Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Засоби та механізми захисту носіїв інформації

Виконавець: студент IV курсу, групи КБ-43мс

_____ **Михайло БРЕХОВ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Іван ПАРХОМЕНКО	

Нормоконтроль	Лариса МИРУТЕНКО	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-43мс** (група) **Михайлу Брехову** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби та механізми захисту носіїв інформації

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Мова програмування Python, хеш-функція для забезпечення цілісності інформації SHA-256, засоби реалізації та функціонування застосунку

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база у сфері захисту інформації, класифікація носіїв інформації, загрози та вразливості, принципи захисту, засоби захисту носіїв інформації, механізми захисту носіїв інформації, опис застосунку для забезпечення цілісності, архітектура застосунку, застосунок для забезпечення цілісності інформації

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Застосунок для захисту цифрових носіїв інформації від модифікації та спотворення інформації на основі хеш-функції SHA-256

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Михайло БРЕХОВ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 04.11.2022	*виконано*
2	Аналіз відкритих	23.01.2023 – 24.02.2023	*виконано*
3	Аналіз нормативно-правової бази та класифікація носіїв інформації	27.02.2023 – 10.03.2023	*виконано*
4	Дослідження загроз та вразливостей носіїв інформації. Огляд принципів захисту	13.03.2023 – 02.04.2023	*виконано*
5	Дослідження засобів захисту носіїв інформації	03.04.2023 – 09.04.2023	*виконано*
6	Дослідження механізмів захисту носіїв інформації	10.04.2023 – 16.04.2023	*виконано*
7	Опис розроблюваного застосунку	17.04.2023 – 23.04.2023	*виконано*
8	Дослідження хеш-функції застосунку та розгляд методів реалізації	24.04.2023 – 07.05.2023	*виконано*
9	Реалізація застосунку для забезпечення цілісності	08.05.2023 – 28.05.2023	*виконано*
10	Оформлення пояснювальної записки та підготовка до захисту	29.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Іван ПАРХОМЕНКО (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Михайло БРЕХОВ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 61 сторінку, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить 2 додатки із загальною кількістю сторінок 5. У пояснювальній записці кваліфікаційної роботи міститься 25 рисунків та посилання на 25 літературних джерел.

Метою роботи є розробка застосунку захисту цифрових носіїв інформації від модифікації та спотворення на основі хеш-функції SHA-256.

Об'єктом дослідження є процес захисту інформації від модифікації та спотворення на цифрових носіях інформації.

Предметом дослідження є набір методів та механізмів, що реалізують процес забезпечення цілісності цифрових носіїв інформації.

Методи дослідження:

- аналіз відкритих джерел;
- класифікація носіїв інформації, їх загроз та вразливостей;
- опис засобів та механізмів захисту носіїв інформації.

Практичною цінністю є розроблений застосунок для захисту цифрових носіїв інформації від модифікації та спотворення інформації на основі хеш-функції SHA-256.

Новизна: розроблений застосунок захисту цифрових носіїв інформації від модифікації та спотворення, який реалізує забезпечення цілісності інформації на основі хеш-функції SHA-256.

Ключові слова: захист інформації, носії інформації, загрози, вразливості, шифрування, цілісність, аутентифікація, контроль доступу, хеш-функція.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

КСЗІ	–	Комплексна система захисту інформації
RSA	–	Rivest-Shamir-Adleman
AES	–	Advanced Encryption Standard
DES	–	Data Encryption Standard
HDD	–	Hard Disk Drive
SSD	–	Intrusion Prevention System
DDoS	–	Denial of Service
ПЗ	–	Програмне забезпечення
2FA	–	Two-Factor Authentication
IDS	–	Intrusion Detection System
CRC	–	Cyclic Redundancy Check
ISO	–	International Organization for Standardization
GUI	–	Graphical User Interface
ООП	–	Об'єктно-орієнтоване програмування
SHA	–	Secure Hash Algorithm

ВСТУП

Засоби та механізми захисту носіїв інформації є одним з найважливіших аспектів у сучасному цифровому світі. З огляду на постійний розвиток технологій та збільшення кількості цифрової інформації, яка зберігається та передається через різні канали, необхідність ефективного захисту носіїв інформації стає критичною.

У міру зростання кількості атак на цифрові системи та збільшення складності технологій, виникає потреба у вдосконаленні засобів та механізмів захисту. Недостатня безпека може призвести до крадіжки особистих даних, фінансових втрат, порушення конфіденційності та порушення довіри.

Історія захисту носіїв інформації охоплює багато століть розвитку та еволюції методів захисту конфіденційної інформації. Вже в давні часи люди використовували різні методи шифрування та інших технік, щоб зберегти інформацію в секреті та запобігти несанкціонованому доступу до неї.

Одним з найвідоміших прикладів історії захисту інформації є «Шифр Цезаря», який використовувався в Давньому Римі. У цьому методі кожна буква повідомлення замінялася на іншу, що розташована на певну кількість позицій в алфавіті. Це дозволяло зберегти важливу інформацію в секреті, оскільки тільки особа з ключем могла розшифрувати повідомлення.

З розвитком технологій у XX столітті з'явилися нові методи захисту інформації. Виникла потреба у більш складних криптографічних алгоритмах та системах шифрування. У цей період розроблялися різні методи шифрування, такі як шифр Хілла, шифр Вернама, шифр DES та інші. Ці методи використовувалися для захисту важливої інформації під час війн, дипломатичних переговорів та комерційних операцій.

З появою комп'ютерів та Інтернету в другій половині XX століття стало ще важливіше захищати носії інформації від несанкціонованого доступу. Розвиток криптографічних алгоритмів, таких як RSA, AES та інші, дозволив забезпечити більшу безпеку під час передачі та зберігання інформації.

Проте, з ростом кількості цифрової інформації та появою нових технологій, таких як штучний інтелект та блокчейн, виникають нові виклики і загрози для захисту носіїв інформації. Сучасні методи захисту повинні враховувати можливість кібератак, викрадення даних, підробку та інші загрози, які виникають у цифровому середовищі.

Таким чином, дана робота присвячена дослідженню засобів та механізмів захисту носіїв інформації в контексті сучасності. Робота спрямована на вивчення засобів та механізмів захисту носіїв інформації, а також враховує можливі виклики, загрози та вразливості для носіїв інформації, що існують на сьогоднішній день.

Відомості, отримані в результаті дослідження, можуть бути використані для впровадження вдосконалених заходів безпеки в організаціях, а також сприяти розвитку нових методів та алгоритмів захисту носіїв інформації. Оскільки безпека інформації залишається важливою складовою сучасного світу, розуміння та покращення захисту носіїв інформації стає невід'ємною умовою для сталого розвитку технологій та суспільства в цілому.

Актуальність роботи: проблема захисту носіїв, які виконують функцію збереження інформації є доволі актуальною. Компанії та підприємства, від малих до великих, а також кожен окремий користувач зберігають інформацію, яка має велику вартість і може бути шкодливо використана, модифікована або спотворена, якщо потрапить у недоброчесні руки. Для забезпечення захисту носіїв інформації потрібно розуміти, які є засоби та механізми їх захисту та як їх використовувати.

Метою роботи є розробка застосунку захисту цифрових носіїв інформації від модифікації та спотворення на основі хеш-функції SHA-256.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні *завдання:*

- проаналізувати види та класифікацію носіїв інформації;
- проаналізувати теоретичні засади захисту носіїв інформації;
- провести дослідження засобів та механізмів захисту носіїв інформації;
- реалізувати застосунок для забезпечення цілісності інформації на цифрових носіях інформації.

Об’єктом дослідження є процес захисту інформації від модифікації та спотворення на цифрових носіях інформації.

Предметом дослідження є набір методів та механізмів, що реалізують процес забезпечення цілісності цифрових носіїв інформації.

Методи дослідження:

- аналіз відкритих джерел;
- класифікація носіїв інформації, їх загроз та вразливостей;
- опис засобів та механізмів захисту носіїв інформації.

Практичною цінністю є розроблений застосунок для захисту цифрових носіїв інформації від модифікації та спотворення інформації на основі хеш-функції SHA-256.

РОЗДІЛ 1
АНАЛІЗ ТЕОРЕТИЧНИХ ЗАСАД ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ

1.1 Аналіз нормативно-правової бази у сфері захисту інформації

Питання захисту носіїв інформації є питанням захисту інформації в цілому, через те, що інформація яку потрібно захищати не існує без її носіїв, а носії без інформації не варті захисту. Для поступового розкриття цього питання потрібно проаналізувати нормативно-правову бузу України у сфері захисту інформації, яка складається з Законів України, постанов Кабінету Міністрів України (КМУ), та інших нормативних документів.

Фундаментом, що регулює сферу інформаційних відносин в країні є Закон України «Про інформацію» прийнятий у 1992 році. Метою цього Закону є забезпечення прав громадян на інформацію та визначення принципів доступу до інформації, її розповсюдження, збереження і використання [1]. Основними положеннями Закону є:

- Право на інформацію: Закон гарантує право громадян на одержання, пошук, отримання та поширення інформації без будь-яких обмежень, крім випадків, передбачених Законом.
- Засади доступу до інформації: Закон встановлює принципи відкритості і прозорості діяльності органів державної влади та органів місцевого самоврядування. Органи влади повинні надавати інформацію громадянам відповідно до Закону та у встановлені строки.
- Конфіденційність інформації: Закон визначає категорії інформації, які можуть бути обмежені в розповсюдженні з метою захисту національної безпеки, громадського порядку, охорони здоров'я тощо. Процедура обмеження доступу до такої інформації повинна бути законною і обґрунтованою.
- Захист інформації: Закон передбачає заходи щодо захисту інформації, що становить комерційну, авторську або іншу конфіденційну інформацію. Він також

встановлює відповідальність за незаконне розповсюдження або використання інформації.

- Доступ до публічної інформації: Закон встановлює правила щодо доступу до публічної інформації, яка належить до сфери діяльності органів державної влади та органів місцевого самоврядування. Органи влади повинні забезпечувати доступ до такої інформації та розповсюджувати її відповідно до Закону.
- Контроль за дотриманням Закону: Закон передбачає інститути, які здійснюють контроль за дотриманням законодавства про інформацію, включаючи Уповноваженого з прав людини, судові та інші органи.

Одним із основних законодавчих актів, який визначає загальні принципи захисту інформації, є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 року. Цей Закон містить положення щодо організації захисту інформації, визначення класів інформації за ступенем її важливості, права і обов'язки суб'єктів інформаційних відносин у сфері захисту інформації [2]. Основними положеннями цього Закону є:

- Предмет і сфера застосування: Закон встановлює норми щодо організації та здійснення захисту інформації в інформаційно-телекомунікаційних системах. Він поширюється на всі суб'єкти інформаційних відносин, які мають доступ до інформації, включаючи органи державної влади, органи місцевого самоврядування, підприємства, установи та громадян.
- Класифікація інформації: Закон розрізняє інформацію за її важливістю та ступенем конфіденційності. Інформацію поділяють на різні класи, такі як державна таємниця, комерційна таємниця, персональні дані тощо. Кожному класу інформації призначається відповідний рівень захисту та встановлюються вимоги до суб'єктів, що працюють з цією інформацією.
- Заходи забезпечення захисту інформації: Закон передбачає низку заходів для забезпечення безпеки інформації. Це включає захист від несанкціонованого доступу до інформації, забезпечення цілісності та конфіденційності даних, контроль доступу до інформації, резервне копіювання та відновлення даних, захист від комп'ютерних вірусів та зловмисного програмного забезпечення.

- Відповідальність за порушення: Закон встановлює відповідальність за порушення правил захисту інформації. Суб'єкти, які не дотримуються вимог Закону або спричиняють шкоду інформаційній безпеці, можуть бути притягнуті до відповідальності, включаючи штрафну, дисциплінарну або кримінальну відповідальність.
- Органи контролю та регулювання: Закон визначає органи, відповідальні за контроль і регулювання в сфері захисту інформації. До них належать спеціалізовані державні органи, такі як Державна служба спеціального зв'язку та захисту інформації України, які здійснюють нагляд, аудит та атестацію інформаційно-телекомунікаційних систем.
- Міжнародне співробітництво: Закон сприяє розвитку міжнародного співробітництва в сфері захисту інформації.

Важливими є Закон України «Про державну таємницю» прийнятий у 1994 році та Закон України «Про захист персональних даних» прийнятий у 2010 році. Обидва Закони, визначають важливі аспекти регулювання доступу до інформації та захисту даних в Україні.

Серед постанов КМУ потрібно виділити дві:

1. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 року. Ця постанова встановлює правила і вимоги щодо захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [3]. Основні положення постанови включають:

- Класифікація інформації: визначаються категорії інформації залежно від ступеня її конфіденційності, а також встановлюються вимоги щодо захисту інформації кожної категорії.
- Заходи забезпечення захисту: встановлюються вимоги до засобів захисту інформації, включаючи захист від несанкціонованого доступу, збереження конфіденційності, цілісності та доступності інформації.

- Організаційні заходи: встановлюються вимоги щодо організації захисту інформації, включаючи призначення відповідальних осіб, проведення аудиту безпеки інформації, надання навчання та підготовки працівників.

2. «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 року. Ця постанова встановлює типову інструкцію, яка регулює порядок обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [4]. Основні положення постанови включають:

- Облік документів: встановлюється порядок обліку документів, включаючи їх реєстрацію, ведення картотек та систематизацію.
- Зберігання документів: встановлюються вимоги щодо зберігання документів, включаючи умови зберігання, охорону від втрати, пошкодження або незаконного доступу.
- Використання і знищення документів: встановлюються правила щодо використання документів, їх передачі, архівації та знищення відповідно до встановлених процедур.

