

SSD (твердотільні накопичувачі) – виконують майже ті ж функції, що і жорсткі диски, але для зберігання даних SSD використовують взаємопов’язані мікросхеми флеш-пам’яті. Як випливає з назви, твердотільний накопичувач, означає, що в SSD немає рухомих частин. Без обертового диска, головки та кронштейна SSD можуть зменшитися до форми та розміру, що робить їх більш гнучкими для невеликих пристроїв.

SSD також мають порти SATA і 2,5-дюймовий формат. Крім того, існують менші твердотільні накопичувачі з міні-SATA (mSATA), які використовуються в слотах mini- PCI (Peripheral Component Interconnect) Express. Більшість сучасних ноутбуків мають SSD, встановлені в слот розширення PCI Express або встановлені безпосередньо на материнській платі. Ці твердотільні накопичувачі, встановлені на платі, використовують форм-фактор, відомий як M.2. [3]

Типи пам’яті SSD-дисків:

SLC (однорівнева комірка) – принцип роботи побудований на одній комірці, яка включена або відключена. Цей тип пам'яті є довговічним і дозволяє швидко записувати та зчитувати інформацію.

Переваги SLC пам'яті:

- підтримує багато перезаписів (близько 100 000 разів);
- висока швидкість;

- надійність;
- термостійка.

Головним недоліком такого типу пам'яті є висока вартість і недоступність для звичайного користувача.

MLC (багаторівнева комірка) – підтримує три-п'ять тисяч перезаписів, відрізняється високою довговічністю, доступною ціною та високою швидкістю, за рахунок чого цей тип пам'яті є найбільш популярним.

MLC має ряд переваг:

- низька вартість;
- доступність;
- широкий асортимент,
- надійніше ніж TLC-пам'ять.

TLC (трирівнева комірка) – підтримує близько від трьох до п'яти тисяч циклів і найчастіше використовується в бюджетних SSD накопичувачах, оскільки має невисоку швидкість. Цей тип пам'яті не використовується в комерційних чи промислових цілях, а призначений виключно для споживачів.

Переваги TLC: найдешевший тип пам'яті.

До недоліків відноситься низька швидкість у порівнянні з MLC та SLC.

Смарт-картки

За своєю природою спеціальні цифрові носії інформації (ЦНІ) є електронними документами спеціального типу з певним інтерфейсом доступу до них, і тому можуть зберігатися на будь-яких носіях інформації. Повністю розкривається потенціал ЦНІ, якщо засоби їх зберігання мають можливість організації спеціального захищеного інтерфейсу роботи з ЦНІ, тобто мають певні обчислювальні можливості.

Найбільш зручними портативними інтелектуальними носіями ЦНІ є інтелектуальні картки (інтелектуальні пластикові картки з пам'яттю) та USB-токени. Зауважимо, що в останній час як самостійні пристрої збереження ЦНІ можуть розглядатися засоби реалізації технології електронного паперу.

Розглянемо деякі портативні інтелектуальні носії ЦНІ більш детально. Найбільш відомими портативними інтелектуальними носіями є інтелектуальні картки (ІК). ІК є частковим випадком пластикової картки з пам'яттю.

Пластикова картка з пам'яттю — пластикова картка, обладнана засобами збереження електронної інформації. Міжнародною організацією зі стандартизації визначаються фізичні розміри картки і те, як вона працює при різноманітних механічних, фізичних, хімічних та інших впливах. Згідно із ISO-7810 для пластикової (пластмасової) картки встановлені розміри 85,6x54x0,76 мм з радіусом в кутах 3,18 мм. На картку можливе нанесення поліграфічного оформлення та додаткові елементи: магнітна стрічка, мікрочіп, підписна панель, голограма, штрих-код та ін. зауважимо, що поняття пластикової картки не ідентичне поняттю пластикової картки з пам'яттю, оскільки пластикова картка може служити носієм тільки візуальної інформації.

Кредитні картки (КК) - найпоширеніший тип пластикових карток. До них належать VISA та Master Card, Americam Exprese та AmEx'S Optima, картки Discovery Card фірми Sears, місцеві та регіональні картки універсальних магазинів.

Дебетові картки (ДК) — це пластикові картки, що використовуються для розрахунків в межах залишку на рахунку. Для дебетових транзакцій найчастіше використовується автоматичний касовий апарат (АКА). Дебетові картки призначені для заміни готівки та персональних чеків. ДК в основному застосовуються для одержання готівки через АКА.

Інтелектуальна картка (ІК) (смарт-картка) — це пластикова картка із вбудованим спеціалізованим обчислювальним пристроєм, що складається з процесора, постійного та оперативного пристрою пам'яті під керуванням спеціалізованої операційної системи. Пристрій постійної пам'яті багаторазового перезапису не вимагає джерела живлення для збереження інформації. Інтелектуальна картка зазвичай має можливість контролю доступу до інформації, що зберігається в ній.

Кишенькові комп'ютери — це самостійний клас обчислювальних засобів, які за своїми функціональними можливостями і форм-фактором займають проміжне положення між смартфонами (інтелектуальними мобільними телефонами з обчислювальними можливостями) та ноутбуками. Віднедавна час до функцій кишенькових комп'ютерів додали можливості мобільних терміналів і вони стали також називати комунікаторами. Класифікація пластикових карт приведена на рис. 1.2.

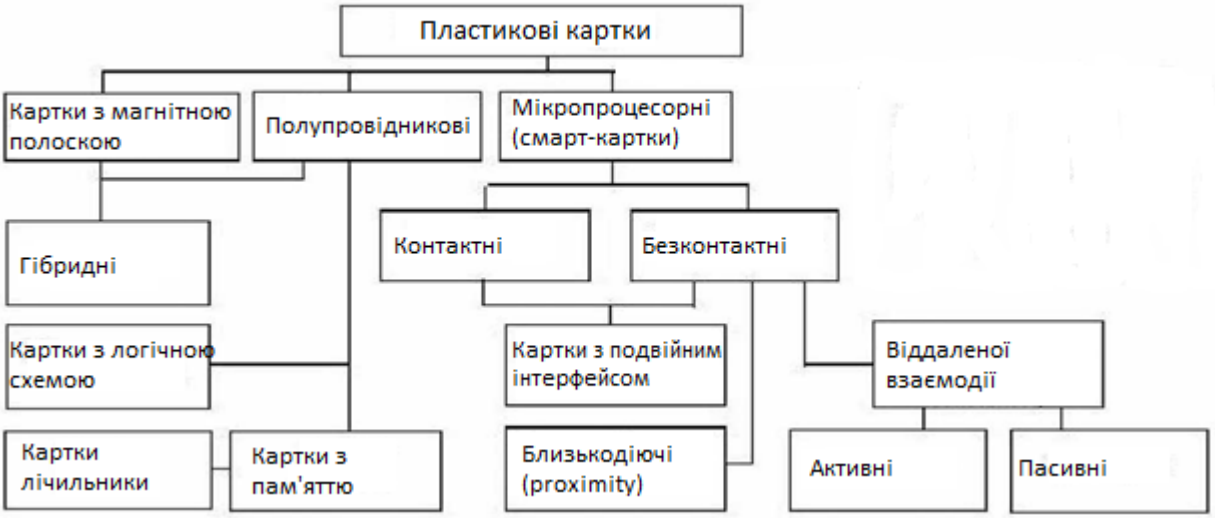


Рис. 1.2. – Класифікація пластикових карт

1.2.4. Накопичувачі на жорсткому магнітному диску

НЖМД - це основний пристрій для довготривалого збереження великих об'ємів даних та програм. Інші назви: жорсткий диск, вінчестер, HDD (Hard Disk Drive).

Жорсткий диск (HDD) складається з пластини, яка містить відсіки для зберігання даних. Ці дані – це ваша операційна система, програми та будь-які файли, які ви створили. Також є рукоятка акумулятора, яка переміщається по тарілкам для читання або запису запитуваної інформації. Щоб зробити цей процес швидшим, пластина обертається, коли рукоятка акумулятора рухається по ній.

Відсіки, що містять дані, можуть бути розкидані по всьому жорсткому диску. Тобто дані не записуються послідовно. Існує система індексації, яка дозволяє рукоятці акумулятора знаходити всі відповідні дані.

Тарілка і рукоятка акумулятора делікатні, тому закриті сталевим корпусом. Це запобігає пошкодженню диска за звичайних обставин.

1.3 Роль та місце накопичувачів на жорсткому магнітному диску у загальній класифікації цифрових носіїв інформації

За результатами вище зробленого аналізу характеристик та властивостей цифрових носіїв інформації, можна порівняти НЖМД з іншими носіями, виділити його переваги, недоліки та визначити їх місце у загальній класифікації цифрових носіїв інформації. Для наочності результатів проведеного аналізу данні наведено у вигляді таблиці:

Таблиця 1.2 - Характеристики та властивості цифрових носіїв інформації

Тип цифрового носія	Характеристики та властивості цифрових носіїв інформації				
	Ємність	Максимальна кількість циклів запису	Галузь використання	Час зберігання інформації	Недоліки
Магнітні стрічки	80 МБ	-	В якості зовнішнього запом’ятовуючого пристрою.	15 років	Низька швидкість запису та зчитування
Гнучкі магнітні диски	100 МБ	10 млн.	В якості зовнішнього запом’ятовуючого пристрою.	30 років	Чутливість до магнітних полів
Оптичні диски	5,2 Гб	100 000 тис.	В якості зовнішнього запом’ятовуючого пристрою.	50 років	Крихкі
Флеш-накопичувачі	1 Тб	50 000 тис.	В якості зовнішнього запом’ятовуючого пристрою.	10 років від часу останнього запису	Легко втратити, висока ціна
НЖМД	16 Тб	Необмежена	Є обов’язковим пристроєм ПЕОМ	Необмежений	Не стійкий до фізичних ушкоджень

Проаналізувавши дані з таблиці, можна наочно побачити переваги НЖМД над іншими типами цифрових носіїв інформації, а саме: НЖМД має максимальну ємність, необмежену кількість циклів запису даних та необмежений час

зберігання інформації. З усіх типів цифрових носіїв інформації НЖМД не має переваги лише у стійкості до фізичних ушкоджень.

Висновки до розділу 1:

Зробивши аналіз класифікації, характеристик та галузей застосування носіїв цифрової інформації, можна зробити наступні висновки:

– галузь застосування цифрових носіїв дуже велика, їх можна використовувати як в приватних так і в державних установах;

– жорсткі магнітні диски, як обов’язкові пристрої ПЕОМ із широко розгалуженою мережею практичного застосування, займають особливе місце у загальній класифікації цифрових носіїв інформації;

– жорсткі магнітні диски потребують дослідження з метою можливого вдосконалення їх характеристик та властивостей, націлених на підвищення рівня захисту інформації, яка записана на них.

РОЗДІЛ 2 ПОБУДОВА ТА ВЛАСТИВОСТІ НАКОПИЧУВАЧІВ НА ЖОРСТКОМУ МАГНІТНОМУ ДИСКУ

2.1. Архітектура НЖМД

Жорсткий диск забезпечує довгострокове, енергонезалежне зберігання даних. Протягом тривалого часу (починаючи від 1980-х років, і принаймні до 2000-х) ЖД є найбільш ємними носіями інформації, що серійно випускаються. На 2006 рік оптимальне співвідношення ціни і ємності забезпечують приблизно на 300 ГБ. На сучасному етапі максимальна доступна ємність НЖМД сягає 16 ТБ.

Жорсткий диск складається із двох основних частин: гермоблока і контролера (рис.2.1):

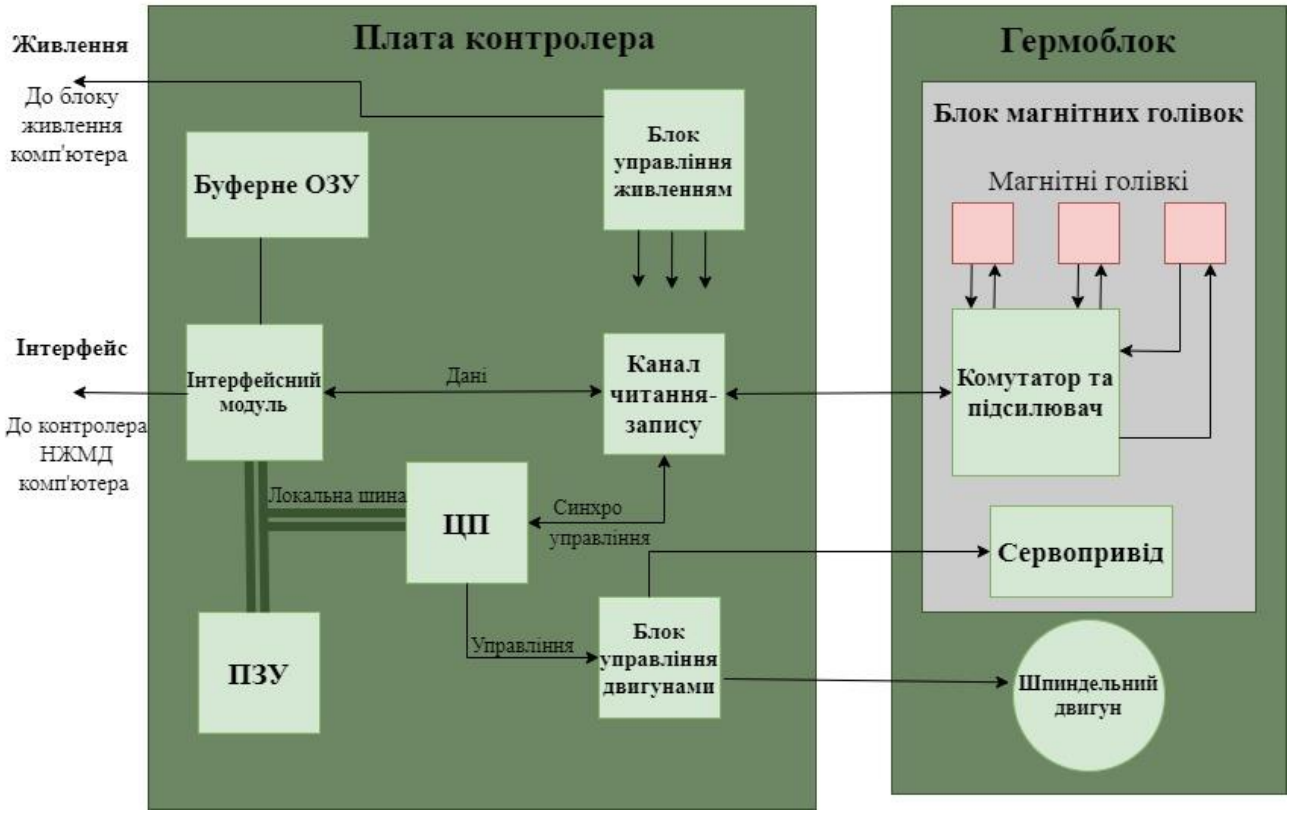


Рис. 2.1 Структурно-модульна схема НЖМД

Гермоблок - являє собою герметичну камеру, наповнену чистим повітрям без пилу, і пакет, що містить магнітний диск і частину магнітної головки (BMG). Незалежно від герметичності, камера з’єднана з навколишнім середовищем через

барометр-фільтр, який вирівнює тиск всередині і зовні камери. Фільтр барометра призначений для запобігання проходження великих частинок пилу (більше 0,5 мкм). Вирівнювання тиску запобігає механічній деформації корпусу. Також є фільтр рециркуляції, який зберігає в камері частини, які можуть бути втрачені всередині (в результаті зносу) або через фільтр барометра. Він розташований на шляху обертання повітряного диска.

Магнітні диски зазвичай виготовляються з алюмінію, зазвичай скла або кераміки, з магнітним покриттям і мають форму тонкої стрічки (феромагнетика), яка виконує роль носія. Магнітні диски встановлені з постійною швидкістю в пакеті, розташованому на осі обертового двигуна. Стабілізація обертання здійснюється контролером на серводвигуні. (Раніше датчик положення диска використовувався окремо). Зазвичай в упаковці не більше трьох дисків, і запис може здійснюватися на одній або обох сторонах кожного диска. Тому диски зазвичай мають від 1 до 6 головок.

Блок магнітної головки рухається по поверхні диска від краю до центру за допомогою сервопривід. На першій рейці сервопривід здійснювався кроковим двигуном, пізніше була використана електромагнітна котушка, подібна до магнітного вимикача. Для керування головками в рейці зберігаються пристрої, які називаються адаптерами — для кожної рейки дані про фізичні властивості сервоголівки — для зберігання необхідної амплітуди та часу електромагнітного керуючого сигналу. Перехідники швидко і майже бездоганно встановлюють головку, надійно тримаючи її на дорозі.

Сама головка являє собою невелику електромагнітну систему, яка забезпечує локальне намагнічування поверхні диска і його намагнічування. Перші електромагнітні головки зчитують інформацію через збуджену ЕРС на котушці. Пізніше магнітні опорні головки стали використовуватися для зчитування спеціальних матеріалів за допомогою магнітних датчиків.

У вимкненому положенні головки лежать на диску паркувального майданчика. Головки фіксуються в цьому положенні, щоб запобігти пошкодженню під час транспортування, і не можуть бути переміщені, поки диск

не повернеться. Під час роботи головки плавають над поверхнею диска і обертаються на відстань в одну десяту мікрометра на одиницю площі. Тому поверхня диска не зношується (як у випадку з дискетами).

Поряд з блоком магнітної головки всередині або поруч з герметичним блоком є перемикач, який перемикає активну голівку і попередньо підсилює сигнал магнітного датчика. Якщо жорсткий диск має одну робочу поверхню, перемикач діє лише як підсилювач. Конструктивно контролер зазвичай виконаний у вигляді друкованої плати, закріпленої на одній стороні пломби. До складу контролера входять блоки живлення, управління електродвигуном вала, сервопривід BMG, зчитування та запис інформації на диск, зовнішній інтерфейсний обмінник, інтерфейсний роз'єм, блок живлення, підключення до герметичного блоку, а також технологічні роз'єми та елементи конфігурації (роз'єми).

Сучасний контролер - вбудована мікропроцесорна система, що виконує мікропрограму.

Основні вузли контролера:

- схема управління живленням;
- модуль управління (мікропроцесорний).
- інтерфейсний модуль;
- канал читання-запису;
- контролер БМГ;
- контролер шпиндельного двигуна;

2.1.1. Технічні характеристики НЖМД

Технічні характеристики дискового накопичувача можуть збивати з пантелику, і їх важко інтерпретувати. У цьому розділі висвітлюються деякі з найважливіших специфікацій, що використовуються з дисковими накопичувачами в додатках для мереж зберігання даних, у тому числі такі:

- Середній час напрацювання на відмову
- Швидкість обертання та затримка
- Середній час пошуку
- Швидкість передачі мультимедіа
- Стійка швидкість передачі

Середній час напрацювання на відмову (MTBF) вказує очікувану надійність дисководів. Властивості MTBF розраховуються за допомогою чітко визначених статистичних методів і перевіряються на великій кількості дисків за короткий період часу. Результати екстраполюються і зазвичай виражаються від 500 000 до 1,25 мільйонів годин. Ці цифри надзвичайно високі для індивідуального водіння – 1,25 мільйона годин – тобто приблизно 135 років.

Індикатори MTBF допомагають створити очікування того, скільки разів диски вийдуть з ладу, коли ви перебуваєте в середині дисків. Використовуючи MTBF 1,25 мільйона годин (135 років), якщо у вас є 135 жорстких дисків, ви вийдете з ладу раз на рік. У середовищі зберігання з великою кількістю дисків – наприклад, понад 1000 дисків – легко помітити, що обов'язково повинні бути резервні диски, оскільки пошкодження диска, яке потрібно відремонтувати, неминуче. Він також підкреслює важливість використання методів резервного копіювання дисків, таких як дзеркала або RAID.

Швидкість обертання та затримка

Одним із найпоширеніших способів визначення ємності диска є визначення його швидкості обертання. Чим швидше обертається диск, тим швидше дані можуть бути записані та прочитані на диск. Різниця в продуктивності може бути величезною. За інших рівних умов диск зі 15 000 об/хв може виконувати вдвічі більше роботи, ніж диск зі швидкістю 7200 об/хв. Якщо в системі обробки транзакцій використовується 50 або більше дисків, легко зрозуміти, чому хтось хоче використовувати диск з більш високою швидкістю.

Швидкість пов'язана з параметром, який називається затримкою обертання. Якщо головки диска знаходяться на правильному шляху на платі диска, ви повинні почекати, поки під ними пройде правильний сектор, перш ніж

передавати дані. Час, необхідний для очікування правильної гілки, називається затримкою і безпосередньо пов’язаний зі швидкістю обертання диска.

Фактично, затримка обертання визначається як середній час очікування для будь-якої випадкової операції введення/виведення і вважається часом, необхідним для завершення півперіоду плити.

Затримки обертання коливаються від 2 до 6 мілісекунд. Це може здатися не таким довгим. Однак це дуже повільно в порівнянні зі швидкістю процесора та пам’яті. Додатки, на які часто впливають блокування введення/виводу, такі як обробка транзакцій, зберігання даних і потік медіа, вимагають високошвидкісних дисків і великих буферів.

Середній час пошуку

На додаток до швидкості обертання, час пошуку є найважливішою характеристикою продуктивності жорсткого диска. Час пошуку вимірює час, необхідний активатору для переміщення головки читання/запису на платі з одного шляху на інший. Середній час пошуку — це середня продуктивність багатьох операцій введення та виведення і відносно подібний до затримки обертання в діапазоні 4-8 мілісекунд.

Обробка транзакцій та інші програми баз даних виконують велику кількість випадкових операцій введення та виведення у швидкій послідовності. Хоча робоче навантаження можна розподілити між кількома дисками, продуктивність програми транзакцій значною мірою залежить від здатності окремого диска швидко обробляти операції введення-виводу. Він поєднує низький час пошуку та високу швидкість.

Швидкість передачі даних

Швидкість даних на диску вимірює продуктивність бітів читання/запису на платі диска. На відміну від більшості параметрів пам’яті, перерахованих у байтах, швидкість передачі медіа вказується в бітах. Швидкість передачі медіа вимірює продуктивність читання/запису на одній доріжці, яка залежить від радіальної довжини доріжки. Іншими словами, доріжки в зоні 0 мають найвищу

швидкість передачі медіа на диску. Тому швидкість медіа іноді визначається за допомогою регіонів.

Стійка швидкість передачі

Більшість операцій введення/виводу на диску виконуються в ряді шляхів і циліндрів, з можливістю зміни положення головки читання/запису. Визначення стабільної швидкості передачі враховує фізичні затримки та затримки пошуку під час пошуку і ближче до вимірювання продуктивності реальних даних, ніж швидкості передачі мультимедіа.

Однак стабільна швидкість передачі є оптимальною умовою, до якої важко підійти при реальному використанні. Є й інші важливі властивості, такі як середній розмір об’єкта даних і рівень розділу файлової системи. Однак стабільна швидкість передачі даних є хорошим показником загальної продуктивності браузера. [2].

Параметри ЖД:

- *Розмір пластини* - параметр, що визначається, як правило, геометричними розмірами ЖД, зазвичай діаметр на 1-2 см менше ширини.
- *Щільність запису на одиницю площі* - визначається технологією виготовлення диска. Вказується зазвичай у гігабітах на квадратний дюйм чи квадратний сантиметр. Зазвичай диски однієї серії мають однакову щільність запису.
- *Об'єм поверхні* - параметр, що залежить від щільності запису і розміру пластини.
- *Кількість робочих поверхонь* – теж саме, що і кількість фізичних голівок. Залежить від конструктивного виконання. (рис 2.2)

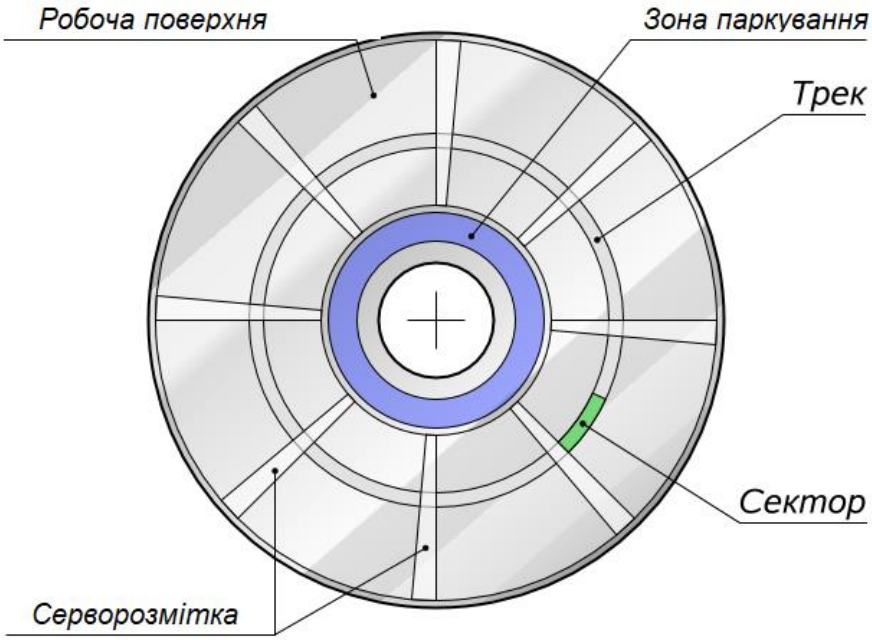


Рис 2.2 Логічна структура та розмітка поверхні магнітного диска

Ємність зберігання

Ємність жорсткого диска вимірюється в байтах. Сучасні браузери мають гігабайти (мільярди байт) і терабайти (трильйони байт) і можуть бути більшими. Ємність - це відношення кількості пластин або дисків, встановлених на накопичувачі, до щільності магнітної ємності цих пластин.

Швидкість доступу

Жорсткий диск - це електромеханічний пристрій. Дані, що зберігаються на магнітній пластині, зчитуються головкою, що плаває на поверхні, коли диск обертається внизу. Головка читання-запису повинна переміщатися в різні частини плати, коли вона обертається, щоб прочитати всі частини файлу. Поєднання швидкості головки та того, наскільки швидко може обертатися пластина під головкою, є основою швидкості проникнення.

Форм-фактор

Ранні жорсткі диски були величезними, розміщувалися в окремих машинах і підключалися до ЦП за допомогою важких кабелів. Сучасні жорсткі диски обмежені трьома фізичними форматами: 3,5-дюймовий, 2,5-дюймовий і 1,8-дюймовий. Менший фізичний розмір обмежує кількість тарілок і діаметр цих

пластин. Наприклад, 1,8-дюймовий накопичувач має максимальну ємність 320 гігабайт.

Інтерфейс

Електронний зв'язок між жорстким диском і процесором з часом змінився. Кожна зміна інтерфейсу покращує швидкість передачі даних, полегшуючи керування жорстким диском на материнській платі комп'ютера. Поточний стандартний інтерфейс - SATA, який є постійним підключенням до передових технологій.

SATA означає послідовне підключення передових технологій. Він використовується для послідовних сигналів для передачі даних, інструкцій та інформації. Основна перевага SATA в тому, що кабелі тонші, довші і вищі. Зовнішні жорсткі диски можуть використовувати інтерфейс SATA, який набагато швидше, ніж USB.

EIDE розшифровується як Enhanced Integrated Drive Electronics. EIDE – це інтерфейс пристрою, який використовує сигнали паралельно для передачі інструкцій та даних тощо. Приблизна швидкість передачі даних EIDE становить до 133 Мбіт/с.