Окрім Законів України та постанов КМУ, сферу захисту інформації регулює низка нормативних документів в галузі технічного захисту інформації та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ. Ці документи встановлюють стандарти та вимоги, які охоплюють різні аспекти захисту носіїв інформації та сприяють забезпеченню конфіденційності, цілісності та доступності інформації. Вони допомагають організаціям реалізувати ефективні заходи для забезпечення безпеки інформації.

Україна активно співпрацює з міжнародними організаціями у сфері захисту інформації. Захист інформації є важливою складовою національної безпеки України, і країна прагне співпрацювати з міжнародними партнерами для підвищення своїх можливостей в цій галузі [5]. Україна співпрацює з Європейським Союзом (ЄС) у рамках Європейської агенції з безпеки мереж і інформації (ENISA) та інших ініціатив. Україна бере участь у програмі «Горизонт Європа» з питань дослідження та

інновацій, де пропонується підтримка проектів у сфері кібербезпеки. Україна бере активну участь у роботі груп та проектів, спрямованих на забезпечення кібербезпеки та обмін досвідом з іншими країнами. Україна підтримує багатосторонні ініціативи з кібербезпеки, такі як Європейський центр кіберзлочинності (EC3) та Міжнародний союз з телекомунікацій (ITU), і активно співпрацює з іншими країнами у рамках цих ініціатив.

Підсумовуючи, нормативно-правова база України у сфері захисту інформації є всебічною та адаптивною, що дуже важливо наразі, коли розвиток, впровадження та розповсюдження інформаційних технологій у житті окремого громадянина та держави в цілому є настільки стрімким.

1.2 Класифікація та опис носіїв інформації

Для подальшого розкриття теми роботи потрібно визначити, що являють собою носії інформації. Отже, носії інформації – це фізичні або електронні засоби, призначені для зберігання, передачі та обробки даних. Вони використовуються для збереження інформації різного типу, включаючи текст, зображення, відео, звук та інші. Кожен носій інформації – це матеріальний об'єкт, який містить відомості, доступні або лише для людини, або лише для обчислювальної машини, або, нарешті, одночасно і для людини, і для машини [6]. У зв'язку з цим усі носії ми можемо підрозділяти на:

- людиночитані;
- машиночитані (машинні);
- комбіновані.

Носії інформації можна класифікувати за різними критеріями, такими як фізична форма, спосіб зберігання, доступність для запису та зчитування, масштабованість та інше.

Ось кілька загальних типів носіїв інформації:

- Паперові носії: це традиційний тип носіїв інформації, що використовує папір для запису даних. Сюди входять книги, журнали, газети, листи та інші документи, які можна читати і писати вручну.
- Оптичні диски: це носії інформації, які використовують принцип оптики для запису та зчитування даних. Зокрема, CD (компакт-диск), DVD (цифровий відеодиск) і Blu-ray диск входять до цієї категорії. Вони здатні зберігати значні обсяги даних і використовуються для музики, фільмів, програмного забезпечення тощо (рис. 1.1).

Рисунок 1.1 – Оптичний диск

- Жорсткі диски: це носії інформації, що складаються з магнітного диска, який зберігає дані, та механізму для його зчитування та запису. HDD зазвичай використовуються для зберігання даних на комп'ютерах та серверах (рис. 1.2).

Рисунок 1.2 – Жорсткий диск

- Флеш-накопичувачі: це невеликі пристрої, що використовують флеш-пам'ять для зберігання інформації. USB-флешки, SD-карти, SSD - це деякі приклади флеш-накопичувачів. Вони мають велику ємність, швидкість передачі даних і зручні для перенесення (рис. 1.3).

Рисунок 1.3 – USB-флешка

- Хмарні носії: зберігання даних в Інтернеті, відоме як хмарне зберігання. Дані зберігаються на віддалених серверах і доступні через Інтернет (рис. 1.4). Популярні сервіси хмарного зберігання включають Dropbox, Google Drive, Microsoft OneDrive та інші.

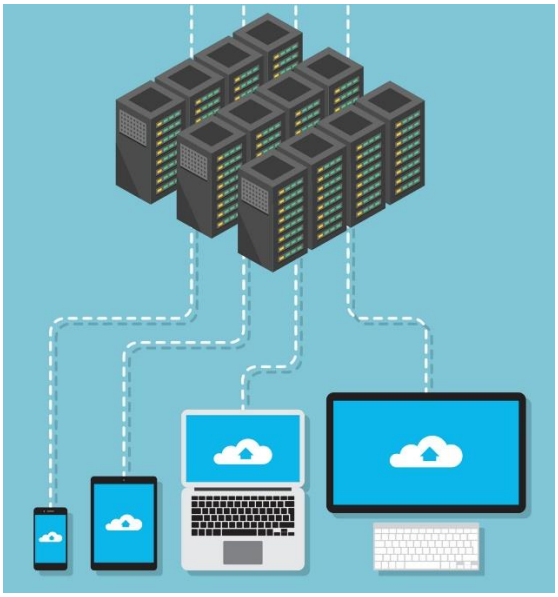

Рисунок 1.4 – Схема роботи хмарного зберігання інформації

- Магнітні стрічки: це носії інформації, які використовуються для довгострокового зберігання великих обсягів даних. Їх використовують у

великих підприємствах і установах для архівування і резервного копіювання (рис. 1.5).

Рисунок 1.5 – Магнітна стрічка

- Електронні накопичувачі: до цієї категорії входять флеш-пам'ять, жорсткі диски, Solid State Drives (рис. 1.6) та інші електронні пристрої, що використовуються для зберігання даних. Вони використовуються в різних пристроях, від комп'ютерів і ноутбуків до мобільних телефонів та планшетів.

Рисунок 1.6 – SSD

Це лише кілька загальних типів носіїв інформації, існує багато інших варіантів, які можуть використовуватися в різних сферах діяльності. Розвиток технологій безперервно призводить до появи нових типів носіїв інформації та засобів зберігання даних.

В роботі увага буде приділена цифровим носіям інформації. Цифрові носії інформації – це електронні пристрої, що використовуються для зберігання, передачі та обробки цифрових даних. Вони здатні зберігати великі обсяги інформації у цифровому форматі, що відображається у вигляді послідовності бітів (1 і 0).

Інформація в цифровому форматі є доступною та відомою для кожного, хто користується комп'ютерами, ноутбуками, смартфонами або планшетами. Це можуть бути індивідуальні користувачі, організації, підприємства тощо, які зберігають свої особисті дані, фотографії, відео, музику та інше.

Кожен тип цифрових носіїв інформації має свій механізм та принцип роботи для запису, збереження та зчитування інформації, але при роботі з ними користувач майже не буде бачити різниці.

Ось кілька загальних типів цифрових носіїв інформації:

- HDD: це електронні пристрої, що складаються з магнітного диска, який зберігає дані, та механізми для їх зчитування та запису. Жорсткі диски широко використовуються в комп'ютерах і серверах для зберігання оперативної і постійної інформації.
- Флеш-накопичувачі (Flash Drives): це малий електронний пристрій, який використовує флеш-пам'ять для зберігання і передачі даних. USB-флешки є одним з найпоширеніших типів флеш-накопичувачів. Вони мають велику ємність, швидкість передачі даних і зручні для перенесення.
- SSD: це пристрої зберігання, які використовують флеш-пам'ять для зберігання даних без рухомих частин, таких як рухомий головка в жорсткому диску. SSD зазвичай мають вищу швидкість передачі даних і надійніші, але вони можуть бути дорожчими за HDD.
- Оптичні диски: цифрові носії інформації, які використовують принцип оптики для запису і зчитування даних. Це включає CD (компакт-диск), DVD (цифровий відеодиск) і Blu-ray диск. Оптичні диски широко використовуються для зберігання музики, фільмів, програмного забезпечення тощо.

- Карти пам'яті: це маленькі електронні пристрої, які використовуються для зберігання інформації на мобільних пристроях, фотоапаратах, планшетах і т. д. Вони можуть використовувати різні формати, такі як SD-карти, MicroSD-карти, CompactFlash і т. д. (рис. 1.7).

Рисунок 1.7 – Карти пам'яті

- Хмарне зберігання: зберігання даних на віддалених серверах через Інтернет. Дані зберігаються на серверах хмарних сервісів, таких як Dropbox, Google Drive, Microsoft OneDrive тощо, і доступні для користувачів з будь-якого пристрою з підключенням до Інтернету.

Цифровий формат зберігання та обробки інформації є найбільш поширеним на сьогодні, бо він має певні суттєві переваги, до них можна віднести:

- Збереження та доступність: цифрова інформація може бути збережена на різних носіях, таких як жорсткі диски, флеш-накопичувачі, хмарні сервіси тощо. Вона займає менше простору порівняно з традиційними фізичними носіями, такими як паперові документи або фізичні копії. Крім того, цифрова інформація може бути легко організована і пошукова за допомогою різних алгоритмів і систем управління даними.
- Легкість передачі: цифрова інформація може бути легко передана через Інтернет або електронні канали зв'язку. Це дозволяє швидко і ефективно обмінюватися даними між різними користувачами та організаціями навіть на великі відстані.
- Легкість копіювання та резервного копіювання: цифрова інформація може бути легко скопійована, створюючи точні копії без втрати якості. Це

робить процес резервного копіювання і збереження даних надійнішим і зручнішим.

- Можливості обробки та аналізу: цифрова інформація може бути легко оброблена та аналізована за допомогою різноманітних програмних засобів. Вона може бути піддана комп'ютерним алгоритмам, статистичним обчисленням, штучному інтелекту тощо, що дозволяє отримати цінні знання та висновки з великих обсягів даних.
- Можливості візуалізації: цифрова інформація може бути легко візуалізована у вигляді графіків, діаграм, таблиць, відео, зображень тощо. Це допомагає зрозуміти та представити дані в більш зручний та доступний спосіб.
- Можливості пошуку та сортування: цифрова інформація може бути ефективно сортована, фільтрована та швидко знайдена за допомогою різних алгоритмів та інструментів пошуку. Це дозволяє швидко знаходити необхідні дані та зберігати час при пошуку інформації.

Кожен з перелічених типів носіїв інформації в цілому та цифрової інформації зокрема має свої певні специфічні заходи для забезпечення захисту інформації, деякі заходи є універсальними, деякі специфічними. В роботі сконцентруємося на забезпеченні захисту цифрових носіїв інформації.

1.3 Основні загрози та вразливості носіїв інформації

В даному підрозділі розберемо основні загрози та вразливості для носіїв інформації. З попереднього підрозділу відомо про різноманіття носіїв інформації, тому кожен з типів носіїв інформації крім універсальних має свої особливі загрози та вразливості. Для зручності поділимо носії інформації на традиційні та цифрові, та розглянемо їх окремо.

1.3.1 Основні загрози та вразливості традиційних носіїв інформації

Традиційні носії інформації, такі як паперові документи, фотографії, магнітні стрічки та інші фізичні носії, є важливими засобами збереження та передачі даних. Проте, вони загрози та вразливості, які можуть призвести до втрати, пошкодження або незаконного доступу до інформації. Розглянемо основні загрози та вразливості традиційних носіїв інформації і розкриємо деталі та нюанси цих проблем:

- Втрата та пошкодження: традиційні носії інформації, такі як паперові документи або фотографії, можуть бути втрачені або пошкоджені через пожежу, повінь, крадіжку або інші фізичні небезпеки. Втрата цих носіїв може призвести до незворотного втрати даних і важливої інформації.
- Обмежений доступ та пошук: пошук інформації на традиційних носіях може бути часомірним і складним завданням. Навіть з належним упорядкуванням та систематизацією, пошук конкретної інформації може зайняти значну кількість часу і зусиль. Крім того, обмежені можливості копіювання та розповсюдження таких носіїв можуть ускладнити доступ до інформації.
- Вразливість до фізичних пошкоджень: традиційні носії інформації, такі як паперові документи або магнітні стрічки, піддаються фізичним пошкодженням, таким як зіпсування, розриви, зношення тощо. Це може спричинити втрату або незчитуваність інформації, особливо якщо немає резервних копій.
- Незахищеність від несанкціонованого доступу: традиційні носії інформації, такі як документи або фізичні носії з даними, можуть бути вразливими до несанкціонованого доступу. Незахищені примірники можуть бути вкрадені або викрадені, надаючи зловмисникам доступ до конфіденційної інформації. Крім того, традиційні носії не можуть забезпечити жорсткого контролю доступу та автентифікації.
- Обмежена масштабованість та мобільність: одна з вразливостей традиційних носіїв інформації полягає в їх обмеженій масштабованості та

мобільності. Вони займають фізичний простір і вимагають спеціальних умов зберігання та транспортування. Це може обмежити швидкість та ефективність передачі та обміну даними.

- Пошкодження в результаті впливу чинників навколишнього середовища: традиційні носії інформації можуть бути пошкоджені під впливом чинників навколишнього середовища, таких як волога, висока або низька температура, ультрафіолетове випромінювання тощо. Це може призвести до погіршення якості інформації або повної втрати.
- Витрати на зберігання та обробку: збереження та обробка традиційних носіїв інформації вимагають фізичного простору, обладнання та ресурсів. Витрати на зберігання, розподіл, оновлення та забезпечення безпеки можуть бути значними, особливо в разі великого обсягу даних.
- Обмежена можливість резервного копіювання: традиційні носії інформації можуть бути вразливими до втрати даних без можливості відновлення через обмежену можливість резервного копіювання. При втраті або пошкодженні такого носія, даних може бути неможливо відновити без додаткових копій.

Усі ці загрози та вразливості показують, наскільки важливо приділяти увагу безпеці традиційних носіїв інформації. Застосування заходів безпеки, таких як фізична захисту, контроль доступу, резервне копіювання та каталогізація, може допомогти зменшити ризики втрати та забезпечити безпеку традиційних носіїв інформації.