SCSI розшифровується як Small Computer System Interface. Він використовується як паралельний сигнал і не може підтримувати від 8 до 15 пристроїв. SCSI може підтримувати жорсткі диски, дисководи, принтери тощо.

Disk cache - він використовується для покращення продуктивності жорсткого диска. Це тип інструкцій та даних RAM програми, з якими працює користувач. Коли ЦП потребує інформації, він спочатку переглядає кеш з жорсткого диска, а якщо йому не потрібна інформація, він отримує інформацію з жорсткого диска.

Швидкодія жорстких дисків

Важливе значення мають швидкісні характеристики ЖД:

Швидкість обертання шпинделя - зазвичай вимірюється в обертах за хвилину (об/хв, rpm). Вона не дає прямої інформації про реальну швидкість обміну, але дозволяє розрізняти більш швидкісні від менш швидкісних.

Стандартні швидкості обертання: 4800, 5600, 7200, 9600, 10 000, 15 000 об/хв. Повільні зазвичай використовуються на ноутбуках та інших мобільних пристроях, найшвидші – у серверах.

Час доступу — кількість часу, необхідне ЖД з моменту прийому команди до початку видачі даних з інтерфейсу. Зазвичай вказується середній та максимальний час доступу.

Час позиціонування голівок - час, за який голівки переміщуються і встановлюються на трек з іншого треку. Розрізняють час позиціонування на сусідній трек (track-to-track), середній (average), максимальний (maximum).

Швидкість передачі даних або пропускна здатність — визначає продуктивність диска під час передачі послідовно великих обсягів даних. Ця величина показує швидкість передачі, коли голівки диска вже на потрібному треку і секторі.

Внутрішня швидкість передачі даних — швидкість передачі між контролером і магнітними голівками.

Зовнішня швидкість передачі даних – швидкість передачі даних за зовнішнім інтерфейсом.

2.1.2. Різновиди жорстких дисків

Комп’ютери використовують жорсткий диск (HDD) для постійного зберігання. Це пристрої зберігання даних, які використовуються для зберігання та отримання цифрової інформації, необхідної для майбутнього використання.

Жорсткі диски нестабільні, а це означає, що вони зберігають дані навіть при відсутності живлення. Якщо жорсткий диск не пошкоджений, збережена інформація залишиться.

На відміну від послідовного доступу, інформація зберігається або зчитується за допомогою довільного доступу. Це означає, що за потреби можна отримати доступ до блоків даних, не перебираючи інший блок даних.

В даний час ми можемо згрупувати жорсткі диски за п’ятьма типами:

- Прикріплення паралельної передової технології (PATA)
- Послідовний ATA (SATA)
- Інтерфейс малих комп’ютерних систем (SCSI)
- Твердотільні накопичувачі (SSD)
- NVM Express

Паралельні передові технології (PATA)

Це були перші типи жорстких дисків. Для підключення до комп’ютера вони використовували стандарт інтерфейсу Parallel ATA.

Ми називаємо ці типи приводів дисками з інтегрованою електронікою (IDE) і вдосконаленою інтегрованою електронікою приводу (EIDE).

Ці диски PATA були представлені в 1986 році компаніями Western Digital і Compaq. Вони забезпечують загальну технологію інтерфейсу для підключення жорстких дисків та інших пристроїв до комп’ютера.

Швидкість передачі даних досягає 133 МБ/с, а до каналу накопичувача можна підключити максимум 2 пристрої. Більшість материнських плат мають два канали, тому ви можете підключити до чотирьох пристроїв EIDE.

Вони використовують 40 або 80-ядерні кабелі з пропускною здатністю для паралельної передачі кількох біт даних. Ці диски зберігають дані за допомогою магнітних сил.

Внутрішня конструкція складається з рухомих механічних частин. Їх замінили послідовні ATA.

Накопичувачі Serial ATA(SATA)

Ці жорсткі диски замінили диски PATA на настільних комп’ютерах і ноутбуках. Основна фізична відмінність між ними - це інтерфейс.

SATA був анонсований в 2000 році і має ряд переваг перед попереднім інтерфейсом PATA. Вони включають зменшений розмір кабелю, нижчу вартість (сім проводів замість 40 або 80), вбудовану гарячу заміну, більш високу швидкість передачі даних і більш ефективні послідовності введення/виводу.

У них однаковий спосіб підключення до комп’ютера. Ось деякі переваги жорсткого диска SATA. Сила у них дуже різна, як і ціна.

Купуючи жорсткий диск, необхідно знати його ємність і обсяг пам’яті.Диски SATA можуть передавати дані швидше, ніж типи PATA завдяки технології послідовної передачі сигналів.

Кабелі SATA тонші та гнучкіші, ніж кабелі PATA.

Вони мають 7-контактне з’єднання передачі даних з обмеженням кабелю до 1 метра.

- Диски не поділяють смугу пропускання, тому що на кожну мікросхему контролера SATA на материнській платі комп’ютера можна використовувати лише один диск.
- Вони споживають менше енергії. Їм потрібно всього 250 мВ, а не 5 В для PATA.

Інтерфейс малих комп’ютерних систем (SCSI)

Вони дуже схожі на жорсткі диски IDE, але для підключення до комп’ютера використовують інтерфейс малої комп’ютерної системи .

SCSI – це набір стандартів для фізичного підключення та передачі даних між комп’ютерами та периферійними пристроями. Ці стандарти визначають команди, протоколи, електричні, оптичні та логічні інтерфейси.

Накопичувачі SCSI можуть бути підключені всередині або ззовні. Ось деякі з їхніх переваг:

- Вони швидші.
- Вони дуже надійні.
- Підходить для роботи у режимі 24/7.
- Найкраща масштабованість та гнучкість масивів.
- Добре адаптований для зберігання та переміщення великих обсягів даних.

Твердотільні накопичувачі (SSD)

Це новітні технології браузера в комп’ютерній індустрії. Вони сильно відрізняються від інших приводів тим, що не складаються з рухомих частин.

Вони також зберігають дані за допомогою магнітних сил. Натомість вони використовують технологію флеш-пам’яті. SSD використовується для постійного зберігання даних, поки не буде зруйнована принаймні інтегральна схема або напівпровідниковий пристрій.

Основою твердотільних накопичувачів є флеш-пам'ять, винайдена Фуджі Масуока в Toshiba в 1980 році і представлена Toshiba в 1987 році.

Перший комерційний SSD на основі флеш-пам'яті був представлений SanDisk у 1991 році. Він мав 20 МБ SSD в конфігурації PCMCIA.

Переваги твердотільних накопичувачів:

- Швидший доступ до даних.
- Менш схильний до шоку.
- Найменший час доступу та затримка.
- Довговічність.
- Менше за енергоспоживання.

Накопичувач NVMe

Unstable Memory Express (NVMe) — це інтерфейс зберігання даних, представлений у 2013 році. «Нестабільна пам’ять» означає, що дані не будуть втрачені під час перезавантаження комп’ютера або вимкнення живлення.

Термін «Express» означає, що дані передаються через інтерфейс PCI Express (PCIe) на материнській платі вашого комп’ютера.

Це дозволяє підключати підключений накопичувач безпосередньо до материнської плати. Це тому, що дані не потрібно передавати через контролер Serial Advanced Technology Attachment (SATA).

Тому накопичувачі NVMe набагато швидше, ніж SATA. Поточний стандарт PCIe 3.0 PCIe має максимальну швидкість передачі 985 мегабайт (Мбіт/с) на повідомлення.

Диски NVMe можуть використовувати до 4 діапазонів PCIe, що теоретично означає максимальну швидкість 3,9 Гбіт/с (3940 Мбіт/с).

Між тим, Samsung 860 Pro, один з найшвидших твердотільних накопичувачів SATA, забезпечує максимальну швидкість читання та запису 560 Мбіт/с.

Диски NVMe бувають різних форм-факторів. Палиця м.2 - найпоширеніша з них.

Ширина 22 мм і довжина 30, 42, 60, 80 або 100 мм. Ці стрижні досить тонкі, щоб лежати на материнській платі. Це робить їх придатними для невеликих комп'ютерів і ноутбуків.

Форм-фактор PCIe-3.0 схожий на графічний процесор і підключений до одного зі слотів PCIe-3.0 на материнській платі. Це нормально для повнорозмірних коробок ATX і материнських плат.

Однак це обмежує ПК невеликим форм-фактором. З іншого боку, це неможливо в коробці для ноутбука.

Hard drive disk (HDD)

Це магнітний запам'ятовуючий пристрій. Інформація повинна бути записана на пластині, покритій феромагнітним матеріалом, на одній осі. Пластини називаються магнітними дисками, а сам жорсткий диск може використовувати кілька магнітних дисків.

HDD керує двигунами та електронними блоками для обертових магнітних пластин - контролює весь процес. Жорсткий диск відформатований для зберігання даних, тобто він розділений на шляхи рівнів, які, у свою чергу, поділяються на гілки, що в свою чергу створює кластер. Важливо знати, що жорсткий диск не є герметичним, але він герметичний, і його відкриття призведе до повного виходу з ладу жорсткого диска.

Порівняльна характеристика SSD та HDD

Твердотілий накопичувач (SSD) і традиційний жорсткий диск (HDD) виконують однакові завдання і виглядають майже однаково за своїми фізичними

характеристиками. Однак вони працюють по-різному і мають свої унікальні особливості.

Таблиця 2.1- Порівняльна характеристика SSD та HDD

SSD	**HDD**
Твердотілий накопичувач	Жорсткий диск
Складається с електронних частин	Складається с рухомих механічних частин
Дороговартісний	Дешевий
Компактний і відносно швидкий	Великих розмірів та порівняно повільніший

Переваги HDD:

- Ємність - з точки зору місткості, жорсткий диск має незначні переваги перед твердотілими накопичувачами, оскільки існує можливість мати багато місця за дешевшою ціною.
- Надійність - оскільки кожна клітинка флеш-пам’яті підтримує обмежену кількість циклів читання/запису, термін служби жорстких дисків вважається більшим, ніж твердотілих дисків.

Недоліки HDD:

- Ємність – на відмінну від SSD використовується більше фізичного простору для зберігання кількох терабайт.
- Надійність - твердотілі накопичувачі вважаються більш довговічними.
- Швидкість – значно нижча швидкість HDD (150МБ/с) порівняно з SSD (550МБ/с).

Порівнявши SSD та HDD доцільно зауважити, що HDD набагато надійніші, але більш сприйнятливі до фізичних пошкоджень, оскільки вони виготовлені з механічних частин. Якщо впустити жорсткий диск або ноутбук, швидше за все, будуть втрачені дані через пошкоджений жорсткий диск або фізичне пошкодження. Жорсткі диски переважають на незначну частку за ємністю, на відміну від SSD. На жаль, HDD програють за швидкістю, що може бути приводом частішого застосування твердотілих накопичувачів. Саме це зумовлює на необхідність дослідження НЖМД для вдосконалення їх характеристик, методів збереження та знищення інформації.

2.1.3. Технології запису та зберігання інформації

Пластини - найважливіші частини жорсткого диска. Як зрозуміло з назви, це диски, виготовлені з твердих матеріалів, таких як скло, кераміка або алюміній, і покриті тонким шаром, який можна намагнічувати або розмагнічувати. Невеликий жорсткий диск має лише одну пластину, але кожна сторона має магнітне покриття. Великі диски розміщують кілька пластин, встановлених у центральному кутку з невеликим проміжком між ними. Пластини обертаються зі швидкістю до 10 000 об/хв (об/хв), так що головки читання-запису мають доступ до будь-якої їх частини.

Кожна папка має дві головки читання-запису: одну для читання зверху, а іншу для нижньої, тому жорсткий диск з п’ятьма дисками (якщо є) потребує десяти окремих головок читання-запису. Головки зчитування і запису встановлені на важелях з електроприводом, які рухаються від центру накопичувача до країв і назад. Щоб зменшити знос, вони фактично не торкаються диска: між головкою і поверхнею диска є шар рідини або повітря.

Читання та запис даних

Найважливіше в пам’яті – це не здатність зберігати інформацію, а здатність згодом її знаходити. Уявіть, що ви зберігаєте намагнічений металевий цвях у купі з 1,6 мільйона однакових цвяхів, і ви матимете чітке уявлення про те, що

станеться, якщо ваш комп’ютер не використовує багато методів зберігання даних. Зберігаючи дані на жорсткому диску комп’ютера, не тільки киньте в коробку намагнічений цвях, але й перемішайте його. Дані дуже акуратно зберігаються на кожній дошці. Біти даних розташовані на централізованій орбіті, яка називається шляхом. Кожен шлях поділено на невеликі ділянки, які називаються гілками. Частина жорсткого диска зберігає карти гілок, які вже витрачені, та інших гілок, які ще вільні. (У Windows ця картка називається таблицею розташування файлів або FAT.) Коли комп’ютер хоче зберегти нову інформацію, він дивиться на карту й знаходить вільні сектори. Потім він доручає головці читання-запису перемістити плату в потрібне місце і зберегти там дані. Цей же процес виконується в зворотному порядку для зчитування інформації.

Як електронний комп’ютер керує всіма механічними компонентами жорсткого диска? Між ними є інтерфейс (апаратний роз'єм), який називається контролером. Це невелика схема, яка керує активатором, вибирає певний шлях читання та запису та перетворює паралельний потік даних з комп’ютера в послідовний потік даних, записаних на диск (і навпаки). Контролер можна встановити на вашу друковану плату або частина материнської плати вашого комп'ютера. .Жорсткі диски — чудова інженерна ідея, оскільки на такому маленькому просторі зберігається так багато інформації. Він має свої переваги (може зберігати 500 компакт-дисків на iPod) і свої недоліки. Одним з недоліків є те, що жорсткий диск може пошкодитися, якщо всередину потрапить бруд. Найменший пил може покотити головку для читання та запису вгору і вниз, врізатися в опорний диск і пошкодити магнітний матеріал. Це називається пошкодженням диска (або пошкодженням головки), яке (не завжди) призводить до втрати всієї інформації на жорсткому диску. Пошкодження диска зазвичай відбувається раптово і без попередження. Тому вам завжди слід створювати резервні копії важливих документів і файлів на інший жорсткий диск, компакт-диск, DVD або флеш-накопичувач.