1.3.2 Основні загрози та вразливості цифрових носіїв інформації

Цифрові носії інформації, такі як комп'ютери, мобільні пристрої, хмарні системи та інші електронні пристрої, надають безліч переваг і зручностей у зберіганні, передачі та обробці даних. Проте, вони також стикаються з різноманітними загрозами та вразливостями, які можуть призвести до втрати,

незаконного доступу або пошкодження інформації. Розглянемо основні загрози та вразливості цифрових носіїв інформації і розкриємо деталі та нюанси цих проблем:

- Віруси, черв'яки та шпигунське програмне забезпечення: ці види шкідливих програм можуть заражати цифрові носії, поширюючись через мережі, електронну пошту, завантажені файли та інші засоби. Вони можуть виконувати шкідливі дії, такі як видалення даних, блокування доступу, перехоплення конфіденційної інформації. Заражені носії можуть швидко поширювати ці програми на інші системи, створюючи широкомасштабні проблеми.
- Фішинг та шахрайство: фішинг - це вид атаки, коли зловмисники намагаються отримати чутливу інформацію, таку як паролі, номери кредитних карток, шляхом підманювання користувачів. Це може включати відправку підроблених електронних листів, створення фальшивих веб-сайтів або використання соціальної інженерії. Зловмисники можуть використовувати отриману інформацію для крадіжки особистих даних або фінансових ресурсів.
- Недостатня безпека мережі: недостатня захищеність мережі може викрити цифрові носії інформації на ризик несанкціонованого доступу. Недостатні паролі, відсутність шифрування, незахищені бездротові мережі - це лише кілька прикладів проблем, які можуть стати джерелом загрози. Нестача обновлень безпеки та вразливостей в операційних системах та програмах також може зробити цифрові носії більш уразливими.
- Втрата або крадіжка пристроїв: фізична втрата або крадіжка цифрових пристроїв, таких як ноутбуки, смартфони, може призвести до втрати чутливих даних та конфіденційної інформації. Якщо пристрій не зашифрований або не захищений паролем, зловмисники можуть отримати доступ до даних, що знаходяться на ньому.
- Несанкціонований доступ та злам систем: злом системи - це процес незаконного проникнення в комп'ютерну систему з метою отримання доступу до конфіденційної інформації або виконання шкідливих дій. Це

може бути здійснене шляхом використання вразливостей в програмному забезпеченні, поганого управління доступом або використання паролів слабкої складності.

- DDoS атаки: атаки типу DDoS спрямовані на перевантаження цифрових носіїв інформації шляхом надмірного навантаження мережі або серверів. Це призводить до втрати доступу до інформації або послуг для законних користувачів. Зловмисники можуть використовувати ботнети (мережу комп'ютерів, заражених шкідливими програмами) для виконання таких атак.
- Несанкціоноване використання та розголошення даних: цифрові носії інформації можуть стикатися з ризиком незаконного використання або розголошення даних. Це може статися внаслідок витоку даних, недостатньої захищеності системи або зловживання доступом до інформації з боку осіб, які мають привілеї.
- Соціальна інженерія: цифрові носії інформації можуть бути піддані атакам соціальної інженерії, де зловмисники намагаються отримати доступ до системи шляхом маніпуляцій з людьми. Це може включати фальшиві дзвінки, електронні листи або повідомлення, що містять підроблену інформацію або просунуті техніки соціального маніпулювання.

Усі ці загрози та вразливості показують, наскільки важливо приділяти увагу безпеці цифрових носіїв інформації. Застосування ефективних заходів безпеки, таких як використання сильних паролів, шифрування даних, оновлення програмного забезпечення, навчання персоналу щодо безпеки та встановлення механізмів виявлення вторгнень, може допомогти зменшити ризики та забезпечити захист цифрової інформації.

1.3.3 Проблема спотворення інформації на цифрових носіях

Окреслимо більш детально таку проблему, як проблема спотворення інформації на цифрових носіях, не пов'язана зі зловмисником, а викликана факторами

навколишнього середовища або недосконалістю обладнання (самого носія інформації), може мати серйозні наслідки для цілісності та доступності даних [7]. Розглянемо основні проблеми, які можуть спричинити спотворення інформації на цифрових носіях, таких як HDD, SSD, флеш-накопичувачі, CD та карти пам'яті:

- Бітові помилки: цифрові носії інформації можуть підвергатися бітовим помилкам, які виникають через фізичні впливи на носії. Наприклад, магнітні носії, такі як HDD, можуть бути схильними до змін поля магніту під впливом магнітних полів навколишнього середовища, що може призвести до спотворення збережених даних. Також, при записі або зчитуванні даних на носій можуть виникати помилки, які можуть призвести до спотворення чи втрати інформації.
- Ефект відображення: при зберіганні даних на флеш-накопичувачах або CD, може виникати проблема, відома як ефект відображення. Це спричиняється нерівномірним розподілом матеріалу запису на поверхні носія, що може призвести до виникнення ефекту відображення сигналу, який впливає на читання даних. Це може спотворити інформацію та призвести до помилкових зчитувань.
- Поганий стан носія: з часом цифрові носії, такі як HDD, SSD або CD, можуть зазнавати фізичного зносу або псуватися. Наприклад, на HDD можуть виникати проблеми з рухом механічних деталей, або на поверхні носія можуть з'являтися подряпини, що може призвести до спотворення даних. У разі SSD, можуть виникати проблеми зі зносом флеш-пам'яті, що призводить до появи «dead cells» та помилок при записі/зчитуванні. Подібні проблеми можуть впливати на цілісність збережених даних.
- Вплив навколишнього середовища: навколишнє середовище, включаючи вологість, температуру та статичну електрику, може мати негативний вплив на цифрові носії інформації. Наприклад, вологість може спричинити корозію контактів на носії або псування матеріалу запису, що призводить до спотворення даних. Висока або низька температура може спричинити

зміни властивостей матеріалів, а статична електрика може призвести до пошкоджень електронних компонентів.

- Недосконаліть обладнання: обладнання, що використовується для запису або зчитування даних на цифрові носії, також може бути причиною спотворення інформації. Наприклад, низька якість оптичних пристроїв на пристроях для запису/зчитування CD може призвести до помилок чи пошкоджень даних. Також, недосконаліть контролерів чи алгоритмів запису/зчитування на накопичувачах SSD може вплинути на цілісність та доступність даних.

Враховуючи ці фактори, важливо приділяти увагу якості і стану цифрових носіїв інформації. Регулярна перевірка та обслуговування обладнання, належне зберігання носіїв у контрольованих умовах, використання надійних та якісних носіїв, а також резервне копіювання даних можуть допомогти запобігти спотворенню інформації. Крім того, застосування методів кодування та контролю помилок може забезпечити виявлення та виправлення помилок під час зчитування даних.

Враховуючи всі ці фактори, важливо мати на увазі, що навіть з надійними цифровими носіями і використанням заходів безпеки, існує певний ризик спотворення інформації. Тому, для забезпечення безпеки та доступності даних, рекомендується постійно оновлювати резервні копії та здійснювати перевірку цілісності даних на носіях.

1.4 Принципи захисту носів інформації

Перед людством вже давно стоїть проблема захисту інформації, ще задовго до появи комп’ютерних технологій, своїм досвідом спробами та помилками воно виділило основні властивості інформації. Вони включають конфіденційність, цілісність та доступність, розглянемо їх детально:

1. Конфіденційність: ця властивість відноситься до забезпечення захисту інформації від несанкціонованого доступу. Це означає, що тільки авторизовані особи мають доступ до конфіденційної інформації, а всі інші особи не мають можливості

отримати доступ до цих даних. Шифрування даних, використання паролів і біометричних ідентифікаторів є деякими засобами досягнення конфіденційності.

2. Цілісність: ця властивість стосується збереження цілісності інформації, що означає забезпечення того, що дані не будуть змінені чи пошкоджені несанкціонованим способом. Для досягнення цілісності інформації використовуються механізми перевірки цілісності даних, контроль доступу і підписи, які дозволяють перевіряти автентичність інформації.

3. Доступність: ця властивість відноситься до забезпечення того, що інформація буде доступна авторизованим користувачам, коли вони цього потребують. Захист від DDoS-атаки, резервне копіювання даних, використання резервних серверів та реплікація даних є деякими засобами досягнення доступності інформації.

Історично людство прийшло до цих властивостей шляхом розвитку технологій і інформаційних систем. З появою комп'ютерів і зв'язку зростала необхідність захищати інформацію від несанкціонованого доступу та зловживань. Такі події, як витоки даних, хакерські атаки і кіберзлочини, допомогли підкреслити важливість захисту інформації.

Як вже було наголошено захист носіїв інформації – це захист інформації як такої, але існує кілька принципів, які можна використовувати для захисту носіїв інформації. Ось декілька з них:

- Фізичний захист: забезпечення фізичної безпеки носіїв інформації включає контроль доступу до приміщень, де зберігаються носії, а також захист від потенційних небажаних втручань або крадіжок. Це може включати встановлення системи контролю доступу, використання сейфів або спеціальних сховищ для носіїв, а також ведення журналу доступу для контролю та моніторингу.
- Шифрування: шифрування даних на носіях є ефективним методом захисту інформації. Шифрування дозволяє перетворити дані у незрозумілий для несанкціонованого доступу вигляд, а доступ до розшифрованих даних може бути наданий лише особам з необхідними правами. Використання

сильних шифрувальних алгоритмів та захищених ключів є ключовими аспектами шифрування даних.

- Резервне копіювання: регулярне створення резервних копій даних є важливим заходом безпеки. Це забезпечує можливість відновлення інформації в разі втрати або пошкодження носія. Резервні копії можуть зберігатися на інших носіях, на віддалених серверах або в хмарних сховищах.
- Антивірусне програмне забезпечення: використання антивірусного програмного забезпечення допомагає виявляти та блокувати шкідливі програми, які можуть впливати на носії інформації. Антивірусне програмне забезпечення дозволяє сканувати носії на наявність вірусів та інших загроз і вживати відповідних заходів для їх усунення.
- Фізична обробка: важливо правильно використовувати та обробляти носії інформації, щоб уникнути їх пошкодження. Носії повинні бути захищені від потенційних небезпек, таких як удари, падіння, перегрівання або надмірна вологість. Дотримання правил експлуатації та зберігання носіїв може значно зменшити ризик виникнення проблем.
- Політики та навчання персоналу: розробка і впровадження політик безпеки даних та навчання персоналу стосовно безпечного використання та збереження носіїв інформації є важливими кроками для захисту. Персонал повинен бути свідомим потенційних загроз та вміти діяти відповідно до встановлених правил.

Ці принципи захисту носіїв інформації є загальними і можуть бути застосовані як до традиційних, так і до цифрових носіїв. Важливо враховувати контекст та специфічні вимоги вашої системи, коли ви впроваджуєте заходи безпеки для захисту носіїв інформації.

Висновки за розділом 1

Метою розділу 1 було проаналізувати теоретичні засади захисту носіїв інформації для подальшого розкриття теми роботи. Було проаналізовано нормативно-правову базу України у сфері захисту інформації, бо захист інформації та захисту носіїв інформації нерозривно пов’язані. Питання захисту носіїв інформації є питанням захисту інформації в цілому, через те, що інформація яку потрібно захищати не існує без її носіїв, а носії без інформації не варті захисту. Після аналізу нормативно-правового фундаменту на якому стоїть вся сфера інформаційної безпеки, було проведено класифікацію та опис носіїв інформації, оскільки носії інформації бувають дуже різними, підходи до захисту можуть відрізнятись. Було виділено два основних типи: традиційні та цифрові носії інформації, а також визначено значущість для сьогодення цифрового типу інформації та цифрових носіїв інформації, таких як HDD, SSD, флеш-накопичувачі, CD та карти пам'яті.

Було визначено та описано основні загрози та вразливості для носіїв інформації, була зосереджена увага на цифрових носіях інформації та їх загрозах, вразливостях та проблемах. Принципи захисту носіїв інформації були приведені та коротко описані, вони є універсальними для різних типів носіїв інформації, а саме: фізичний захист, шифрування, резервне копіювання, антивірусне ПЗ, фізична обробка, політики та навчання персоналу.

Загалом розділ дає теоретичну основу для подальшого поглиблення в питання засобів та механізмів захисту носіїв інформації.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ЗАСОБІВ ТА МЕХАНІЗМІВ ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ

2.1 Різниця між поняттями засіб захисту та механізм захисту

Засоби захисту носіїв інформації та механізми захисту носіїв інформації є двома поняттями, пов'язаними зі забезпеченням безпеки й конфіденційності інформації, але мають трохи різне значення. Якщо також ми не забудемо про різницю між різними носіями інформації, та те що підходи до забезпечення їх безпеки можуть в деталях суттєво відрізнятись, то розуміння різниці стає ще більш важливим.

Засоби захисту носіїв інформації включають конкретні інструменти, програмне забезпечення, апаратні засоби або технології, які використовуються для захисту інформації. Наприклад, це можуть бути файрволи (firewalls), антивірусне програмне забезпечення, шифрування даних, системи контролю доступу та інші технічні засоби, які використовуються для запобігання несанкціонованому доступу до інформації або злому безпеки.

Механізми захисту носіїв інформації охоплюють ширший спектр стратегій, політик, процедур і підходів, що використовуються для забезпечення безпеки інформації. Вони включають організаційні політики, правила, стандарти, процедури, навчання персоналу, фізичну безпеку і т. д. Механізми захисту інформації не обмежуються лише технічними аспектами, вони також враховують людей, процеси і процедури, які сприяють безпеці інформації.

Отже, різниця між засобами та механізмами захисту носіїв інформації полягає в тому, що засоби захисту стосуються конкретних технічних інструментів і технологій, тоді як механізми захисту охоплюють ширший спектр стратегій, політик, процедур і підходів, включаючи організаційні аспекти та навчання персоналу. Успішна система захисту інформації вимагає використання як засобів, так і механізмів захисту, щоб забезпечити комплексний підхід до безпеки інформації.

2.2 Аналіз основних засобів захисту носіїв інформації

Як стало зрозуміло з попереднього матеріалу засоби захисту носіїв інформації різноманітні, їх багато, кожен закриває свій певний спектр загроз та вразливостей для носія інформації. Також враховуючи різноманіття носіїв інформації, кожен засіб захисту може впроваджуватись по різному або бути унікальним [8]. Розглянемо та опишемо основні засоби захисту носіїв інформації.

Шифрування є процесом перетворення звичайного тексту у криптографічний за допомогою спеціальних алгоритмів та секретного ключа. Шифрування забезпечує конфіденційність даних, оскільки лише авторизовані користувачі, які володіють секретним ключем, можуть розшифрувати зашифрований текст та отримати доступ до вихідної інформації.

Аутентифікація використовується для перевірки ідентичності користувача або пристрою, що намагається отримати доступ до інформації. Це може бути зроблено за допомогою різних методів, таких як паролі, біометричні дані, смарт-карти та цифрові сертифікати. Аутентифікація дозволяє гарантувати, що тільки авторизовані користувачі можуть отримати доступ до конфіденційної інформації.

Контроль доступу визначає, хто має право доступу до конкретних ресурсів на основі їхньої ідентичності, ролі або авторизації. Це гарантує, що лише авторизовані користувачі мають доступ до конфіденційних даних та можуть виконувати необхідні дії з ними.

Забезпечення цілісності полягає в забезпеченні того, що дані на носії інформації не були змінені під час транспортування або зберігання. Це може бути досягнуто за допомогою контрольної суми або хеш-функції. Забезпечення цілісності даних гарантує, що вони не були змінені або пошкоджені без відома користувача.

Антивіруси - це програми, які виявляють і запобігають розповсюдженню вірусів та інших шкідливих програм [20]. Вони аналізують систему на наявність вірусів та інших загроз, блокують небезпечні файли та процеси, забезпечують автоматичне оновлення баз даних вірусів та виявлення нових загроз (рис. 2.1).

Рисунок 2.1 – Найпоширеніші антивірусні програми

Файрволи - це програми або пристрої, які контролюють мережевий трафік та фільтрують його за правилами безпеки. Вони забезпечують захист мережевого з'єднання від атак, спрямованих на отримання несанкціонованого доступу до системи (рис. 2.2).

IDS - це програмні та апаратні рішення, які моніторять мережу на наявність небезпечних дій та відповідно реагують на них. Вони допомагають виявляти та запобігати атакам на систему, забезпечують захист від витоку конфіденційної інформації та несанкціонованого доступу до системи (рис. 2.2).

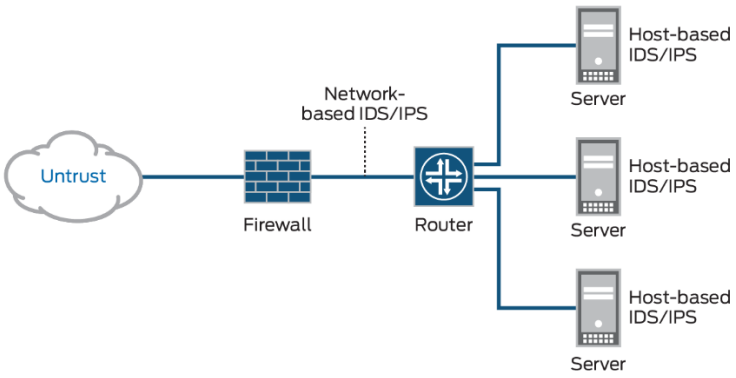

Рисунок 2.2 – Схема розміщення засобів IDS та файрволу в системі

Пристрої з обмеженням доступу до даних - це пристрої, які забезпечують контроль доступу до інформації на носіях. Вони дозволяють обмежувати доступ до певних файлів або директорій залежно від прав доступу, встановлених користувачем.

Апаратні токени - це спеціальні пристрої, які забезпечують авторизацію та аутентифікацію користувача. Вони містять електронні ключі та сертифікати, які використовуються для ідентифікації користувача та забезпечення безпеки в мережі (рис. 2.3).

Рисунок 2.3 – Апаратні токени різних конструкцій

Спеціалізовані захищені пристрої зберігання даних - це пристрої, які забезпечують захист інформації від несанкціонованого доступу та втрати даних. Вони забезпечують апаратний рівень захисту даних за допомогою шифрування, контролю доступу та інших захисних механізмів.

Список можна продовжувати довго, стає зрозумілим широкий спектр підходів до забезпечення безпеки носіїв інформації. Зараз найбільш поширеним, особливо серед звичайних користувачів, є цифровий формат зберігання, оброблення та передачі інформації. Реалізується він цифровими носіями інформації, основними та найбільш поширеними засобами їх захисту є шифрування, аутентифікація, контроль доступу та забезпечення цілісності, тож розглянемо їх детально.

2.2.1 Шифрування, як засіб захисту носіїв інформації

Шифрування є важливим засобом захисту інформації шляхом перетворення даних у зашифрований формат, який може бути розшифрований лише з допомогою

відповідного ключа. Цей процес забезпечує конфіденційність та цілісність даних, навіть якщо вони потрапляють у руки несанкціонованої сторони.

Розглянемо декілька методів та рішень шифрування:

- Симетричне шифрування: у цьому методі використовується один ключ для як шифрування, так і розшифрування даних. Відправник і отримувач повинні мати спільний ключ. Дані шифруються з допомогою ключа і розшифровуються з тим самим ключем на протилежному кінці комунікації. Алгоритми, такі як Advanced Encryption Standard (AES), DES (Data Encryption Standard) і Triple DES, є прикладами симетричного шифрування.
- Асиметричне шифрування: в асиметричному шифруванні використовується пара ключів: публічний і приватний. Публічний ключ використовується для шифрування даних, а приватний ключ використовується для розшифрування даних. Публічний ключ може бути розповсюджений відкрито, тоді як приватний ключ повинен бути триманий в секреті. Алгоритми, такі як RSA (Rivest-Shamir-Adleman) і ECC (Elliptic Curve Cryptography), використовуються для асиметричного шифрування [12].
- Хешування: хешування є методом перетворення даних фіксованої довжини (хешу) за допомогою хеш-функції. Хеш-функція приймає вхідні дані будь-якої довжини і генерує унікальний вихідний код, відомий як хеш. Цей хеш може бути використаний для перевірки цілісності даних. Хеш-функції, такі як MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm 1) і SHA-256, є прикладами алгоритмів хешування [14].
- Векторне шифрування: векторне шифрування (Vector Encryption) є методом, в якому використовуються вектори або матриці для шифрування даних. Векторні шифри використовують пару ключів, векторний ключ і ключ ініціалізації. Вони забезпечують високу швидкодію та безпеку шифрування даних. Прикладом векторних шифрів є шифр AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) [17].

Ці методи шифрування можуть бути використані окремо або в комбінації для забезпечення безпеки інформації. Шифрування дозволяє захищати дані під час трансляції через мережі, зберігання на носіях інформації, а також зменшує ризик доступу до даних несанкціонованими особами.

2.2.2 Аутентифікація, як засіб захисту носіїв інформації

Аутентифікація є важливим засобом захисту інформації, який використовується для перевірки та підтвердження ідентичності користувача або суб'єкта, який намагається отримати доступ до системи, даних або ресурсів. Цей процес дозволяє переконатися, що лице, яке намагається отримати доступ, дійсно має право на цей доступ.

Розглянемо декілька основних методів аутентифікації:

- Щось, що ви знаєте (Something you know): цей метод базується на знанні конфіденційної інформації, такої як пароль, PIN-код або відповідь на секретне питання. При аутентифікації користувач повинен ввести правильну інформацію, щоб підтвердити свою ідентичність.
- Щось, що ви маєте (Something you have): цей метод використовує фізичний предмет, такий як смарт-карта, токен або мобільний пристрій, який містить унікальну ідентифікаційну інформацію. Користувач повинен мати фізичний доступ до цього предмета для успішної аутентифікації.
- Щось, що ви є (Something you are): цей метод базується на біометричних характеристиках, таких як відбиток пальця, розпізнавання обличчя, голосовий або сканування ока. Біометричні дані користувача порівнюються з заздалегідь збереженими образами, щоб підтвердити ідентичність [17].
- Двофакторна аутентифікація (2FA): цей метод поєднує два або більше зазначених вище факторів аутентифікації для підвищення безпеки (рис. 2.4). Зазвичай це поєднання чогось, що ви знаєте (наприклад, пароль) і

щось, що ви маєте (наприклад, одноразовий код, який надсилається на мобільний пристрій) [11].

Рисунок 2.4 – Схема 2FA аутентифікації

Методи аутентифікації можуть використовуватися окремо або в комбінації, залежно від рівня безпеки, який необхідно досягти. Наприклад, багато систем використовують поєднання паролів (щось, що ви знаєте) і одноразових кодів, які надсилаються на зареєстрований мобільний пристрій (щось, що ви маєте) для забезпечення більшого рівня безпеки [9].

Важливо зазначити, що аутентифікація не обмежується лише одним методом. Застосування комплексних стратегій аутентифікації, таких як багатофакторна аутентифікація, біометрична ідентифікація і т. д., може забезпечити більшу надійність захисту інформації і унеможливити несанкціонований доступ.

2.2.3 Контроль доступу, як засіб захисту носіїв інформації

Контроль доступу є важливим засобом захисту інформації, який визначає, які користувачі або суб'єкти мають дозвіл на доступ до конкретних ресурсів, систем або даних. Цей процес забезпечує обмеження прав доступу, зменшує ризик несанкціонованого доступу та потенційних загроз безпеці.

Розглянемо декілька методів та рішень контролю доступу:

- Рольовий контроль доступу (Role-Based Access Control, RBAC): в цьому підході доступ до ресурсів призначається на основі ролей, які визначаються для користувачів. Кожна роль має набір прав доступу, які

відповідають її функціональності. При рольовому контролі доступу адміністратор системи призначає ролі користувачам, а не окремі права доступу, спрощуючи процес управління доступом [10].

- Ідентифікація та аутентифікація: цей метод контролю доступу передбачає перевірку ідентичності користувача перед наданням доступу. Він може включати в себе аутентифікацію за допомогою пароля, біометричних даних, смарт-карт або інших факторів. Після аутентифікації користувачу надаються права доступу відповідно до його облікового запису або ролі.
- Правила доступу на основі політики (Policy-Based Access Control, PBAC): в цьому підході доступ до ресурсів контролюється на основі набору правил та політик. Правила можуть включати умови, такі як час доступу, місцезнаходження, тип з'єднання та інші параметри. Адміністратор визначає ці правила, які визначають, які користувачі або групи користувачів мають дозвіл на доступ до ресурсів.
- Привілейований доступ: цей метод контролю доступу надає особливі привілеї певним користувачам, які мають повний контроль над системою або ресурсами. Такі користувачі зазвичай є адміністраторами або системними операторами. Привілейований доступ має бути суворо контрольованим та обмеженим, щоб запобігти можливим зловживанням.

Ці методи контролю доступу можуть бути реалізовані за допомогою різних технологій та рішень, таких як системи керування доступом (Access Control Systems), системи ідентифікації та аутентифікації (Identity and Authentication Systems), системи управління правами доступу (Access Rights Management Systems) та інші. Комплексне використання цих методів та технологій допомагає забезпечити ефективний контроль доступу та зменшити ризик несанкціонованого доступу до інформації.

2.2.4 Забезпечення цілісності, як засіб захисту носіїв інформації

Забезпечення цілісності є важливим засобом захисту носіїв інформації та гарантує, що дані залишаються недоторканими, незмінними та не піддані

несанкціонованим змінам протягом всього процесу їх зберігання та передачі. Це важливо для запобігання втраті інформації, втраті її цілісності та порушенню довіри до системи.

Для забезпечення цілісності інформації використовуються такі методи та рішення:

- Хеш-функції: хеш-функції використовуються для обчислення унікального хеш-коду або цифрового відбитка вхідних даних. Хеш-код є фіксованого розміру і є результатом застосування хеш-функції до вхідних даних. Якщо навіть невелика зміна в вхідних даних, буде мати суттєвий вплив на хеш-код. Перевірка хеш-коду дозволяє виявити недопустимі зміни в даних, тим самим забезпечуючи цілісність.
- Цифрові підписи: цифрові підписи використовуються для перевірки автентичності та цілісності даних. Вони забезпечують ідентифікацію відправника та довіреність даних. Цифровий підпис формується з використанням приватного ключа відправника та перевіряється з використанням відповідного публічного ключа. Якщо дані були змінені після створення цифрового підпису, перевірка цифрового підпису не буде успішною, що вказує на порушення цілісності [19].
- Контрольні суми (checksums): контрольні суми використовуються для перевірки цілісності даних шляхом порівняння контрольної суми отриманих даних з передбаченою контрольною сумою [16]. Контрольна сума є значенням, яке обчислюється з використанням певного алгоритму, такого як CRC або Adler-32. Якщо контрольна сума, отримана при отриманні даних, не співпадає з передбаченою контрольною сумою, це свідчить про зміну даних і порушення цілісності.
- Ведення журналу подій та аудит: ведення журналу подій та аудит використовується для реєстрації подій та змін в системі або носії інформації. Це дозволяє виявити незвичайну або несанкціоновану діяльність, яка може вказувати на порушення цілісності даних. Журнали

дій можуть бути перевірені для виявлення зловмисної діяльності або втрати цілісності даних.