Метод повздовжнього (паралельного) запису

Як зазначено в назві, поздовжній запис - це метод запису даних на жорсткий диск (HDD) таким чином, що біти даних вирівняні по горизонталі щодо диска приводу, що обертається, який паралельний поверхні диска. По суті ви записуєте на магнітний матеріал, де біти (сукупність намагнічених частинок) розташовуються встик. Поздовжній запис - це реальний метод запису бітів на диски. Напрямок цього магнітного заряду горизонтально по відношенню до середовища, що означає, що північний та південний полюси намагнічених частинок вирівняні паралельно поверхні диска.

Поздовжній запис був стандартним методом запису понад 50 років. Перший комерційний жорсткий диск було представлено 1956 року. За ці роки ми побачили безліч технологічних змін у поздовжньому записі, які призвели до появи дисків більшої ємності. Ми перейшли з 5, 25-дюймових дисків на 2, 5-дюймові, кількість пластин та головок було зменшено при одночасному збільшенні щільності запису (тобто кількості даних на квадратний дюйм носія). Однак з усіма цими змінами необхідність фізичної зміни способу запису даних на диск також розглядалася для більшої ємності сховища.

Місткість пам’яті з поздовжнім записом була значною мірою збільшена за рахунок зменшення розміру магнітних зерен, з яких складаються біти даних. У міру того, як магнітні зерна ставали меншими, на диску можна було зберігати більше даних. На жаль, магнітні зерна мають свої межі. Продовжуючи стискати їх, точка, в якій цілісність даних буде порушена, вже не за горами. Цей ефект називається суперпарамагнітним ефектом.(рис. 2.3)

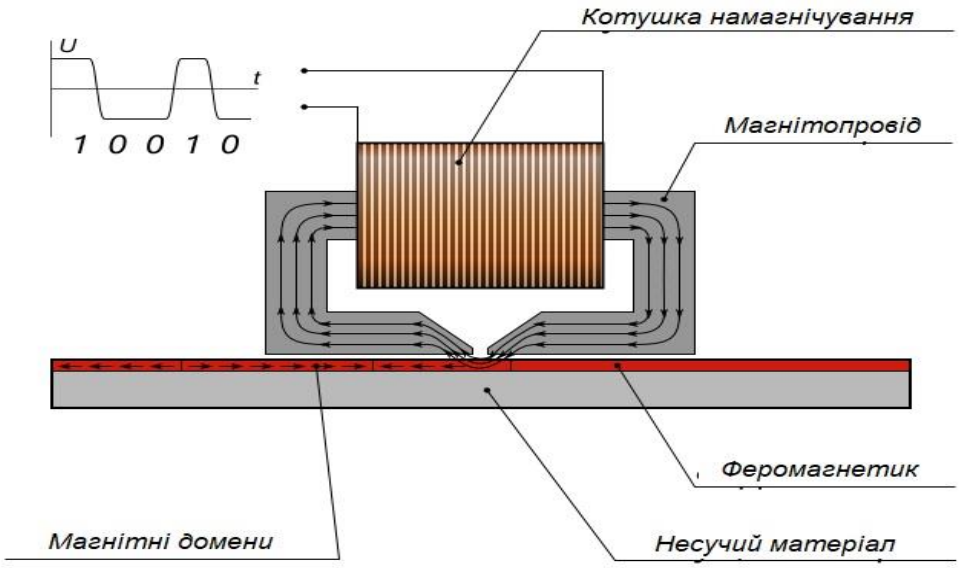


Рис 2.3 Паралельний метод магнітного запису

Метод теплового запису

У технології зберігання магнітних дисків метод теплового запису відноситься до коливань намагніченості через теплове збудження. Коли щільність запису (кількість бітів, які можуть зберігатися на квадратному дюймі дискового носія), дискового носія досягає 150 Гб на квадратний дюйм, магнітна енергія, що утримує біти на місці на носії, стає рівною оточуючої теплової енергії. усередині самого дисководу. Коли це відбувається, біти більше не утримуються в надійному стані і можуть перевертати і шифрувати дані, які були раніше записані.

Очікувалося, що через суперпарамагнетизм технології жорстких дисків перестануть розвиватися, коли вони досягнуть щільності 150 Гб на квадратний дюйм. Звичайно, коли ви бачите, що виробник жорстких дисків оголошує про випуск жорсткого диска на 400 ГБ, ви можете поставити питання, що трапилося з суперпарамагнітним ефектом? Фактично цей тип диска міститиме три пластини, здатні зберігати до 133 ГБ кожна, в результаті чого виходить жорсткий диск на 400 ГБ, а не 400 ГБ на одній пластині.

Метод перпендикулярного запису

Розуміючи, що обмеження упаковки дрібніших магнітних зерен наближали до виникнення суперпарамагнетизму, виробникам, як і раніше, був

потрібний спосіб упаковки більшої кількості даних на кожен диск. Перпендикулярний запис відрізняється від поздовжнього запису тим, що біти даних вирівняні по вертикалі (а не по горизонталі) або перпендикулярно до диска, що дає додаткове місце на диску для упаковки більшої кількості даних, що забезпечує більш високу щільність запису. Широко поширена думка, що при перпендикулярному записі бар'єр суперпарамагнетизму може бути зрушений ще далі, забезпечуючи безперервне зростання поверхневої густини носія протягом деякого часу.

Hitachi вважає, що ця технологія запису згодом може призвести до створення 3, 5-дюймового жорсткого диска, здатного зберігати цілий терабайт даних. Перпендикулярна запис вплине як на настільні сховища, а й споживчі пристрої, що є основною рушійною силою продажів сховищ. Найменші диски (1, 8 дюйма), такі як ті, що використовуються в популярному Apple iPod, також збільшаться у ємності. Свого часу ми побачимо iPod та аналогічні пристрої з об'ємом пам'яті 80 ГБ та вище. В якості альтернативи його можна використовувати для виробництва більш тонких і тонких жорстких дисків великої ємності для споживчих пристроїв. Однак технологія перпендикулярного запису не запускається і не зупиняється при зміні способу вирівнювання даних. Подібно до збільшення ємності поздовжнього запису, технологічним досягненням у пластинах.

Результати дослідження архітектури та характеристик різних типів НЖМД викладено у таблиці:

Таблиця 2.2 - Характеристики та властивості сучасних НЖМД

Тип НЖМД	Характеристики та властивості цифрових носіїв інформації					
	Ємність	Рівень шуму	Термін дії	Швидкість читання	Швидкість запису	Собівартість
SATA	250 Гб	34 дБ	3 роки	150 Мб/с	150 Мб/с	100 грн
SCSI	36 Гб	32 дБ	3 роки	320 Мб/с	320 Мб/с	500 грн
HDD	16 Тб	27 дБ	необмежений	150 Мб/с	150 Мб/с	2000 грн (1Тб)
SSD	20 Тб	0 дБ	8 років	550 Мб/с	525 Мб/с	3000 грн (1Тб)

Висновки до розділу 2:

Дослідивши архітектуру НЖМД, їх різновиди та методи запису даних, можна зробити наступні висновки:

- використовуються різні види ЖД в залежності від типів та призначення комп’ютерів;
- розглянувши характеристики та властивості сучасних НЖМД, доцільно зауважити, що SSD переважають за швидкістю читання/запису даних та за відсутністю шуму під час роботи. Але, HDD мають значні переваги відносно до ємності, терміну дії та ціни;
- на даний момент, найпоширенішою технологією запису інформації на ЖД є метод паралельного запису, а найперспективнішою - метод теплового магнітного запису;
- в основу методів запису інформації на ЖД покладено технології, які пов’язані із зміною фізичних властивостей певних зон поверхонь дисків, що у подальшому є передумовами можливого відновлення інформації у разі її стирання. Ці обставини вимагають дослідження питань, пов’язаних із забезпеченням надійного збереження інформації на ЖД, а також гарантованого її знищення на носієві у разі потреби.

РОЗДІЛ 3 НАДІЙНЕ ЗБЕРІГАННЯ ТА ЗНИЩЕННЯ ІНФОРМАЦІЇ НА МАГНІТНИХ НОСІЯХ ЦИФРОВОЇ ІНФОРМАЦІЇ

3.1. Методи атак на жорсткі диски

Жорсткі диски (HDD) стали найбільш часто використовуваним типом енергонезалежного сховища через їх підвищену надійність, відмовостійкість, ємність зберігання тощо.

Ці технологічні досягнення в жорстких дисках разом із постійно зростаючою потребою в зберіганні величезної кількості даних зробили їх одним із основних компонентів сучасних обчислювальних систем. Дійсно, жорсткі диски зараз є невід'ємною частиною численних повсюдно поширених систем, включаючи, але не обмежуючись ними, персональні комп'ютери, хмарні сервери, системи закритого телебачення (CCTV) і банкомати.

Таким чином, ефективна і легко здійснювана DoS-атака на жорсткі диски може призвести до значних проблем у реальному світі для окремих осіб та організацій.

Ефективність атаки залежить від здатності зловмисника створювати акустичний сигнал поблизу цільового пристрою, таким чином, що викликає значні вібрації у внутрішніх компонентах накопичувачів.

Зловмисник потенційно може скористатися перевагами віддаленого використання програмного забезпечення (наприклад, дистанційно керувати мультимедійним програмним забезпеченням у транспортному засобі чи персональному пристрої), обдурити користувача, щоб відтворити шкідливий звук, прикріплений до електронного листа чи веб-сторінки, або вставити шкідливий звук у поширеній мультимедіа (наприклад, телереклама).

Для того, щоб напад залишився непоміченим, а його природа невідомою, сигнал повинен бути нижче діапазону слуху людини (20–20 000 Гц).

Обмеження атак

Дослідники продемонстрували життєздатність атаки, зумівши зупинити операції читання/запису диска в пристрої цифрового відеореєстратора (DVR) системи відеоспостереження, а також у персональному комп'ютері. В останньому прикладі атака призвела до різних несправностей.

Але виявилось, що успіх атак залежав не тільки від частоти акустичного сигналу, а й від кута нахилу динаміка до жорсткого диска. Таким чином, джерело звуку не може бути занадто далеко від цілі.

Найдальша успішно виконана атака була на відстані 71 см (92,8 дБА) для жорсткого диска ємністю 1 ТБ на частоті 9,1 кГц і 44 см (102,6 дБА) для жорсткого диска 4 ТБ на частоті 8,5 кГц.

Крім того, зловмисник повинен знайти спосіб дізнатися марку та модель цільових накопичувачів, щоб він зміг вибрати амплітуду акустичного сигналу, який викличе акустичний резонанс і вплине на компоненти накопичувача.

Майбутні, більш успішні атаки такого роду залежатимуть від того, чи зловмисники знайдуть дієві рішення цих проблем.

Безпека жорстких дисків ігнорується, незважаючи на їхню критичну роль у обчислювальних системах. На жорстких дисках зберігаються важливі програмні компоненти (наприклад, операційна система) та різні форми конфіденційної інформації (наприклад, відео з камер відеоспостереження), і тому вони можуть бути привабливою цільцю для безлічі зловмисників.

Існує мало шансів побачити масову експлуатацію реальних пристроїв з використанням акустичних атак на жорсткі диски, оскільки такий сценарій, ймовірно, непрактичний через величезну кількість критеріїв, яким повинен відповідати зловмисник.

Тим не менш, акустичні атаки за своєю суттю підходять для цільових атак на ретельно відібрані критично важливі системи.

Акустичні сигнали, що використовуються для атаки, залежать від моделі ЖД.(рис. 3.1) [14].

Частотні діапазони атак для чотирьох моделей HDD

Модель HDD	Ємність	Діапазони частоти (Гц)
WD3200AAKS-75L9A0	320 ГБ	[2300 — 2510]
WD5000AAKS-75A7B0	500 ГБ	[2240 — 2520] [3800 — 4020] [4725 — 5006]
WD10EZEX-08WN4A0	1 ТБ	[2265 — 2281] [2455 — 2503] [6700 — 6845] [8212 — 8873] [12 839 — 12 840]
WD40EZRZ-00GXCB0	4 ТБ	[4590 — 6550] [7502 — 7900] [8398 — 8618] [9420 — 10 200]

Рис. 3.1 Частотні діапазони атак для чотирьох моделей HDD

Дослідивши акустичну атаку та її методи впливу на периферійні пристрої, пропонуємо використання датчика реагування допустимої частоти пристрою. Тобто датчик реагуватиме на наявність недопустимої частоти та буде відображати на екрані попередження. У разі якщо людина не буде знаходитись біля свого пристрою, повністю блокувати операційну систему і пристрій в цілому.

3.2. Методи захисту жорстких дисків

Метод фізичного захисту

Звернемо увагу на те, що не всі жорсткі диски повинні бути розміщені всередині комп’ютера. Жорсткі диски комп’ютера можна зберігати в окремому з`ємному корпусі, який може бути під’єднаний до хост-комп’ютера на час роботи. Це надає можливості після закінчення роботи на комп’ютері

від’єднувати від нього корпус із жорстким диском та забезпечити надійне зберігання разом із інформацією, яка міститься на ньому, у сховищі виділеного приміщення.

Метод мережевого сховища (NAS)

Суть метода *мережевого сховища (NAS)* полягає у тому, що жорсткі диски ПЕОМ зберігаються на міні-сервері, і інформація з них повертається користувачу через домашню чи офісну мережу. Перевагою цього методу є суттєве збільшення обсягу інформації, що підлягає збереженню. Замінюючи жорсткі диски або додаючи до NAS-сервера (деякі можуть вмістити до 12 жорстких дисків), можливості збільшення обсягів інформації є нескінченними. Навіть з невеликим домашнім NAS-сервером можливе зберігання мільйонів фотографій, величезної кількості аудіо та відео інформації. Сервери NAS чудово підходять для людей, які діляться своїми цифровими файлами з іншими, оскільки ви можете отримати доступ до сервера NAS через Інтернет-з'єднання. Системи NAS можуть містити місце як для традиційних жорстких дисків, так і для SSD.

Метод використання надлишкового масиву незалежних дисків (RAID)

Метод використання надлишкового масиву незалежних дисків (RAID) забезпечує підвищену надійність збереження інформації.

Цей метод може бути реалізований кількома способами, а саме:

- рівень RAID 0: перемежування;
- рівень RAID 1: віддзеркалення;
- рівень RAID 3;
- рівень RAID 5: розподілений паритет;
- рівень RAID 0 + 1 (RAID 10).

Розглянемо ці способи:

Рівень RAID 0: перемежування

Перемежування може прискорити пропускну здатність диску, оскільки він не дублює жодних даних, а лише проштовхує їх через конвеєр. Усі диски

працюють на одному рівні, але резервні копії ваших даних ніколи не створюються.

Рівень RAID 1: віддзеркалення

Віддзеркалення виконує те ж саме, що і перемежування, воно швидко переміщує дані, але дублює дані на іншому диску, тому ви завжди можете відновити дані з неушкодженого диска в разі збою диска.

Рівень RAID 3

RAID рівня 3 розподіляє інформацію на кілька дисків, але використовує один диск для зберігання основних даних. Це дозволяє відновити після збою дані але тільки якщо один диск вийшов з ладу (відновлено з «фрагментів» даних з інших дисків. Однак, якщо вийшли з ладу більше одного диска, ви можете втратити всі дані.

Рівень RAID 5: розподілений паритет

Хоча цей рівень схожий на рівень 3, цей рівень найкраще використовувати для даних, розподілених невеликими фрагментами. Великі потоки даних можуть обмежити продуктивність і безпеку.

Рівень RAID 0 + 1 (RAID 10)

Спосіб поєднання рівнів RAID. Він є дороговартістним.

Один диск дзеркально відображається на кількох альтернативних дисках, і інформація є безпечною навіть у разі збою диска, якщо несправний диск не є дзеркальним диском. Наприклад, у вас є пульт дистанційного керування, який керує кількома продуктами. Якщо один продукт виходить з ладу, ви можете використовувати інші продукти, але якщо виходить з ладу пульт дистанційного керування, нічого не працює.

Коли за допомогою портативного чи настільного комп’ютера обробляється дуже конфіденційна інформація, така як інформація про клієнтів або інше, пов’язана з роботою, кожен власник бізнесу має піклуватися про безпеку даних. Особливо ноутбуки вразливі до ризиків безпеки через їх мобільний характер. Коли ноутбук втрачається або викрадається, злом даних може дорого обійтися.

3.2.1. Метод шифрування для захисту ЖД

Існує кілька причин для захисту ноутбуків і даних у них, і, на щастя, існують різні способи пом’якшити ризики безпеки. Одним із потужних інструментів є повне шифрування диска.

Повне шифрування диска - це метод захисту даних, який перетворює інформацію на носії даних у секретний формат, який можуть зрозуміти лише люди або системи, яким дозволено доступ до інформації.

Що таке шифрування диска?

Шифрування - це спосіб зробити доступну для читання інформацію недоступною для людей, які не повинні мати до неї доступу. Коли ви шифруєте свою інформацію, її потрібно спочатку розшифрувати, перш ніж її можна буде прочитати.

Шифрування є частиною галузі криптології, науки, яка займається навмисним скремблуванням інформації. У той час як криптографічні методи понад 2000 років тому були примітивними та базовими – просто переставляючи кілька символів, - сьогоднішні методи використовують складні математичні алгоритми.

Розширений стандарт шифрування (AES) є найбільш часто використовуваним алгоритмом через його швидкість і надзвичайно високий рівень безпеки. Наразі не існує практичного способу атаки на AES, хоча метод шифрування добре відомий.

AES, також відомий як алгоритм Rijndael на честь його винахідників, ділить інформацію, яку потрібно шифрувати, на 128-бітові блоки даних, які кодуються ключем довжиною 128, 192 або 256 біт. Ці блоки записуються в двовимірну таблицю, до якої потім застосовуються різні математичні перетворення.

Двійкові дані все ще можна прочитати з жорсткого диска після того, як вони були зашифровані, але це більше не має жодного сенсу. Навіть неможливо сказати, що було зашифровано. Це можуть бути зображення, текстові файли або виконувані файли. Навіть якщо алгоритм шифрування відомий, дані не можуть

бути декодовані без правильного ключа. Так воно залишиться прихованим від незнайомців.

Чи безпечний AES?

Перевірка всіх можливих комбінацій (або «злом коду») 128-бітного ключа зайняла б кілька мільйонів років обчислювального часу. Однак завдяки сучасному апаратному забезпеченню доступ до зашифрованих даних (у поєднанні з правильним ключем) відбувається майже миттєво.

Іншими словами, ви не помітите жодних проблем з продуктивністю, коли ваші дані шифруються (під час їх збереження) та розшифровуються (під час читання чи розшифровки). Це тому, що центральний процесор вашого комп'ютера працює набагато швидше, ніж жорсткий диск може читати або записувати дані.

Чому слід використовувати шифрування жорсткого диска?

Якщо хтось отримує фізичний доступ до вашого комп'ютера, а ви не використовуєте шифрування диска, він може дуже легко вкрасти всі ваші файли.

Не має значення, чи є у вас хороший пароль, тому що зловмисник може просто завантажитися в нову операційну систему з USB-накопичувача (і обійти ваш пароль), щоб переглянути ваші файли. Або вони можуть видалити ваш жорсткий диск і помістити його в інший комп'ютер, щоб отримати доступ.

Комп'ютери стали продовженням нашого життя, а особиста інформація постійно накопичується на наших жорстких дисках. Ваш комп'ютер, ймовірно, містить робочі документи, фотографії та відео, бази даних паролів, історію веб-переглядача та іншу розрізнену інформацію, яка не належить нікому, крім вас. Ви повинні запустити повне шифрування диска на вашому комп'ютері, щоб ця інформація була конфіденційною.

Чотири вагомі причини, чому ви повинні використовувати шифрування жорсткого диска:

- Шифрування жорсткого диска вбудовано у всі основні операційні системи.

- Це єдиний спосіб захистити свої дані на випадок втрати або крадіжки ноутбука.
- Щоб розпочати та використовувати, потрібні мінімальні зусилля.
- Це унеможливлює доступ до ваших файлів іншим особам.

Як працює шифрування жорсткого диска?

Коли ви вмикаєте комп'ютер, перш ніж запустити операційну систему, ви повинні розблокувати диск, ввівши правильний ключ шифрування.

Файли, з яких складається ваша операційна система, знаходяться на вашому зашифрованому диску. Тому комп'ютер не зможе працювати з ними, поки диск не буде розблоковано.

Введення вашої парольної фрази не розблокує весь диск, а лише розблокує ключ шифрування. І ключ шифрування потім розблокує все на диску.

Але вам потрібно бути обережними, використовуючи шифрування жорсткого диска, яке можна розблокувати лише за допомогою парольної фрази, яку ви запам'ятали. Забудьте парольну фразу, і ви назавжди втратите доступ до власного комп'ютера.

Коли комп'ютер увімкнено і ви ввели парольну фразу, шифрування диска стане повністю прозорим. Все працює як зазвичай. Ваші файли відкриваються та закриваються. Ваші додатки чи програми просто працюють. І ви не помітите жодного впливу на продуктивність.

Просто пам'ятайте, що коли ваш комп'ютер увімкнено та розблоковано, той, хто його використовує, має доступ до всіх ваших файлів і даних. Тому що шифрування тепер прозоре.

ВАЖЛИВО: шифрування диска не робить ваш комп'ютер «безпечним».

Шифрування диска корисне лише проти зловмисників, які мають фізичний доступ до вашого комп'ютера. Це не ускладнює атаку вашого комп'ютера через мережу.

Усі поширені способи для злому, все ще застосовуються:

- Зловмисники все ще можуть обманом змусити встановити зловмисне програмне забезпечення.
- Ви все ще можете відвідувати шкідливі веб-сайти, які використовують помилки програмного забезпечення у вашому програмному забезпеченні, веб-сайтах чи незліченними іншими способами.
- Коли ви відвідуєте «дружні» веб-сайти, мережеві зловмисники все ще можуть таємно зробити їх шкідливими, змінюючи або перехоплюючи веб-сторінки під час передачі.
- Зловмисники все ще можуть використовувати служби, запущені на вашому комп’ютері, такі як обмін файлами в мережі, спільний доступ до музичних списків відтворення або торрент-сервіс, і це деякі з них.
- А шифрування диска не зупиняє спостереження за Інтернетом.

Способи шифрування жорсткого диска

Існує багато доступних програм шифрування, основні відмінності яких полягають у рівні складності та в тому, чи є вони безкоштовними чи платними.

Одним із варіантів шифрування диска є Bitlocker (для Windows)

BitLocker - це технологія шифрування диска Microsoft. Він включений лише до:

- Видання Ultimate і Enterprise Windows Vista і Windows 7
- Видання Windows 8 і 8.1 Enterprise і Pro

3.2.2 Практична реалізація методу шифрування

Використання даного методу полягає у шифруванні даних для посилення захисту інформації.

При виконанні даного методу було перевірено функціональність відповідно до вимог пункту 3.2.1

Поетапно опишемо процес виконання методу шифрування. Отже, для виконання даного методу необхідно здійснити такі налаштування: (Див. рис.3.2.-3.9.)

Для початку необхідно відкрити BitLocker, де можна побачити локальний диск (C:), локальний диск D (E:) та USB-дисковод(F:) (Див. рис.3.2.).

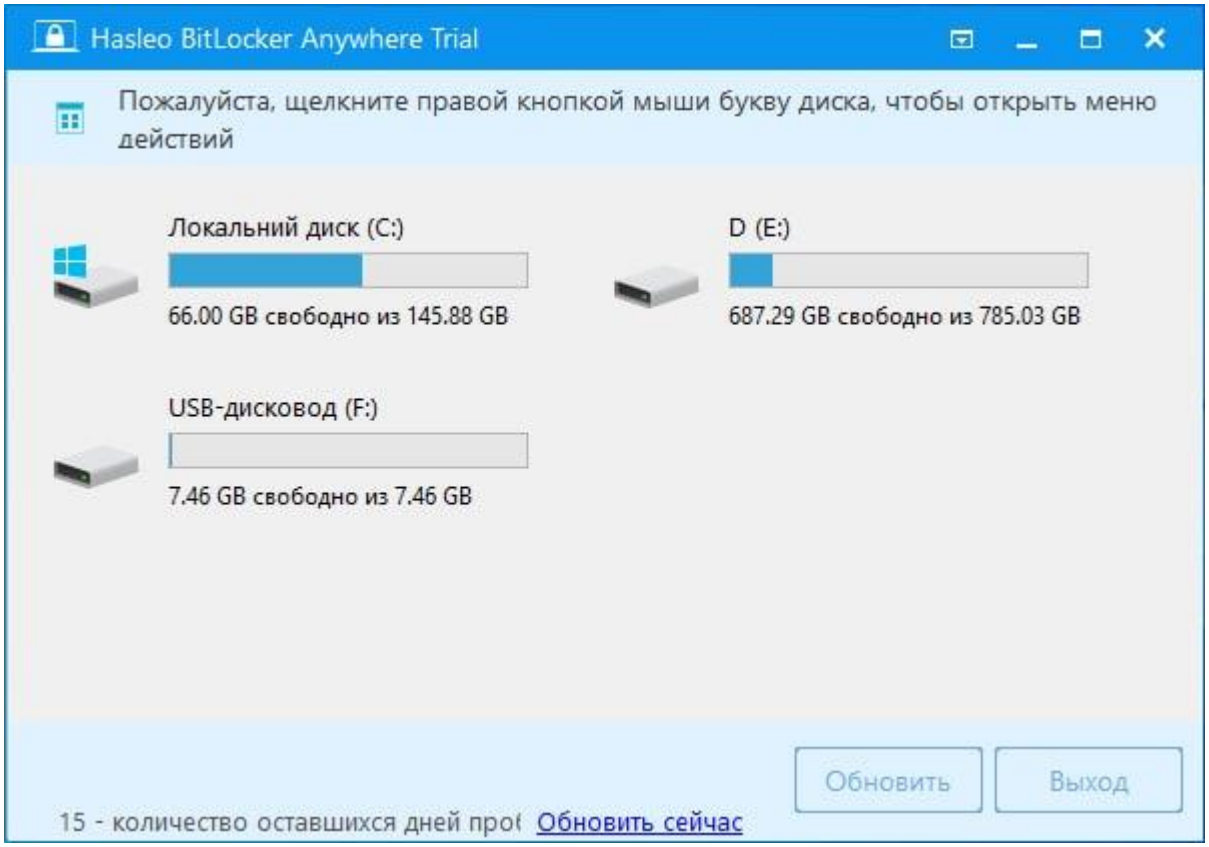


Рис. 3.2 - Налаштування BitLocker

Наступним етапом є включення BitLocker (Див. рис. 3.3)