Ці методи та рішення допомагають забезпечити цілісність інформації шляхом виявлення незаконних змін або втрати даних. Вони використовуються в різних галузях, таких як мережева безпека, бази даних, електронна комерція тощо, для забезпечення безпеки та надійності інформації.

2.3 Аналіз основних механізмів захисту носіїв інформації

Механізми захисту носіїв інформації включають широкий спектр стратегій, політик, процедур і підходів, які призначені для забезпечення безпеки інформації. Вони охоплюють не тільки технічні аспекти, але й залучають організаційні політики, правила, стандарти, процедури, навчання персоналу, фізичну безпеку і багато іншого [15]. Давайте розглянемо кожну з цих позицій більш детально:

1. Організаційні політики: це набір документів, що визначають правила і принципи, які визначають, як організація буде захищати свою інформацію. Ці політики охоплюють різні аспекти безпеки, включаючи доступ до інформації, обмін даними, управління паролями, захист від зловживань та інші.

2. Правила і стандарти: це конкретні правила і стандарти, які організація встановлює для захисту своєї інформації. Ці правила можуть охоплювати використання конкретного програмного забезпечення, налаштування мережі, використання паролів, резервне копіювання даних та інші аспекти безпеки.

Правила і стандарти є важливою складовою механізмів захисту носіїв інформації. Вони встановлюють конкретні норми і вимоги, які мають бути виконані для забезпечення безпеки інформації. Давайте розглянемо ці дві позиції детальніше:

Правила: правила є конкретними директивами і вказівками, які встановлюють, як слід поводитися щодо захисту інформації. Вони можуть охоплювати такі аспекти, як:

- Використання паролів: правила можуть визначати вимоги до довжини паролів, складності, періодичності зміни паролів і заборону використання слабких паролів.
- Керування доступом: правила можуть визначати, хто має доступ до певних категорій інформації, які права доступу мають користувачі, і які механізми контролю доступу використовуються.
- Використання програмного забезпечення: правила можуть встановлювати вимоги до використання конкретного програмного забезпечення, оновлення до останньої версії, антивірусного програмного забезпечення, перевірки на наявність шкідливих програм тощо.
- Захист фізичних носіїв інформації: правила можуть включати вимоги до фізичної безпеки, такі як блокування робочого місця при відсутності працівника, захист комп'ютерів від несанкціонованого доступу і т. д.

Правила встановлюють стандарти, які мають бути дотримані всіма користувачами інформації в організації. Вони можуть бути документованими у вигляді внутрішніх правил організації або базуватись на стандартах безпеки, таких як ISO 27001 (рис. 2.5).

Рисунок 2.5 – Стандарт ISO 27001

Стандарти: стандарти є узгодженими наборами вимог і рекомендацій, які встановлюються організаціями, професійними організаціями або урядовими

органами для забезпечення безпеки інформації. Деякі з популярних стандартів безпеки включають ISO 27001, NIST SP 800-53, PCI DSS та HIPAA [13].

Стандарти встановлюють рамки і рекомендації для різних аспектів безпеки інформації і можуть включати такі елементи:

- Організаційні вимоги: стандарти можуть встановлювати вимоги до організаційних політик, процедур управління безпекою, визначення ролей та відповідальності, проведення аудитів та інших аспектів управління безпекою.
- Фізична безпека: стандарти можуть встановлювати вимоги до фізичної безпеки приміщень, включаючи захист серверних кімнат, контроль доступу, системи відеоспостереження і т. д.
- Технічні заходи: стандарти можуть включати вимоги до конфігурації мережі, шифрування даних, захисту від вторгнень, резервного копіювання даних та інших технічних аспектів безпеки.

Використання стандартів забезпечує уніфікований підхід до безпеки інформації та допомагає організаціям досягти вищого рівня захисту шляхом впровадження рекомендацій та норм безпеки, що міжнародно визнані.

Враховуючи правила і стандарти, організації можуть розробити внутрішні правила безпеки, які відповідають їхнім специфічним потребам, і впроваджувати набір вимог, які забезпечують належний рівень безпеки інформації.

3. Процедури: це документовані кроки, які повинні бути виконані для забезпечення безпеки інформації. Ці процедури можуть включати процедури входу/виходу персоналу, реагування на інциденти безпеки, копіювання даних, моніторинг мережі та інші.

4. Навчання персоналу: забезпечення належного навчання персоналу є важливим аспектом безпеки інформації. Це включає навчання персоналу про правила безпеки, ідентифікацію потенційних загроз, процедури поводження з конфіденційною інформацією та інші аспекти безпеки.

5. Фізична безпека: це заходи, які спрямовані на захист фізичних носіїв інформації, таких як серверні кімнати, центри обробки даних, комп'ютери, диски і т.

д. Ці заходи можуть включати контроль доступу, використання систем відеоспостереження, фізичну охорону та інші заходи.

Всі вищеперераховані механізми захисту носіїв інформації є більш актуальними для великих фірм, організацій та структур, окремо взятому користувачу для забезпечення захисту своїх носіїв інформації вони будуть неактуальними, більш доречним буде використання одного чи декількох засобів захисту. Все ж пам’ятати та розуміти механізми захисту потрібно кожному.

Висновки за розділом 2

Метою розділу 2 було дослідити існуючі засоби та механізми захисту носіїв інформації, їх сутність та сферу використання. Було розглянуто методи та рішення, які реалізують окремі засоби та механізми захисту носіїв інформації. Узагальнюючи, засоби та механізми захисту носіїв інформації є необхідною складовою частиною інформаційної безпеки.

Захист цінної інформації вимагає комплексного підходу та регулярної перевірки безпеки. Важливо розуміти, що кожен окремий реальний процес забезпечення інформаційної безпеки має свої унікальні потреби та ризики, тому вибір заходів захисту повинен відповідати конкретним потребам та ризикам.

Використання таких засобів, як шифрування, аутентифікація, контроль доступу та забезпечення цілісності, дозволяє зменшити ризики витоку чутливої інформації та захистити її від несанкціонованого доступу.

Загалом розділ дає розуміння широти питання роботи, окресливши конкретні засоби захисту носіїв інформації, була виконана підготовка до реалізації такого засобу захисту носіїв інформації, як забезпечення цілісності.

РОЗДІЛ 3
РОЗРОБКА ТА РЕАЛІЗАЦІЯ ЗАСТОСУНКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ ІНФОРМАЦІЇ

3.1 Функціональність застосунку, що розробляється, та його цілі

Задача полягає в розробці застосунку, дамо йому назву «Data Integrity Checker» (Перевірка цілісності даних), він надає можливість користувачеві перевірити цілісність даних у вибраному носії інформації шляхом порівняння хеш-сум файлів з попереднім збереженим «знімком».

Основний функціонал застосунку:

- Вибір носія інформації: користувач може вибрати будь який цифровий носій інформації чи його розділ або директорія, в якій буде проводитись перевірка цілісності даних.
- Створення «знімка»: після вибору носія інформації, користувач може створити «знімок», що представляє собою збереження хеш-сум кожного файлу в директорії на момент створення «знімка».
- Перевірка цілісності: користувач може перевірити цілісність даних вибраного цифрового носія шляхом порівняння хеш-сум файлів з «знімком». Якщо будь-який файл має змінену хеш-суму, він відображається у спливаючому повідомленні.

Застосунок перевірки цілісності даних за допомогою хеш-функції детектуватиме наступні зміни:

- Додавання нових файлів: якщо у вибраній директорії (наприклад, на флеш-накопичувачу) були додані нові файли після створення «знімка» стану даних, ці файли будуть розпізнані як зміни.
- Видалення файлів: якщо файли, які знаходяться у вибраній директорії (наприклад, на флеш-накопичувачу), були видалені після створення «знімку», вони будуть розпізнані як зміни.

- Зміна вмісту файлів: якщо вміст файлу змінився після створення «знімка», наприклад, якщо у файлі були внесені зміни або файл було перезаписано, ця зміна буде виявлена.
- Змінення імені файлу: якщо ім'я файлу було змінено після створення «знімка», це також буде розпізнане як зміна.
- Переміщення файлів: якщо файл було переміщено до іншої директорії після створення знімка, це буде сприйнято як зміну.

Застосунок буде порівнювати хеш-суми файлів у вибраній директорії зі збереженим «знімком» і визначить, якщо відбулися будь-які з перерахованих вище змін.

Застосунок добре працюватиме з різними носіями даних, включаючи:

- Жорсткі диски (HDD): програма зможе перевіряти цілісність даних на жорстких дисках, які є найпоширенішим типом зберігання даних на комп'ютерах.
- SSD-накопичувачі: програма також працюватиме з SSD-накопичувачами, які використовують флеш-пам'ять для зберігання даних. Вона зможе перевіряти цілісність даних на таких накопичувачах.
- USB-флешки: програма може працювати з USB-флешками, дозволяючи перевірити цілісність даних, збережених на флеш-накопичувачах.
- Зовнішні жорсткі диски: якщо зовнішній жорсткий диск підключено до комп'ютера, програма зможе перевірити цілісність даних на цьому носії.
- Мережеві диски: якщо комп'ютер підключено до мережевого сховища або хмарного сховища, програма може працювати з даними, що зберігаються на таких дисках.
- Інші носії даних, що підтримуються: програма зможе працювати з іншими типами носіїв, що підтримуються, включаючи CD/DVD-диски, Blu-ray диски і т. д. Проте для роботи з деякими специфічними типами дисків можуть знадобитися додаткові налаштування або бібліотеки.

Загалом застосунок призначена для роботи з різними носіями даних, що підтримуються операційною системою Windows або Linux, і здатна перевіряти цілісність даних на цих носіях.

Застосунок написаний на мові програмування Python [21] та використовує бібліотеку tkinter для створення графічного інтерфейсу користувача (GUI). Він також використовує модулі hashlib [22] та pickle [23] для обчислення хеш-сум та зберігання «знімків» даних.

Ціль застосунку – надати засіб для перевірки цілісності даних, що може бути корисним в ситуаціях, коли необхідно виявити, чи були змінені файли на носії інформації чи в певній директорії, наприклад, внаслідок несанкціонованого доступу або помилок в процесі зберігання або передачі даних.

3.2 Архітектура та технічні особливості застосунку

Загалом архітектуру застосунку можна описати наступним чином.

Графічний інтерфейс:

- Використовується бібліотека tkinter для створення графічного інтерфейсу користувача.
- Головне вікно створюється за допомогою tk.Tk().
- Клас DataIntegrityChecker використовує головне вікно як батьківський елемент для всіх інших елементів графічного інтерфейсу.
- Елементи графічного інтерфейсу, такі як мітки (Label), текстові поля (Entry), кнопки (Button) та спливаючі повідомлення (messagebox), створюються та налаштовуються у методі create_widgets().

Tkinter є стандартною бібліотекою Python, яка використовується для створення графічного інтерфейсу користувача (GUI). Вона надає набір інструментів і класів для побудови віконних додатків і віджетів [25].

Основним компонентом Tkinter є Tk, що є бібліотекою, написаною на мові Tcl і використовується для створення вікон та елементів управління. Tkinter включає у

себе обгортки для цієї бібліотеки, які дозволяють використовувати її зі зручним інтерфейсом Python.

За допомогою Tkinter можна створювати вікна, кнопки, текстові поля, списки, меню, діалогові вікна та інші елементи інтерфейсу. Вона також надає можливості для обробки подій, таких як натискання кнопок або рух миші.

Одна з переваг Tkinter полягає в тому, що вона входить до стандартної бібліотеки Python, тому вона доступна з початку при встановленні Python. Це робить Tkinter досить поширеною і простою у використанні бібліотекою для створення GUI-додатків у Python.

Також варто зазначити, що Tkinter має простий синтаксис і досить добре документована. Існують також додаткові бібліотеки, які розширюють функціональність Tkinter, наприклад, ttk (Themed Tkinter), яка надає більше стильних елементів управління.

Операції з даними:

- Клас DataIntegrityChecker має методи для взаємодії з даними та проведення перевірки цілісності.
- Метод browse_directory() дозволяє користувачеві вибрати директорію за допомогою діалогового вікна filedialog.askdirectory() та зберігає вибрану директорію в змінну self.directory.
- Метод create_snapshot() створює снімок стану даних у вибраній директорії. Він отримує список файлів у директорії, обчислює хеш-суму кожного файлу, зберігає ці хеш-суми у словнику snapshot та зберігає снімок у файлі data_snapshot.pkl.
- Метод verify_integrity() перевіряє цілісність даних у вибраній директорії. Він отримує список файлів у директорії, обчислює хеш-суму кожного файлу та порівнює його зі збереженими хеш-сумами з снімка. Якщо хеш-сума файлу відрізняється від збереженої хеш-суми, файл вважається зміненим.
- Методи get_file_list(), calculate_hash(), save_snapshot() та load_snapshot() служать для виконання відповідних операцій з файлами та хеш-сумами.

Події та управління:

- Головне вікно застосунку запускається за допомогою методу root.mainloop(), що дозволяє обробляти події та управляти взаємодією користувача з інтерфейсом.
- Кнопки та інші елементи графічного інтерфейсу відреаговують на події від користувача, такі як натискання кнопки. Кожна кнопка має пов'язану з нею функцію, яка викликається при виникненні події.
- Наприклад, кнопка «Огляд» (self.browse_button) має функцію self.browse_directory як команду, яка виконується при натисканні кнопки.

Застосунок виконує досить прості функції для перевірки цілісності даних у вибраній директорії та надає користувачеві зручний спосіб взаємодії з ним за допомогою графічного інтерфейсу.