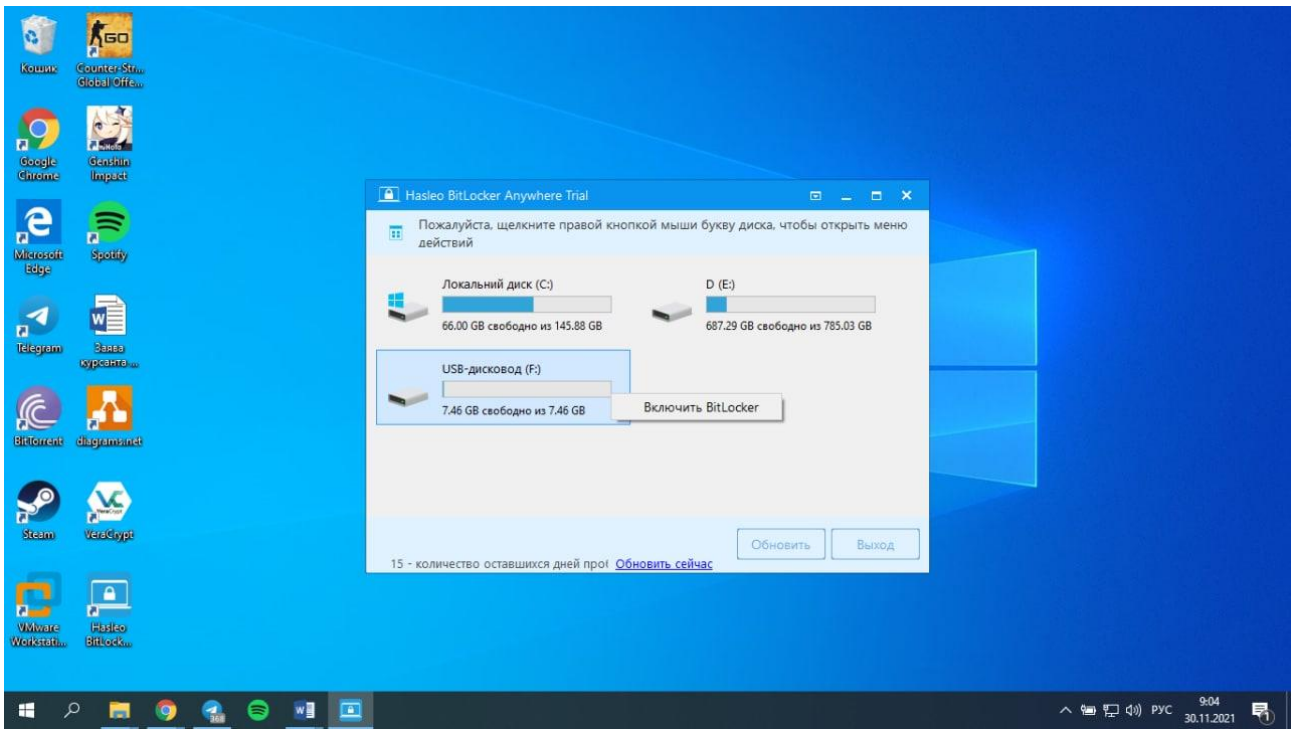
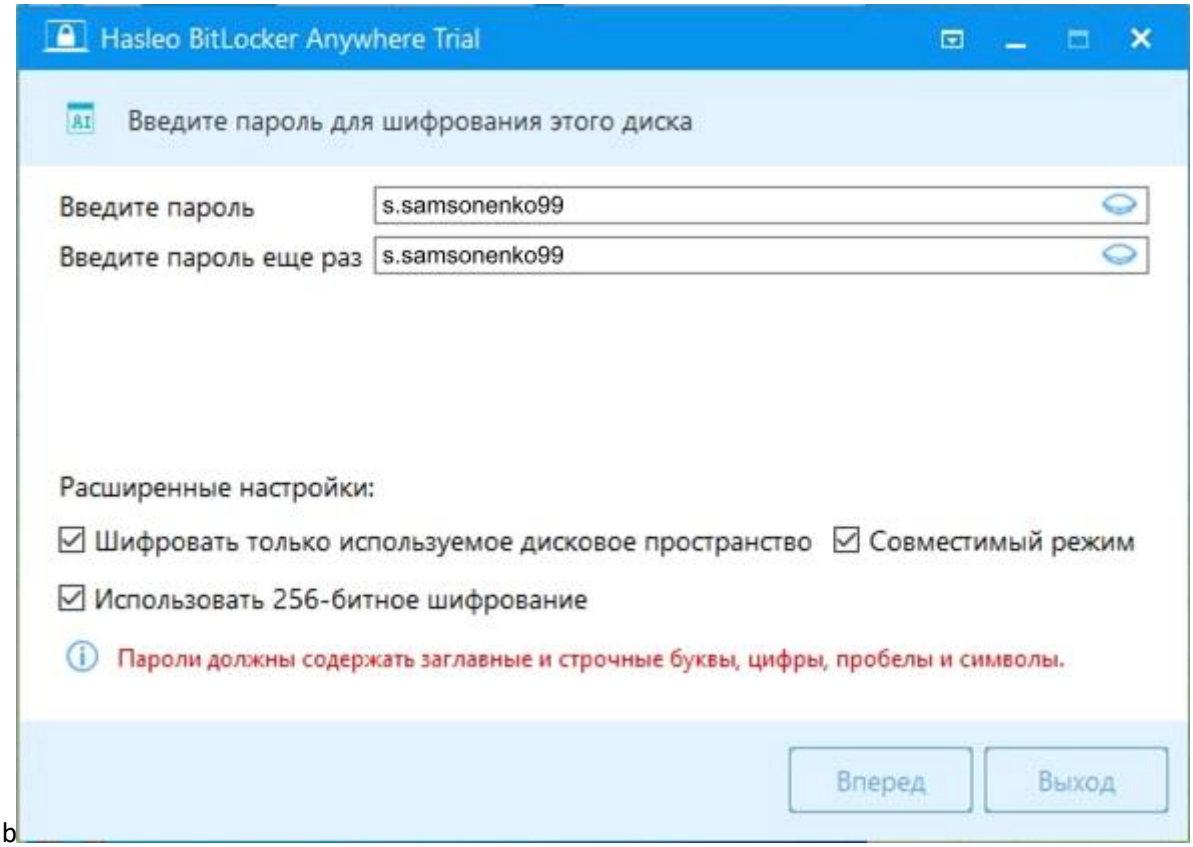


Рис. 3.3. – Включення BitLocker



]b

Рис. 3.4. - Введення паролю для шифрування диску

Як показано на рис. 3.4. після включення BitLocker необхідно вести пароль для шифрування диску. При цьому пароль повинен мати лише букви, цифри та символи.

Наступний крок полягає в резервному копіюванні ключа для відновлення доступу до диску (Див. рис. 3.5. та 3.6.)

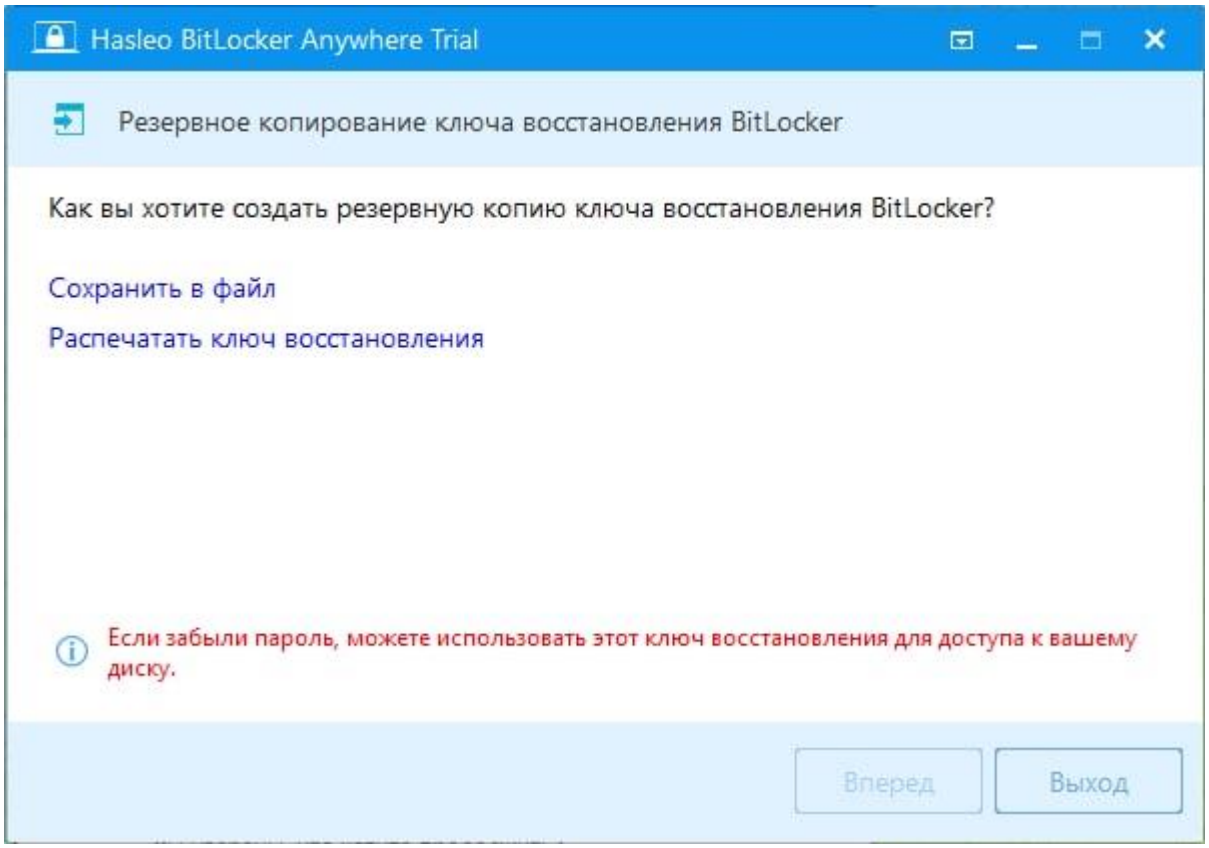


Рис. 3.5. – Резервне копіювання ключа для відновлення доступу до диску

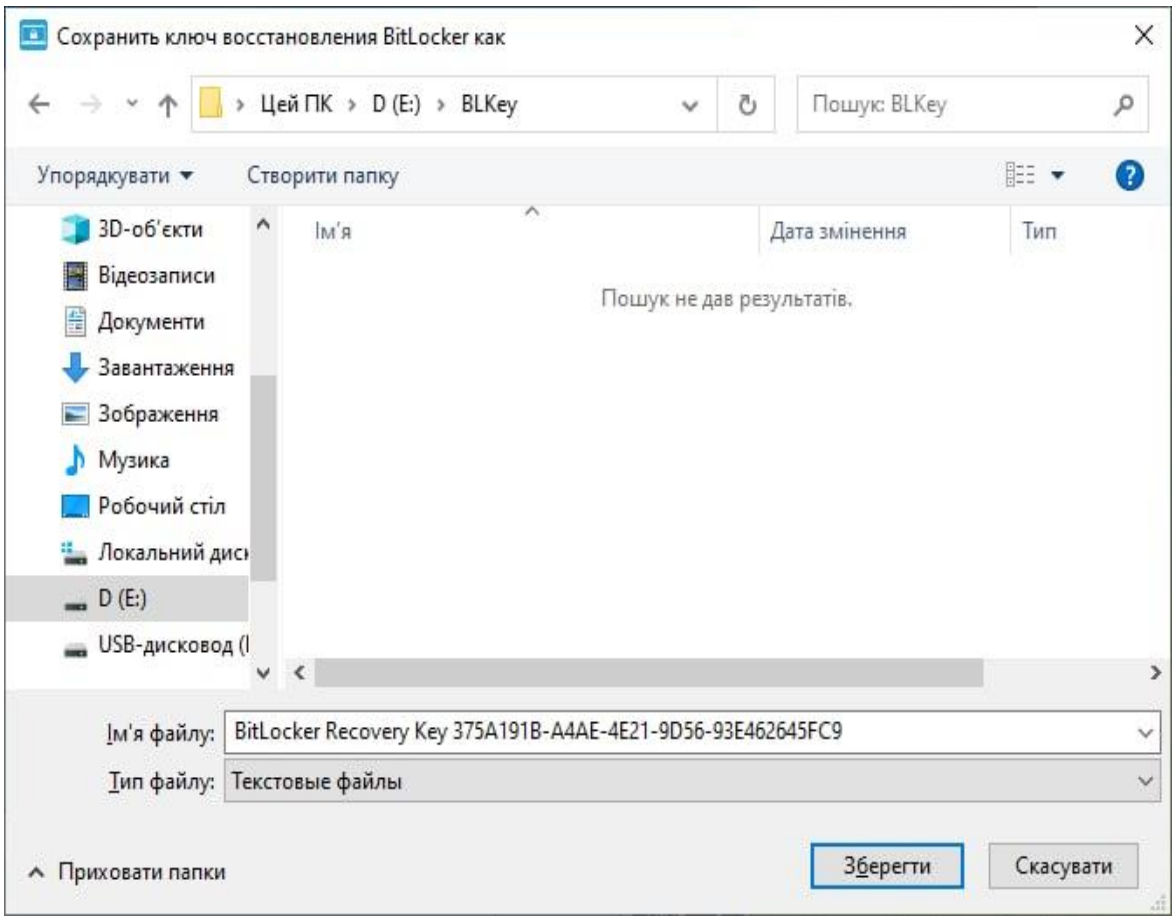


Рис. 3.6. – Вибір папки для зберігання копії ключа

Далі відбувається сам процес шифрування диску (Див. рис. 3.7.)

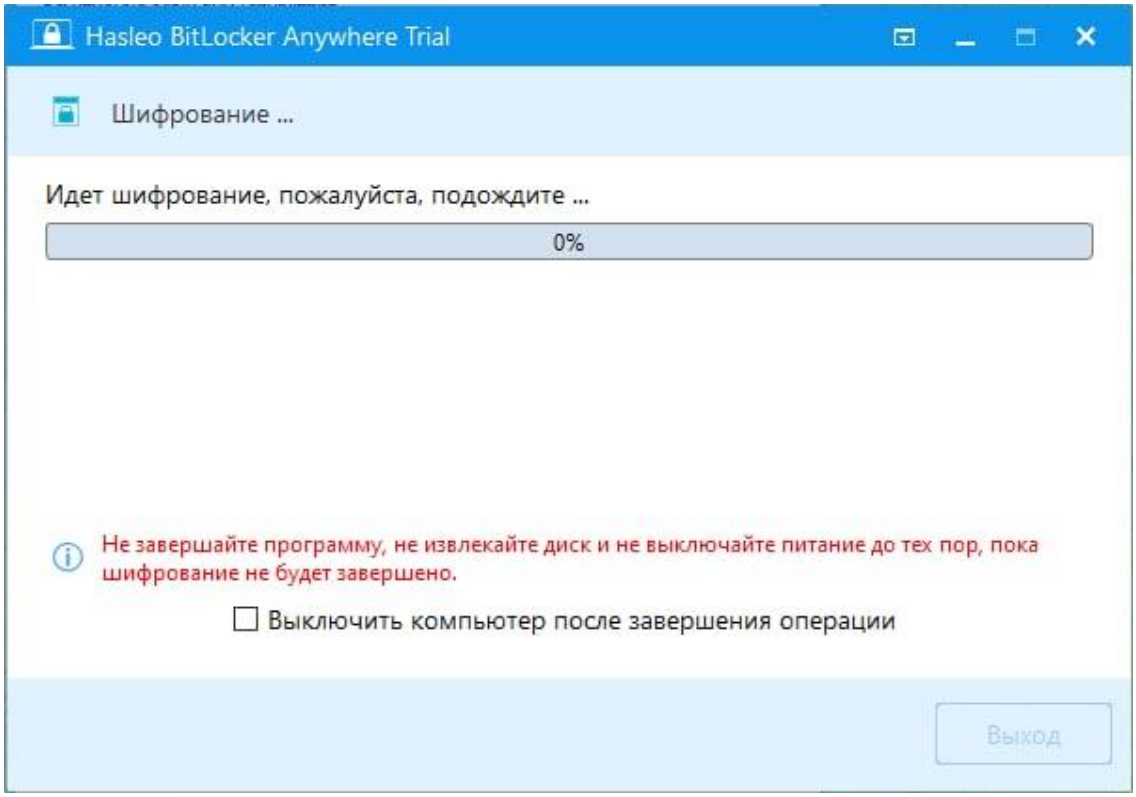


Рис. 3.7. - Шифрування диску

Як показано на рисунку 3.8. ми можемо бачити вже зашифрований диск (F:)

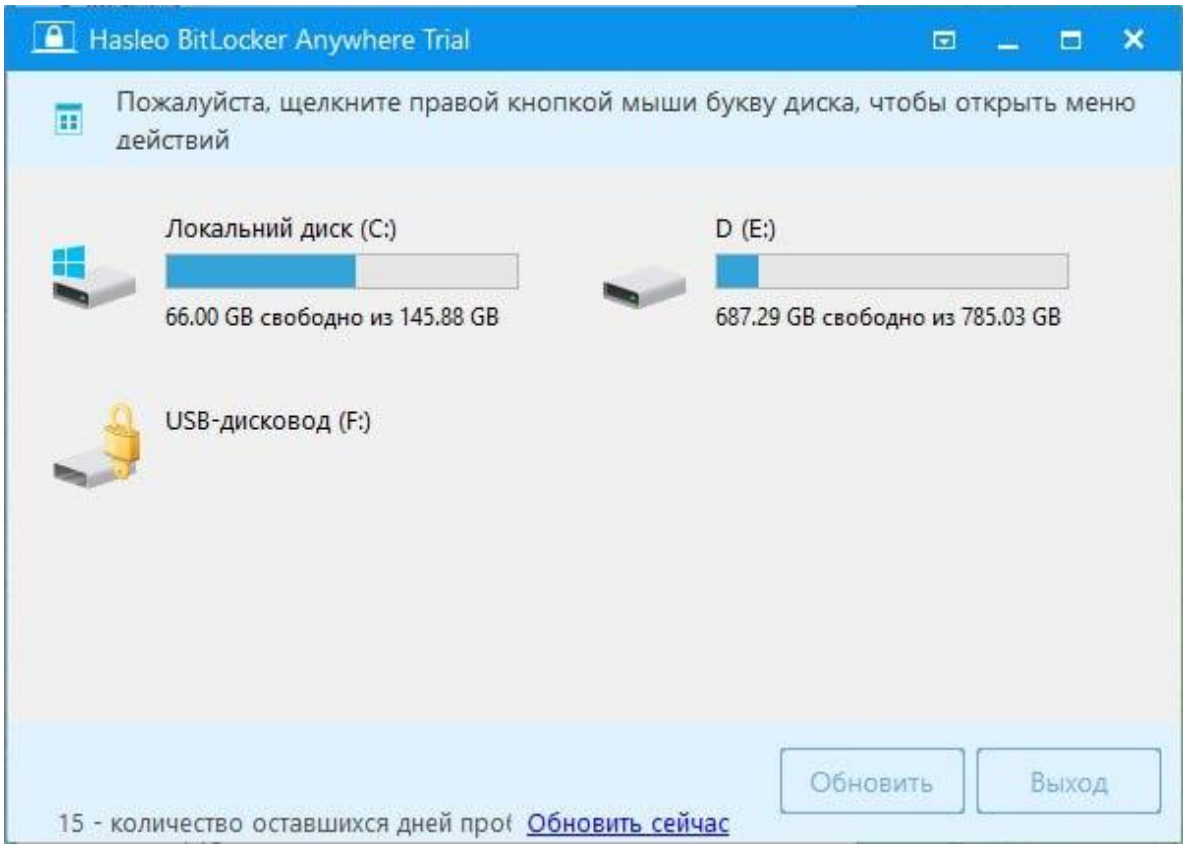


Рис. 3.8. – Зашифрований диск

Для перевірки правильної роботи BitLocker заходимо на диск (F:) та вводимо пароль для розблокування (Див. рис. 3.9.)

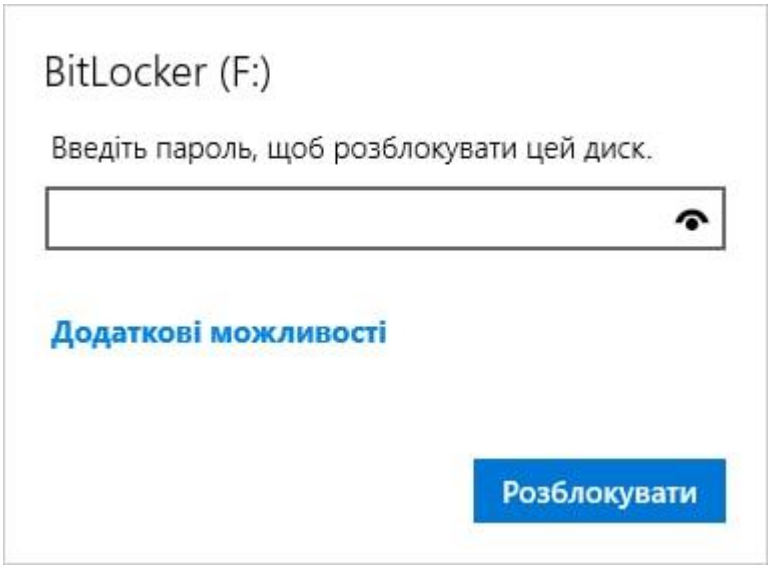


Рис. 3.9. - Введення паролю для розблокування диску

3.3. Методи знищення інформації на жорстких дисках

Що таке знищення даних?

Коли ви знищуєте дані, мета полягає в тому, щоб зробити їх абсолютно нечитабельними, незалежно від форми електронного носія, на якому вони спочатку зберігалися. Процес знищення даних також передбачає забезпечення того, що ці дані не можуть бути відновлені та використані в несанкціонованих цілях.

Знищення даних означає, що вони більше не можуть бути прочитані операційною системою або програмою. Простого видалення файлу недостатньо. Коли ви видаляєте файл на електронному пристрої, ви можете більше не бачити його, але інформація все ще зберігається на жорсткому диску, пристрої або чіпі пам'яті. Знищення даних тягне за собою перезапис поточних даних випадковими даними, доки поточні дані більше не можна буде відновити, або фактичне знищення електронного носія.

Важливість знищення даних

У сучасному світі цифровізації та залежності від електронних носіїв усі дані, які створює цей пристрій, мають бути надійно захищені. Але наприкінці свого життя його потрібно безпечно знищити. Він може містити важливу інформацію, яку ніхто не повинен мати.

Тому важливість видалення всіх даних очевидна. Однак деякі дослідження показують, що до 10 відсотків усіх використовуваних жорстких дисків, які продаються в Інтернеті, все ще містять особисту інформацію. Деякі люди не можуть видалити всі дані.

Для організації важливо врахувати ряд важливих факторів, перш ніж вирішити, як утилізувати старі дані.

Час: Кожен із різних методів, розглянутих нижче, діє в різному часовому масштабі. Знання того, скільки часу ви хочете витратити на знищення даних, може вплинути на вибір методу.

Вартість: Чи існує зацікавлення у повторному використанні старих електронних носіїв для нових цілей? Відповідь на це питання визначить тип методу знищення, який ви хочете використовувати.

Перевірка та сертифікація: Якщо ви видаляєте дані, оскільки це юридична або нормативна проблема у вашій галузі, вибраний вами метод дозволить вам продемонструвати, що ви дотримуєтесь будь-яких стандартів і вимог щодо видалення даних.

Загалом, видалення інформації на жорсткому диску може бути наслідком ряду несприятливих факторів (спонтанних або несанкціонованих дій зловмисників) або в результаті юридичних процедур, проведених працівниками за планом.

Загалом реалізацію несприятливих факторів, які можуть викликати проблеми з цілісністю та доступністю інформації на жорсткому диску, можна розділити на дві великі категорії.

- логічні пошкодження (за допомогою ПЗ): проблеми з жорстким диском, які належать до цієї категорії, пов'язані з програмним забезпеченням та способом зберігання та отримання даних у файловій системі. Це може виникнути через помилку мікропрограми, проблеми з драйверами, шкідливе програмне забезпечення, переформатування, відключення електроенергії та інші причини. Жорсткий диск, який зазнав логічних пошкоджень, працює належним чином, але дані, збережені на ньому, можуть бути недоступними. У більшості випадків ви можете відновити дані, збережені на логічно пошкодженому жорсткому диску, за допомогою програмного забезпечення для відновлення даних.

- фізичні пошкодження: з іншого боку, проблеми з жорстким диском, викликані якимось фізичним пошкодженням, заважають жорсткому диску працювати належним чином (або навіть увімкнутися взагалі). Такі проблеми включають мертві та розірвані голівки, подряпини диска та інші пошкодження, зупинення двигуна та пошкодження навколишнього середовища. Ці проблеми часто проявляються через звуки клацання та інші шуми, і їх необхідно вирішити,

перш ніж програмне забезпечення для відновлення даних можна буде використовувати для відновлення даних.

Порівняння властивостей логічних та фізичних пошкоджень жорстких дисків наведено у Таблиці 3.1.

Таблиця 3.1- Переваги та недоліки видів пошкоджень ЖД

Вид пошкодження ЖД	**Переваги**	**Недоліки**
Логічний	Безкоштовний; ЖД залишається придатним для подальшого використання	Не досить надійний
Фізичний	Безкоштовний; Не залишає ніякої можливості для відновлення даних	Необхідна професійна підготовка

Знищення інформації на жорстких дисках, яка здійснюється персоналом у плановому порядку може здійснюватись:

- *програмними методами стирання інформації;*
- *руйнуючими методами знищення інформації.*

3.3.1 Програмні методи стирання інформації

Стирання інформації на жорстких дисках

Видалення інформації на жорсткому диску є найпоширенішим способом очищення даних на жорсткому диску. Це не завжди означає найкращий шлях. Правда полягає в тому, що просте видалення інформації на жорсткому диску не видаляє інформацію взагалі, а лише переміщує її в інше місце на жорсткому

диску. Це помилкове уявлення про те, як працює «видалення», призвело до викрадення незліченної кількості особистої інформації.

Рекомендується використовувати безпечне стирання, щоб перезаписати інформацію на жорсткому диску. Правильне перезапис жорсткого диска не зможе повністю відновити інформацію на жорсткому диску за допомогою новітньої криміналістичної технології. Стандартне програмне забезпечення, яке виконує багатоетапне перезапис, може зайняти години і пропустити інформацію про пошкоджені сектори жорсткого диска. Рекомендується використовувати Secure Erase, оскільки це не залежить від BIOS вашого комп'ютера. Secure Erase перезапише все на диску, навіть пошкоджені гілки. Secure Erase тепер підключається безпосередньо до майже всіх жорстких дисків, що набагато швидше, ніж зовнішнє програмне забезпечення для перезапису.

Secure Erase - це назва набору команд, доступних із вбудованого програмного забезпечення жорстких дисків на основі PATA і SATA. Команди безпечного стирання використовуються як метод очищення даних для повного перезапису всіх даних на жорсткому диску. Це єдиний метод, який використовується всередині жорсткого диска: програма говорить ЖД «видалити дані безпечним способом», і далі контролер HDD виконує стирання даних.

Після того, як жорсткий диск був стертий за допомогою програми, яка використовує команди SecureErase, жодна програма відновлення файлів або розділів не зможе витягти дані з диска. Працює цей метод так:

Заповнення одиницями або нулями

Жодна перевірка перезапису тут не потрібна, тому що процес перезапису контролюється прошивкою жорсткого диска. Завдяки цьому, SecureErase працює швидше за інші методи очищення даних і, можливо, більш ефективно.

Докладніше про Secure Erase

Оскільки Secure Erase - це лише метод очищення даних всього диска, він недоступний для безпечного знищення окремих файлів або папок, що можуть робити файлові шредери.

Використання SecureErase для видалення даних із жорсткого диска часто вважається найкращим способом, тому що він здійснюється на низькому рівні. Ні операційна система, ні файлова система не мають відношення до процесу, коли контролер послідовно перезаписує весь жорсткий диск.