Застосунок використовує формат «pkl» (pickle) для збереження «знімків» стану даних файли. Pickle - це модуль у мові програмування Python, який дозволяє серіалізувати та десеріалізувати об'єкти Python. Він дозволяє зберігати складні структури даних, включаючи списки, словники, класи тощо у двійковому форматі.

Вибір формату «pkl» для збереження «знімків» стану мав такі переваги:

- Простота використання: модуль pickle вбудований у стандартну бібліотеку Python, тому немає потреби встановлювати додаткові сторонні бібліотеки чи модулі.
- Повна серіалізація: pickle може серіалізувати та десеріалізувати майже всі об'єкти Python без необхідності явного перетворення даних.
- Підтримка складних структур даних: pickle дозволяє зберігати та відновлювати складні структури даних, такі як вкладені списки, словники та класи, зі збереженням їхньої ієрархії та зв'язків.

Бінарний формат: «pkl» зберігає дані в двійковому форматі, що може бути корисно для ефективного зберігання великих обсягів даних і забезпечення їх безпеки.

Однак варто враховувати, що формат «pkl» може мати й деякі обмеження та недоліки:

- Залежність від версії Python: pickle може бути залежним від версії Python та несумісний з іншими мовами програмування;
- Безпека: завантажені «pkl» файли можуть бути потенційно небезпечними, оскільки вони можуть виконувати довільний код при десеріалізації. Необхідно бути обережним під час завантаження файлів «pkl» з ненадійних джерел.

Загалом вибір формату «pkl» для збереження «знімків» стану даних залежить від конкретних вимог та контексту програми. Якщо безпека або сумісність з іншими мовами є важливими факторами, можна розглянути альтернативні формати, такі як JSON або YAML. У випадку використання даного застосунку формат «pkl» більш ніж підходить для використання.

У застосунку використовується хеш-функція SHA-256 (Secure Hash Algorithm 256-bit). Це сильна хеш-функція, яка генерує хеш-суму завдовжки 256 біт (рис. 3.1). Вона забезпечує хорошу стійкість до колізій (ситуація, коли двом різним вхідним даним відповідає однакова хеш-сума) і широко застосовується для перевірки цілісності даних [24].

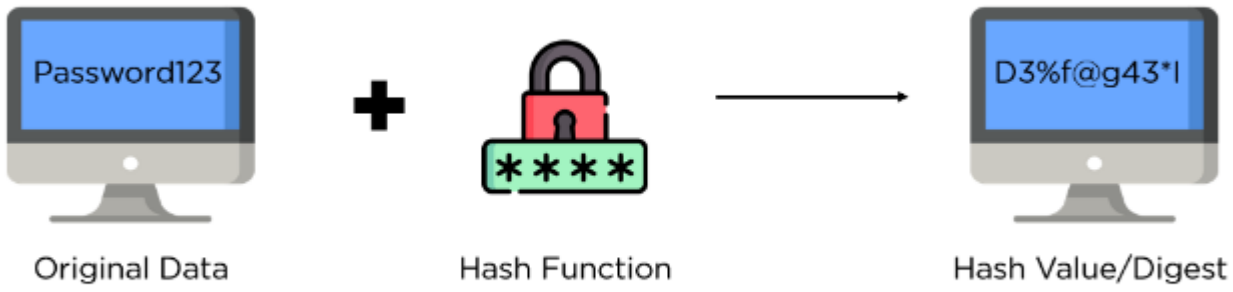

Рисунок 3.1 – Схема роботи хеш-функції

У програмному коді використовується клас hashlib.sha256 зі стандартної бібліотеки Python для створення об'єкта хеш-функції SHA-256. Потім метод update() використовується для оновлення стану хеш-функції з даними файлу, а метод

hexdigest() повертає остаточну хеш-суму у вигляді рядка, що подається у шістнадцятковому форматі.

3.3 Процес розробки та вибрані методології

При написанні застосунку для перевірки цілісності даних на цифровому носії інформації з використанням хеш-функції було використано наступні методології та підходи:

Застосовано принципи ООП для структурування програмного коду. Створено клас DataIntegrityChecker, який інкапсулює логіку програми та її стан. Кожен метод класу відповідає за певну функціональність програми.

Модульність: було розбито функціональність програми на окремі методи та функції, щоб полегшити читання, розуміння та тестування коду. Кожен метод виконує певну задачу, що сприяє підвищенню читання та керованості коду.

Використання стандартних бібліотек: для реалізації функцій хешування, роботи з файлами, діалоговими вікнами та повідомленнями використовувалися стандартні бібліотеки Python, такі як hashlib, os, pickle, tkinter та messagebox. Це дозволяє використовувати готові та перевірені інструменти для вирішення завдань та підвищує переносимість програми.

Поділ відповідальності: функціональність програми було розділено на незалежні частини, кожна з яких відповідає за конкретне завдання. Наприклад, методи create_snapshot та verify_integrity відповідають за створення «знімка» стану даних та перевірку цілісності відповідно.

Обробка помилок та винятків: передбачено обробку можливих помилок та виняткових ситуацій у додатку, наприклад, при неправильному виборі носія інформації або помилці збереження/завантаження «знімка» стану даних. У таких випадках користувачу виводяться повідомлення про помилку.

Інтерфейс користувача (GUI): було використано бібліотеку tkinter для створення графічного інтерфейсу користувача (GUI) програми. Використання GUI

дозволяє зручно взаємодіяти з користувачем, вибирати директорії, відображати повідомлення та результати перевірки цілісності даних.

Тестування: було проведено тестування програми на різних сценаріях, включаючи створення «знімка», зміну даних та перевірку цілісності. Тестування допомагає виявити можливі помилки та переконатися у правильній роботі програми.

В цілому, при розробці застосунку використовувалися стандартні практики та підходи до програмування, сфокусовані на модульності, ООП, обробці помилок і створенні зручного інтерфейсу для взаємодії з користувачем.

3.4 Демонстрація роботи застосунку та його можливостей

У даному підрозділі проведемо демонстрацію застосунку, покажемо покрокове його використання та можливості, які він надає. Програмний код застосунку ми можемо розмістити в будь якому місці на ПК, для більшої коректності це не має бути саме той носій інформації, який ми перевіряємо, але це не принципово. На рисунку 3.2 показано розміщення застосунку, просто запускаємо файл.

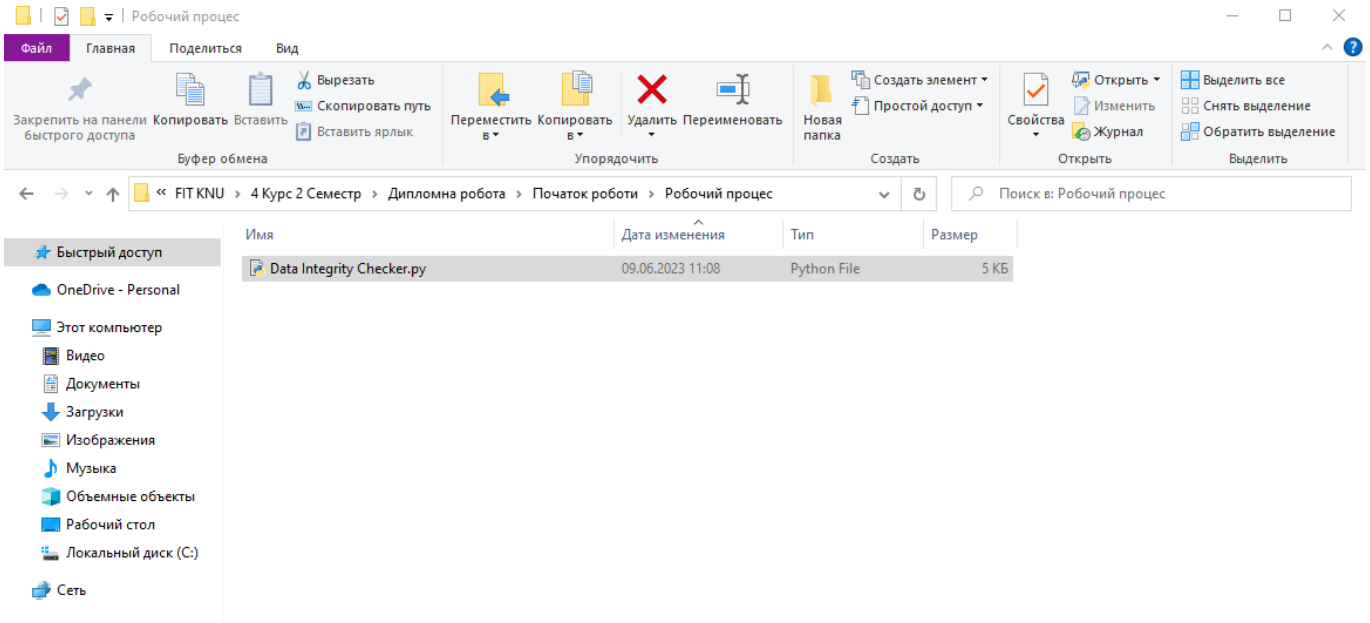

Рисунок 3.2 – Директорія з розміщеним програмним кодом застосунку

Запустивши на виконання код, нам відкриється головне меню застосунку (рис. 3.3), в якому ми побачимо поле вводу носія інформації вручну, кнопку «Огляд», яка

дозволить нам вибрати його, кнопку «Створити знімок», яка виконає перевірку носія інформації хеш-функцією SHA-256 та збереже отриманий результат до файлу .pkl, який буде розміщено в директорії знаходження застосунку, а також кнопку «Перевірити цілісність», вона виконає звірення даних та покаже чи були зміни та які саме.

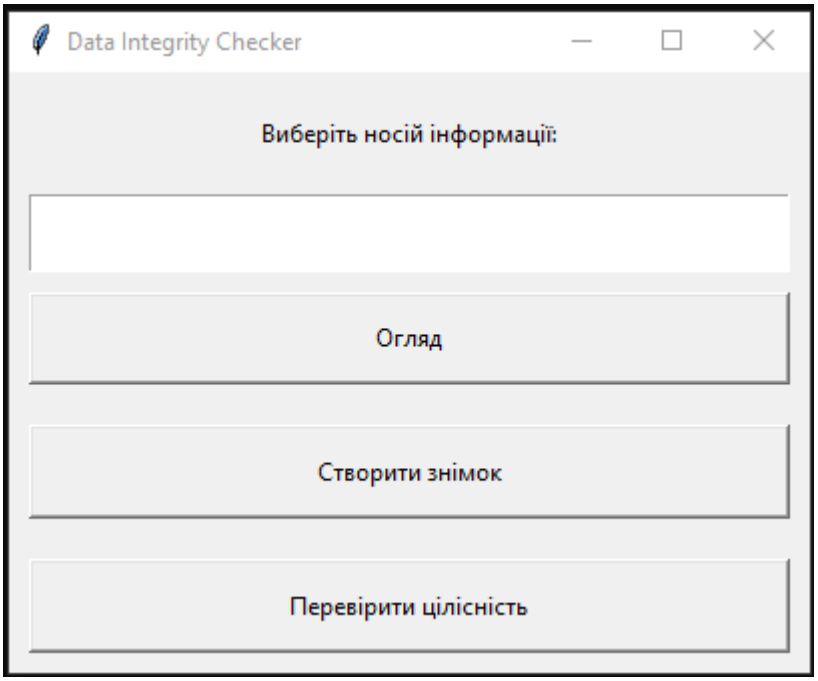

Рисунок 3.3 – Головне меню застосунку

Якщо немає бажання вводити адресу носія інформації, його можна вибрати натиснувши кнопку «Огляд», з’явиться наступне вікно вибору (рис. 3.4), в якому легко та наглядно видно, що можна вибрати.

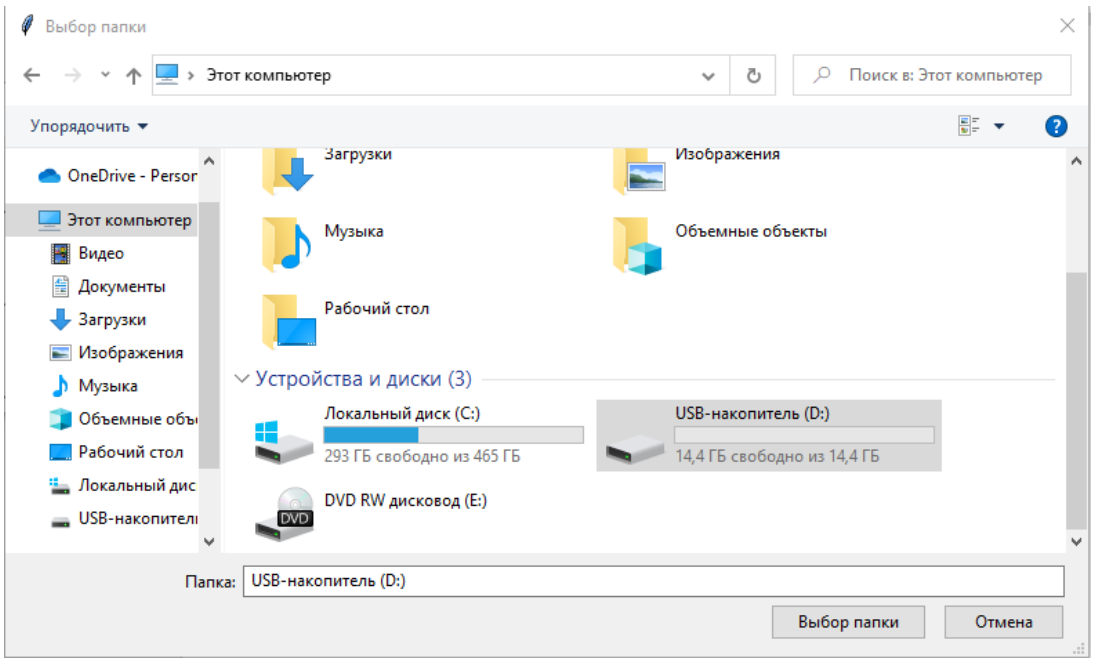

Рисунок 3.4 – Вікно огляду доступного для вибору носія інформації

Після вибору вибраний носій інформації, його адреса з’явиться в полі вводу зображено на рисунку 3.5. Коли в полі введена адреса, застосунок всі подальші дії виконує по відношенню саме до цього носія інформації, якщо є необхідність можна вибрати інший, застосунок переключиться на нього.

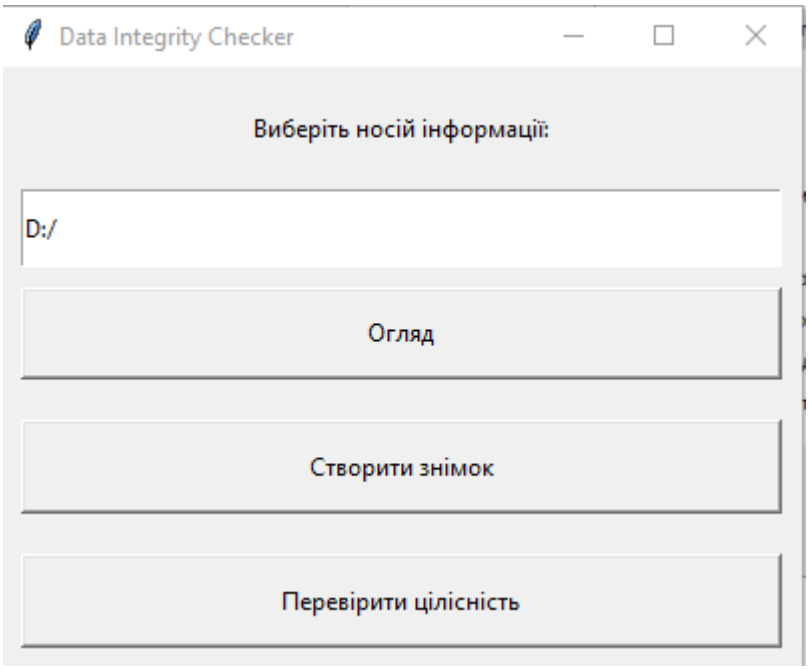

Рисунок 3.5 – Вид головного меню після вибору носія інформації

Тепер коли носій вибраний, можна натиснути кнопку «Створити знімок», застосунок видає наступне повідомлення, яка показано на рисунку 3.6. Якщо навіть виникне якась помилка, що мало ймовірно в даному фрагменті коду, передбачено виключення, застосунок продовжить роботу, це дає змогу розібратися в чому була проблема, щоб її вирішити. Створений «знімок» зберігається, як показано на рисунку 3.7.

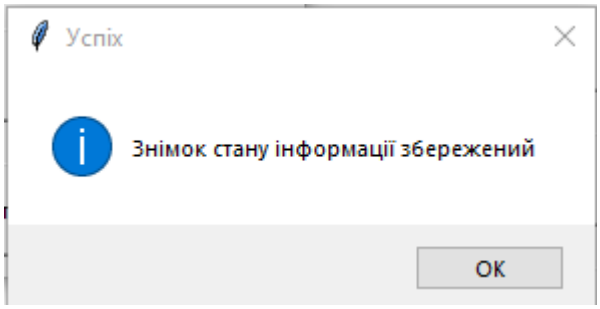

Рисунок 3.6 – Повідомлення про успішне створення «знімку» стану даних

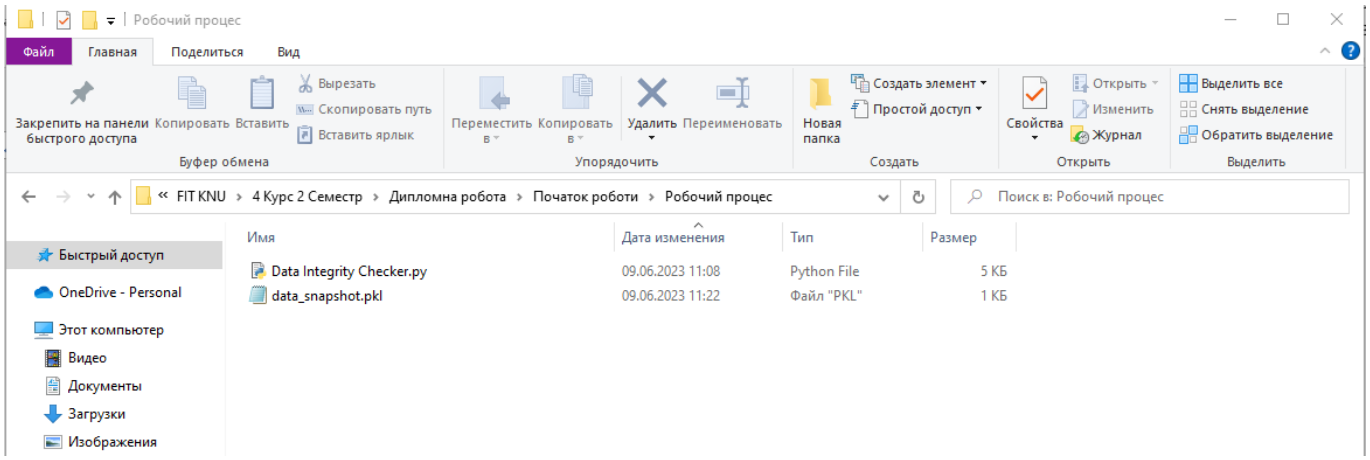

Рисунок 3.7 – Створений файл «знімку» стану даних в форматі .pkl

Файл data_snapshot.pkl має наступний вміст, як показано на рисунку 3.8. Це хеш-сума перевіреного носія інформації. Вона не є людиночитною, без застосунку неможливо з цього набору даних щось зрозуміти. Цей файл можна зберігати для можливості перевірки носія через деякий час.

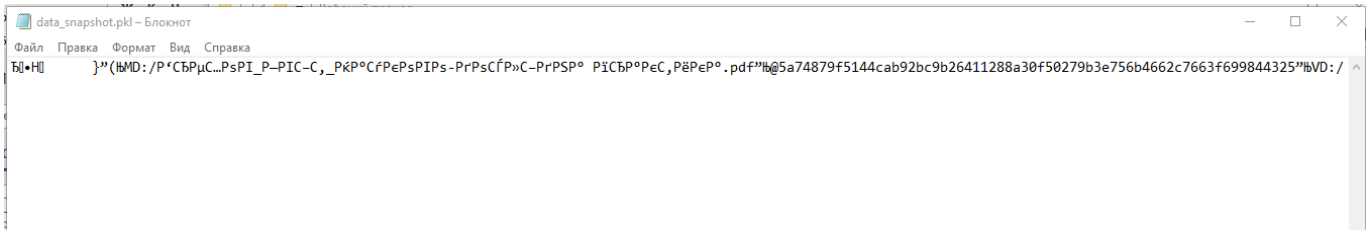

Рисунок 3.8 – Вміст файлу data_snapshot.pkl

Тепер перейдемо до директорії носія інформації в даному прикладі це флеш-накопичувач, його вміст показаний на рисунку 3.9. Бачимо список з документів, розуміємо, що застосунок створив «знімок» на основі цього стану носія, тому виконаємо ряд змін для демонстрації роботи застосунку.

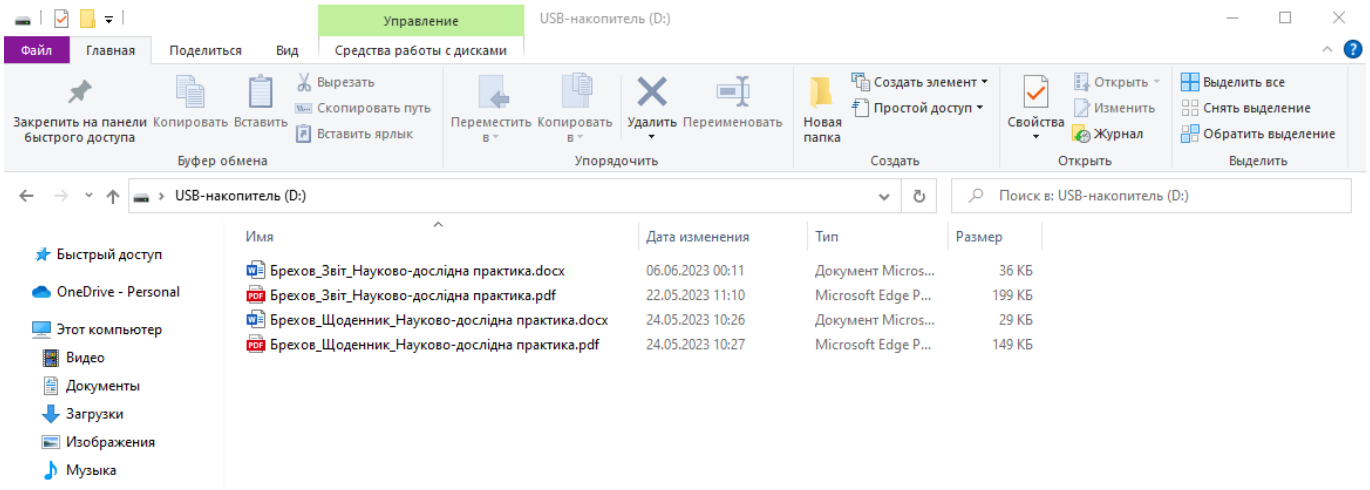

Рисунок 3.9 – Вміст флеш-накопичувача

До початку внесення змін, виконаємо перевірку цілісності, перевіримо вивід застосунку в цьому випадку. Бачимо на рисунку 3.10 повідомлення, що зміни не були виявленні, а значить поки робота коректна, йдемо далі.

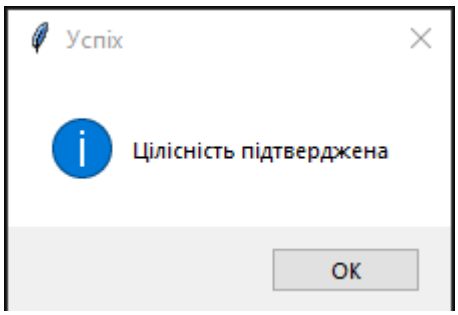

Рисунок 3.10 – Повідомлення про відсутність змін

Для початку внесемо зміни в якійсь файл, в нашому випадку документ .docx, видалимо слово, це будуть легкі зміни тому наглядно видно степінь його детектування (рис. 3.11).

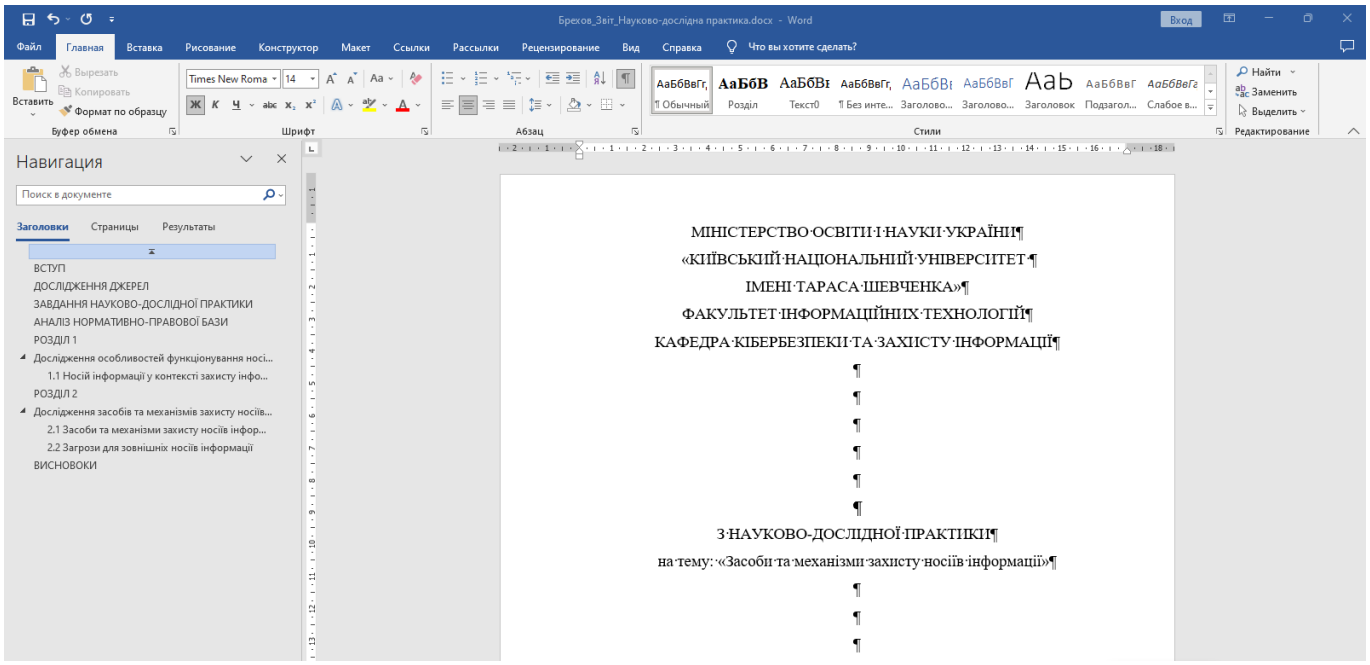

Рисунок 3.11 – Внесені зміни до файлу .docx, видалено слово

Наступним кроком, створимо новий файл Тест.accdb, а також перейменуємо інший файл давши йому назву Тест2, це такі собі найрозповсюдженіші зміни, які можуть виникнути. На рисунку 3.12 показано вигляд директорії накопичувача на момент внесених змін.