Щоб виконати команду SecureErase, необхідно використовувати програму, яка взаємодіє безпосередньо із жорстким диском. Однією з таких програм є HDD Erase.

Функція SecureErase реалізована не у всіх жорстких дисках та SSD. Деякі файлові шредери та програми очищення даних використовують слова Secure Erase у технічних характеристиках, але якщо вони спеціально не вказують на підтримку цієї функції, ймовірно вони використовують якісь інші алгоритми.

3.3.2 Руйнуючі методи знищення інформації

Руйнуючими методами знищення інформації на НЖМД є:

- метод розмагнічування;
- механічний (дезінтеграція, механічне подрібнення, проколювання);
- термічний;
- піротехнічний;
- металевотермічний;
- хімічний;
- радіаційний.

Метод розмагнічування жорстких дисків

Розмагнічування жорстких дисків є високоефективним методам знищення інформації. Розмагнічувачі, по суті, є тонко налаштованими магнітами, які при контакті з іншими магнітними носіями, такими як жорсткі диски, руйнують магнітний підпис будь-яких збережених даних. Магнітні розмагнічувачі - це обладнання для знищення даних, яке вимірюється в Ерстедах. Є багато речей, які визначають ефективність розмагнічування, але в цілому, чим вище Ерстед

рейтингу, тим потужніший розмагнічувач. Існує багато видів розмагнічувачів, які можуть сильно відрізнятися за ціною.

Механічний метод

Дезінтеграція жорстких дисків

Дезінтегратори - це типи обладнання для знищення даних, які широко використовуються в промисловості знищення та переробки даних для знищення багатьох видів матеріалів, включаючи метал. Дезінтегратори жорстких дисків, були розроблені для вирішення специфічних проблем, пов'язаних із жорсткими дисками. Дезінтегратори жорстких дисків використовують технологію ножового фрезерування, щоб постійно розрізати жорсткий диск на частини, поки вони не стануть достатньо малими, щоб провалитися через екран дезінтеграторів. Хоча дезінтеграція жорстких дисків відбувається трохи повільніше, ніж подрібнення жорстких дисків, результатом є набагато більш дрібні залишки та набагато вищий рівень безпеки. Навіть невеликий фрагмент жорсткого диска може містити тисячі частин потенційно шкідливих даних. Створення більш високого рівня знищення, мабуть, найважливіше, коли ви маєте справу з пристроями зберігання даних, такими як жорсткі диски.

Подрібнення жорстких дисків

Для подрібнення жорстких дисків потрібен тип подрібнювача, спеціально розроблений для роботи з товстими шматками металу, пов'язаними з жорсткими дисками. У подрібнювачах жорстких дисків використовуються ріжучі вали із загартованої сталі з розширеними зазорами, а також конвеєрні стрічки з синхронізацією по часу для запобігання переподачі. Залишки подрібнення жорсткого диска не схожі на тонку консистенцію подрібнювача паперу. Залишки подрібнювача жорсткого диска складаються з великих шматків металу, які залежно від того, як вони вдаряються в подрібнювальну головку, сильно відрізняються від диска до диска.

Проколювання жорстких дисків

Найпростіший спосіб очищення інформації на жорсткому диску - це фізичне її знищення. Оскільки багато жорстких дисків створені з використанням

посилених алюмінієвих корпусів і пластин із сплаву, фізичне знищення не завжди таке просте, як здається. Ось чому були створені спеціалізовані типи обладнання для знищення даних, щоб подбати про деякі важкі роботи. Деякі поширені методи фізичного знищення - свердління жорстких дисків, дроблення жорстких дисків, проколювання жорстких дисків і згинання жорстких дисків. Хоча пластини не повністю зруйновані, згинання їх пластин порушує магнітний слід, що зберігає інформацію. Хоча фізичне знищення таким чином не захищає від усіх криміналістичних методів відновлення даних, воно захищає жорсткі диски від більшості поширених типів крадіжки цифрових даних.

Термічний метод (розплавлення жорстких дисків)

Деякі експерти з безпеки вважають, що інформація на жорсткому диску не знищується, якщо його не знищити повністю. Розплавлення жорстких дисків зазвичай реалізується як завершальний етап знищення жорсткого диска. Багато центрів переробки металу приймають використані жорсткі диски як металобрухт і закладають у чан з гарячим рідким металом.

Піротехнічний метод

Основна вимога для піротехніки – це отримання максимального спеціального ефекту, тобто для різних засобів спеціальний ефект обумовлений різними факторами. Для руйнування носія, в нашому випадку ЖД, використовується вибух.

Металево-термічний метод

Знищення підкладки диска, безпосередньо на яку нанесено магнітне покриття, високою температурою високотемпературного синтезу, що самопоширюється (СВС). При цьому на підкладку у процесі виробництва наноситься спеціальний шар термітного покриття.

Хімічний метод

Руйнування робочого шару чи основи носія хімічно агресивними середовищами. При даному методі є небезпека для людини, яка використовує цей метод.

Радіаційний метод

Даний метод передбачає руйнування носія іонізуючими випромінюваннями. Він може бути екологічно небезпечним, не забезпечує надійнійне знищення інформації, при цьому потребує дороговартісного обладнання. [15]

Результати дослідження методів та ступеня надійності знищення інформації, яка зберігалась на НЖМД, наведено у Таблиці 3.2.

Таблиця 3.2 - Методи та ступінь надійності знищення інформації на НЖМД

	Методи знищення	**Реалізація методу**	**Ступінь надійності знищення інформації**
1.	**Програмні методи**		
1.1	***Стирання:***		
1.1.1	Безпечне стирання	Реалізується програмним забезпеченням SecureErase	Можливе відновлення інформації
1.1.2	Багатопрохідне перезаписування	Стандартне програмне забезпечення	Можливе часткове відновлення інформації
2.	**Руйнуючі методи знищення інформації**		
2.1	***Механічний:***		
2.1.1	Дезінтеграція	Механічне пошарове фрезерування металевого диска	Можливе гарантоване знищення
2.1.2	Механічне подрібнення	Подрібнення носія, його руйнування механічним впливом	Можливе гарантоване знищення
2.1.3	Проколювання	Механічним обладнанням проколюють носій	Можливе гарантоване знищення
2.2	***Термічний***	Нагрів носія до температури до знищення його основи(або до точки Кюрі)	Гарантоване знищення
2.3	***Піротехнічний***	Руйнування носія вибухом	Можливе гарантоване знищення. Проблема забезпечення безпеки оператора
2.4	***Металево-термічний***	Знищення основи носія високою температурою саморозповсюджуючого	Гарантоване знищення

		високотемпературного синтезу (СВС)	
2.5	**Хімічний**	Руйнування робочого шару або основи носія хімічно-агресивними засобами	Можливе гарантоване знищення. Проблема забезпечення безпеки оператора
2.6	***Радіаційний***	Руйнування носія іонізуючим опроміненням	Небезпека опромінення

Висновки до розділу 3:

Дослідивши методи атак на ЖД, методи захисту та знищення інформації на НЖМД, можна зробити висновки:

– самим актуальним методом атак на ЖД є акустичний, але для реалізації цього методу необхідна невелика дальність фізичного доступу до периферійного пристрою, на якому встановлений об’єкт атаки, або принаймні необхідно знати відомості про модель ЖД;

– в сучасному світі цифровізації захист інформації є безумовною необхідністю, для НЖМД одним з кращих засобів захисту є повне шифрування даних, що перетворює інформацію у вигляд, незрозумілий для людей. Але варто пам’ятати, що даний метод не є безпечним для атак, що виконуються на основі мережевого з’єднання, оскільки розшифрування відбувається під час запуску операційної системи (на цьому етапі вводиться ключ розшифрування);

– розглянувши методи знищення інформації на ЖД, необхідно розуміти, що програмні методи стирання небезпечні, оскільки не видаляють дані повністю, а лише змінюють місце їх зберігання або погіршують можливість доступу до них. З метою виключення будь-якої можливості відновлення інформації зловмисниками, разом із використанням цих методів необхідно обов’язково реалізовувати заходи, які виключають несанкціонований доступ сторонніх осіб до ЖД;

– гарантоване знищення інформації, яка записана (або була видалена програмними методами) на ЖД, можлива тільки руйнуючими методами;

– за результатом проведеного дослідження методів знищення інформації на ЖД (узагальнені данні наведено в таблиці 3.2) можна зробити висновок, що найбільше ефективними та економічно доцільними є термічний та металево-термічний методи знищення інформації. Завдяки, високій температурі відбувається нагрівання носія до знищення його основи (магнітного диску).

ВИСНОВКИ

Завдання, які потрібно розробити в магістерській роботі, виконані у повному обсязі. Мета роботи досягнута.

У ході проведених досліджень у обсязі поставлених завдань були зроблені такі висновки:

По-перше, галузь застосування цифрових носіїв дуже велика, їх можна використовувати як в приватних так і в державних установах. Жорсткі магнітні диски, як обов'язкові пристрої ПЕОМ із широко розгалуженою мережею практичного застосування, займають особливе місце у загальній класифікації цифрових носіїв інформації. Вони є об'єктом дослідження з метою можливого вдосконалення їх характеристик та властивостей, націлених на підвищення рівня захисту інформації, яка записана та зберігається на них.

По-друге, архітектура побудови, методи запису інформації на НЖМД не гарантують її надійне зберігання на носієві; властивості інформації можуть бути порушені в результаті атак зловмисників. Самим актуальним методом атак на ЖД є акустичний, але для реалізації цього методу необхідна невелика дальність фізичного доступу до периферійного пристрою, на якому встановлений об'єкт атаки, або принаймні необхідно знати відомості про модель ЖД. Рекомендовано використання датчиків реагування на гранично допустимі частоту та амплітуду небезпечного акустичного сигналу атаки, в залежності від моделі периферійного пристрою та ЖД, що повинно забезпечити негайне припинення обробки інформації на час атаки.

По-третє, для НЖМД одним з кращих методів захисту є повне шифрування даних, але даний метод не є безпечним для атак, що виконуються на основі мережевого з'єднання, оскільки розшифрування відбувається під час запуску операційної системи (на цьому етапі вводиться ключ розшифрування);

По-четверте, розглянувши методи знищення інформації на ЖД, необхідно розуміти, що програмні методи стирання небезпечні, оскільки не видаляють дані повністю, а лише змінюють місце їх зберігання або погіршують можливість доступу до них. З метою виключення будь-якої можливості відновлення

інформації зловмисниками, разом із використанням цих методів необхідно обов’язково реалізовувати заходи, які виключають несанкціонований доступ сторонніх осіб до ЖД;

По-п’яте, гарантоване знищення інформації, яка записана (або була видалена програмними методами) на ЖД, можливе тільки руйнуючими методами, серед яких найбільше ефективними та економічно доцільними є термічний та металево-термічний методи знищення інформації.

При виконанні магістерської роботи було запропоновано нову методику для периферійних пристроїв, а саме: використання датчиків реагування на гранично допустимі частоту та амплітуду небезпечного акустичного сигналу атаки, в залежності від моделі периферійного пристрою та ЖД, що повинно забезпечити негайне припинення обробки інформації на час атаки та запобігти несанкціонованому доступу до ПЕОМ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про електронний документообіг» та Законом України «Про електронний цифровий підпис».

2. Коженевський С.Р. Методи і засоби відновлення та знищення інформації на жорстких магнітних дисках: Автореферат., 2006. – 27с.

3. Campbell S., Jeronimo M. Applied virtualization technology. Usage models for IT professionals and software developments. – IntelPress, 2006. – 252 p.

4. Задірака 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.

5. Kriese K., Finkelstein F. Building of network of trust for Web services with RSA BSAFE Secure Web Services for Java Platform. – Режим доступу: www.rsa.com

6. Bagga W., Molva R. Policy-based cryptography and application. – Режим доступу: www.citeseer.com

7. Каминская Л. Электронная бумага: из мира научной фантастики – в реальность. – Режим доступа: http://itc.ua

8. Патент США 3 668 658: обложка диска с магнитной записью, автор Ральфа Флореса, Герберта Э. Томпсона, IBM Corporation, 6 июня 1972 года. Один из оригинальных патентов IBM на гибкие диски, в котором довольно подробно описывается структура и производство (хотя слово «дискета» здесь не используется. t используется где-либо в этом документе).

9. Патент США 4210959: Контроллер для магнитного диска, записывающего устройства и т.п. Стивен Г. Возняк, Apple Computer, Inc., 1 июля 1980 г. Этот ранний патент Apple четко объясняет работу типичного контроллера диска.

10. https://t4tutorials.com/hard-disk-components-characteristics-performance-and-hard-disk-controllers/

11. Пластиковые карты / Быстров Л.В., Воронин А.С., Гамольский А.Ю. и др. – 5-е изд., перераб. и доп. – «БДЦ-пресс», 2005. – 624 с.

12. Чеппелл Д. Виртуализация для Windows: обзор технологий. Microsoft, 2007. – 30 с. – Режим доступа: www.microsoft.ru

13. Жуков А.Е. Криптоанализ по побочным каналам. – Режим доступа: http://www.ruscrypto.ru/

14. Bellare M., Boldyrevay A. The security of chaffing-and-winnowing. – Режим доступу: www.citeseer.com 10. Krause M., Lucks S. On the minimal hardware complexity of pseudorandom function generators. – Режим доступу: www.citeseer.com

15. Научная статья опубликована 21 декабря 2017 р. https://sohabr.net/habr/post/409225/

16. Коженевский С.Р., Чеховский С., Прокопенко С., Научные исследования. - Режим доступа: www.epos.ua/view.php/about_research_datakill

ВІДОМІСТЬ МАГІСТЕРСЬКОЇ РОБОТИ

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1	А4		Титульний аркуш	1	
2	А4		Завдання на магістерську дисертацію	3	
3	А4		Реферат	6	
4	А4		Пояснювальна записка	74	
5	А4		Відгук	1	
6	А4		Рецензія	1	
7	А4		Відомість магістерської дисертації	1	