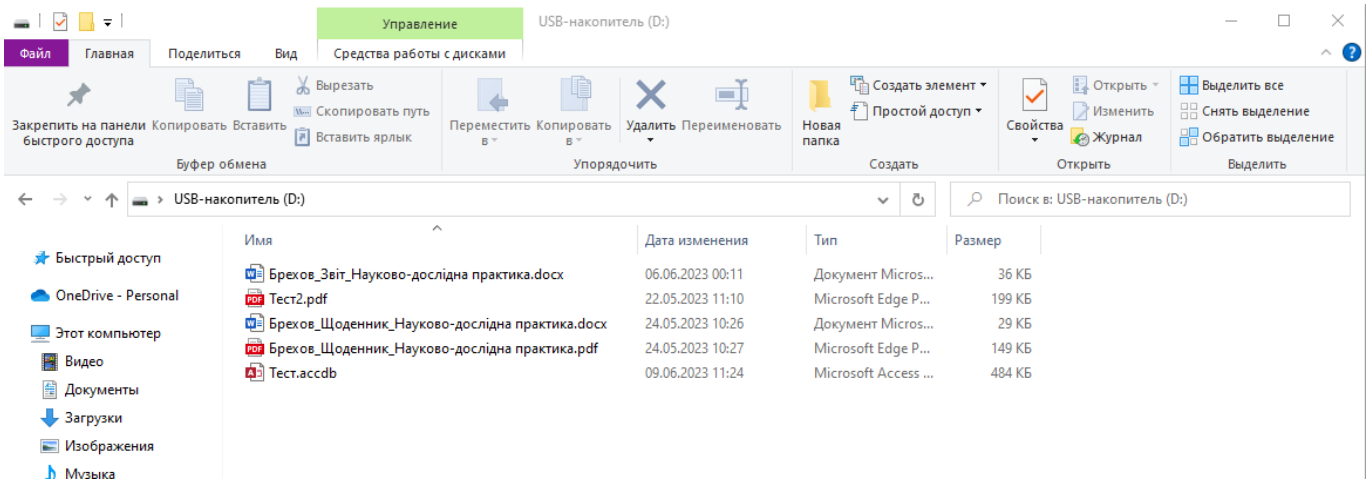

Рисунок 3.12 – Внесені зміни до файлів на носії інформації

Запустимо застосунок та натиснемо кнопку «Перевірити цілісність», я нас вже є «знімок» стану даних, потрібно тільки знову вибрати потрібний носій інформації. Застосунок виконує перевірку та видає наступне повідомлення, яка показано на рисунку 3.13.

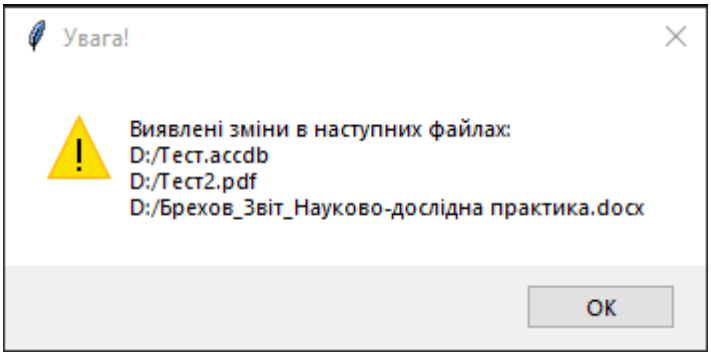

Рисунок 3.13 – Виявленні зміни в цілісності даних на носії інформації

Застосунок в повідомленні розміщує список файлів, які підлягли змінам, це дає змогу одразу відреагувати на проблему, яка виникла.

Висновки за розділом 3

Метою розділу 3 було розробити та реалізувати застосунок для забезпечення цілісності даних на цифрових носіях інформації. Захист від модифікації та спотворення є важливим, тому що наразі проблема підробки інформації, або некоректної роботи з нею є актуальною. Застосунок демонструє роботу такого засобу захисту, як забезпечення цілісності, використання хеш-функції SHA-256 є чудовим, простим та сильним рішенням. Функція легка у використанні, швидкодіюча при здатності реагувати на незначні зміни.

В розділі був описаний функціонал застосунку, як та з чим він буде працювати, в нашому випадку він працює з більшістю цифрових носіїв інформації, але функціонал дозволяє масштабувати його на рівень окремих директорій. Була описана архітектура застосунку по окремих реалізованих функціях, а також описані технічні особливості: формат .pkl, хеш- функція SHA-256, а також бібліотека tkinter. Було описано принципи реалізації та вибрані методології, продемонстровано його роботу.

ВИСНОВКИ

У кваліфікаційній роботі було проведено дослідження засобів та механізмів захисту носіїв інформації. Розділ 1 було присвячено теоретичним засадам захисту носіїв інформації, включаючи аналіз нормативно-правової бази, класифікацію носіїв інформації та основні принципи захисту носіїв інформації. В розділі 2 було досліджено існуючі засоби та механізми захисту носіїв інформації, акцентувалося на шифруванні, аутентифікації, контролі доступу та забезпеченні цілісності. Розділ 3 був присвячений розробці та реалізації застосунку для забезпечення цілісності даних на цифрових носіях інформації, за допомогою хеш-функції SHA-256.

Узагальнюючи, дана робота вирішує актуальну проблему захисту інформації, зосереджуючись на носіях інформації, які є нерозривно пов'язаними з самою інформацією. Вона надає теоретичну та практичну основу для ефективного захисту цифрових носіїв інформації. Результати досліджень показують, що використання відповідних засобів і механізмів захисту може зменшити ризики витоку інформації та несанкціонованого доступу до неї. Застосунок, розроблений у розділі 3, демонструє ефективну роботу використання хеш-функції SHA-256 для забезпечення цілісності даних.

Отже, ця робота пропонує внесок у галузь інформаційної безпеки, підготовляючи ґрунт для подальшого дослідження та розробки засобів та механізмів захисту носіїв інформації.

Виходячи із поставленої мети кваліфікаційної роботи були в повному обсязі виконані наступні *завдання:*

- проаналізовано види та класифікацію носіїв інформації;
- проаналізовано теоретичні засади захисту носіїв інформації;
- проведено дослідження засобів та механізмів захисту носіїв інформації;
- реалізовано застосунок для забезпечення цілісності інформації на цифрових носіях інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

3. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

4. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736 [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF#Text.

5. Україна поглиблює співпрацю з Агентством ЄС із мережевої та інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://it.novyny.live/vzaimnoe-partnerstvo-ukraina-razvivaet-sotrudnichestvo-s-enisa-57681.html.

6. Носії інформації, їх класифікація та основні характеристики [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/9706703/page:29/.

7. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

8. Mark S. Information Security: Principles and Practice [Електронний ресурс] / Stamp Mark // Wiley. – 2011. – Режим доступу до ресурсу: https://muktadesaiblog.files.wordpress.com/2019/06/information-security-principles-and-practice-2nd-edition-stamp.pdf.

9. The Current State Of Authentication: We Have A Password Problem [Електронний ресурс] – Режим доступу до ресурсу: https://www.smashingmagazine.com/2016/06/the-current-state-of-authentication-we-have-a-password-problem/.

10. Контроль доступу (Access control) до інформації як один із ключових елементів інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://bsoprivacygroup.com/gdpr-personal-data-access-control/.

11. NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management [Електронний ресурс] – Режим доступу до ресурсу: https://pages.nist.gov/800-63-3/sp800-63b.html.

12. Шифрування [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Шифрування.

13. Стандарти інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Стандарти_інформаційної_безпеки.

14. Хеш-функція [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Хеш-функція.

15. Механізми захисту від навмисних загроз [Електронний ресурс] – Режим доступу до ресурсу: https://stud.com.ua/53396/informatika/mehanizmi_zahistu_navmisnih_zagroz.

16. Контрольна сума [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Контрольна_сума.

17. Galois/Counter Mode [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Galois/Counter_Mode.

18. Understanding the Three Factors of Authentication [Електронний ресурс] – Режим доступу до ресурсу: https://www.pearsonitcertification.com/articles/article.aspx?p=1718488.

19. Електронний цифровий підпис [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Електронний_цифровий_підпис.

20. Антивірусна програма [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/ Антивірусна_програма.

21. Путівник мовою програмування Python [Електронний ресурс] – Режим доступу до ресурсу: https://pythonguide.rozh2sch.org.ua.

22. Hashlib — Захищені хеші та дайджести повідомлень [Електронний ресурс] – Режим доступу до ресурсу: https://docs.python.org/uk/3/library/hashlib.html.

23. Модуль pickle. Серіалізація об’єктів. Приклади використання для запису/читання інформації з бінарних файлів [Електронний ресурс] – Режим доступу до ресурсу: https://www.bestprog.net/uk/2020/05/06/python-module-pickle-serialization-of-objects-examples-of-use-for-writing-reading-information-from-binary-files-ua/.

24. A Definitive Guide to Learn The SHA-256 (Secure Hash Algorithms) [Електронний ресурс] – Режим доступу до ресурсу: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm.

25. Бібліотека tkinter мови Python [Електронний ресурс] – Режим доступу до ресурсу: http://www.kievoit.ippo.kubg.edu.ua/kievoit/2016/tkinter/index.html.

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Тези наукових доповідей:

1. Брехов М. Засоби та механізми захисту носіїв інформації / Михайло Брехов, Іван Пархоменко / VI Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) 27 квітня 2023, Київ, Україна, стр. 95-96.

ДОДАТОК Б
РЕАЛІЗАЦІЯ ЗАСТОСУНКУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Програмний код застосунку для забезпечення цілісності інформації:

```
import hashlib
import os
import pickle
import tkinter as tk
from tkinter import filedialog, messagebox


class DataIntegrityChecker:
    def __init__(self, root):
        self.root = root
        self.root.title("Data Integrity Checker")
        self.directory = tk.StringVar()
        self.snapshot_path = os.path.abspath("data_snapshot.pkl")
        self.hash_function = hashlib.sha256

        self.create_widgets()

    def create_widgets(self):
        self.directory_label = tk.Label(self.root, text="Виберіть носій інформації:")
        self.directory_label.pack(fill=tk.BOTH, expand=True, padx=10, pady=10)

        self.directory_entry = tk.Entry(self.root, textvariable=self.directory)
        self.directory_entry.pack(fill=tk.BOTH, expand=True, padx=10)

        self.browse_button = tk.Button(self.root, text="Огляд", command=self.browse_directory)
        self.browse_button.pack(fill=tk.BOTH, expand=True, padx=10, pady=10)

        self.snapshot_button = tk.Button(self.root, text="Створити знімок",
command=self.create_snapshot)
```

```
        self.snapshot_button.pack(fill=tk.BOTH, expand=True, padx=10, pady=10)

        self.verify_button = tk.Button(self.root, text="Перевірити цілісність",
command=self.verify_integrity)
        self.verify_button.pack(fill=tk.BOTH, expand=True, padx=10, pady=10)

        self.root.bind("<Configure>", self.on_window_resize)

    def browse_directory(self):
        selected_directory = filedialog.askdirectory()
        self.directory.set(selected_directory)

    def create_snapshot(self):
        directory = self.directory.get()
        if not directory:
            messagebox.showerror("Помилка", "Виберіть носій інформації")
            return

        file_list = self.get_file_list(directory)
        snapshot = self.generate_snapshot(file_list)
        self.save_snapshot(snapshot)

        messagebox.showinfo("Успіх", "Знімок стану інформації збережений")

    def get_file_list(self, directory):
        file_list = []
        for root, _, files in os.walk(directory):
            for file in files:
                file_path = os.path.join(root, file)
                file_list.append(file_path)
        return file_list

    def generate_snapshot(self, file_list):
        snapshot = {}
        for file_path in file_list:
```

```
                with open(file_path, "rb") as file:
                    data = file.read()
                    file_hash = self.calculate_hash(data)
                    snapshot[file_path] = file_hash
            return snapshot

        def calculate_hash(self, data):
            hash_object = self.hash_function()
            hash_object.update(data)
            return hash_object.hexdigest()

        def save_snapshot(self, snapshot):
            try:
                with open(self.snapshot_path, "wb") as file:
                    pickle.dump(snapshot, file)
            except Exception as e:
                messagebox.showerror("Помилка", "Не вдалося зберегти знімок стану інформації: {}".format(str(e)))

        def verify_integrity(self):
            directory = self.directory.get()
            if not directory:
                messagebox.showerror("Помилка", "Виберіть носій інформації")
                return

            file_list = self.get_file_list(directory)
            snapshot = self.load_snapshot()
            modified_files = []

            for file_path in file_list:
                with open(file_path, "rb") as file:
                    data = file.read()
                    file_hash = self.calculate_hash(data)
                    if file_path not in snapshot or file_hash != snapshot[file_path]:
                        modified_files.append(file_path)
```

```
            if modified_files:
                messagebox.showwarning("Увага!", "Виявлені зміни в наступних файлах:\n" +
"\n".join(modified_files))
            else:
                messagebox.showinfo("Успіх", "Цілісність підтверджена")

        def load_snapshot(self):
            try:
                with open(self.snapshot_path, "rb") as file:
                    snapshot = pickle.load(file)
                    return snapshot
            except FileNotFoundError:
                return {}
            except Exception as e:
                messagebox.showerror("Помилка", "Не вдалося завантажити знімок стану інформації:
{}".format(str(e)))

        def on_window_resize(self, event):

            self.root.update_idletasks()
            self.root.minsize(400, 300)


    if __name__ == "__main__":
        root = tk.Tk()
        app = DataIntegrityChecker(root)
        root.mainloop()
```