Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Кібербезпека»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Мелкозьорова О. М.

_____

« » червня 2024 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

за спеціальністю: 125 - Кібербезпека

на тему: «Аналіз технологій та дослідження можливостей сучасних засобів знищення даних»

оцінка « »

Голова ЕК

Лемешко О.В._____

Керівник: Малахов С. В._____

(прізвище та ініціали/підпис)

Рецензент: Гостєв О. Л._____

(прізвище та ініціали/підпис)

Виконавець: студентка групи КБ-41

Щербець Н. В._____

(прізвище та ініціали/підпис)

Харків – 2024

РЕФЕРАТ

Пояснювальна записка містить: 52 сторінки, 7 таблиць, 97 рисунків, 40 використаних джерел та 4 додатки.

Мета роботи: — аналіз існуючих технологій знищення інформації та дослідження властивостей відомих програмних засобів видалення даних.

Об'єкт дослідження: — технології і методи знищення даних на різних типах носіїв інформації.

Предмет дослідження: — способи та засоби знищення і відновлення інформації для основни типів носіїв даних.

Основними методами досліджень є аналіз та порівняння результатів тестування програмних засобів (ПЗ) знищення та відновлення даних.

В роботі досліджені відомі технології і стандарти знищення інформації. Визначені основні принципи організації файлових систем та способи розмітки дискового простору. Узагальнено відомості щодо особливостей функціонування сучасних моделей накопичувачів, насамперед HDD та SSD дисків. Зроблен аналіз деяких показових нормативних вимог, стосовно специфіки знищення даних у різних країнах світу. Виконано огляд найбільш відомих апаратних та програмних засобів для знищення і відновлення даних. Проведено тестування найбільш показових зразків спеціалізованого ПЗ для знищення та відновлення даних з різних типів носіїв інформації. Оцінено результати тестувань та надано рекомендації, щодо їх використання та можливостей.

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний матеріал для підвищення рівня компетенцій персоналу сучасних організацій при вирішенні завдань утилізації накопичувачів даних та знищення «чутливої» корпоративної інформації.

Ключові слова: ЗНИЩЕННЯ ДАНИХ, ВІДНОВЛЕННЯ ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, НАКОПИЧУВАЧ ДАНИХ, ІНСАЙД.

ABSTRACT

The explanatory note contains: 52 pages, 7 tables, 97 figures, 40 used sources and 4 appendix.

The purpose of the work: - analyze the existing technologies of information destruction and study the properties of known data deletion software.

The object of research: - technologies and methods of data destruction on various types of storage media.

Subject of research: - methods and tools for data destruction and recovery for the main types of storage media.

The main research methods are the analysis and comparison of the results of testing software for data destruction and recovery.

The work examines the known technologies and standards of information destruction. The basic principles of file system organization and methods of disk space allocation are defined. Information on the peculiarities of the functioning of modern models of drives, primarily HDD and SSD disks, is summarized. Analyzed are some indicative regulatory requirements regarding the specifics of data destruction in different countries of the world. The most famous hardware and software tools for data destruction and recovery are reviewed. The most representative examples of specialized software for data destruction and recovery from various types of storage media were tested. The test results are evaluated and recommendations on their use and capabilities are given.

The results of this work can be used for educational purposes and as a support material to improve the competence of personnel of modern organizations in solving the problems of data storage utilization and destruction of “sensitive” corporate information.

Keywords: DATA DESTRUCTION, DATA RECOVERY, INFORMATION SECURITY, DATA STORAGE, INSIGHT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

SSD – твердотілий накопичувач (Solid-state drive);

HDD – жорсткий диск (Hard disk drive);

FAT – таблиця розміщення файлів (File Allocation Table);

NTFS – файлова система нової технології (New technology file system);

Ext – розширена файлова система Linux (Extended file system);

APFS – файлова система, розроблена Apple (Apple File System);

HFS – ієрархічна файлова система (Hierarchical File System);

GDPR – загальний регламент захисту даних (General Data Protection Regulation);

GNU – проект вільного програмного забезпечення (GNU's Not Unix);

GDPR – система запобігання вторгненням (Intrusion Prevention System);

ДСТУ – Державні стандарти України;

ISO – Міжнародна організація зі стандартизації (Internation Organization for Standardization);

ПЗ – програмне забезпечення;

ОС – операційна система;

NOR – вид флеш-пам'яті;

NAND – вид флеш-пам'яті;

SATA – інтерфейс обміну даними з накопичувачами інформації (Serial ATA).

ВСТУП

У сучасному цифровому світі, де обмін та зберігання інформації є невід'ємною складовою кожного аспекту нашого життя, питання збереження та безпеки даних стає надзвичайно актуальним. Швидкий розвиток технологій супроводжується не лише збільшенням обсягів цифрової інформації, але й підвищенням загроз безпеці її зберігання.

Ця робота присвячена дослідженню найбільш поширених методів та засобів знищення даних на різних типах носіїв інформації. Дослідження охоплює аналіз принципів організації файлових систем, а також методів знищення інформації на твердотільних та магнітних накопичувачах. Зосереджуючись на таких аспектах, як нормативні вимоги, апаратні засоби та властивості спеціалізованого програмного забезпечення (ПЗ), робота буде сфокусована на дослідженнях основних принципів та методів забезпечення безпеки цифрової інформації при виконанні процедур безпечної утилізації використовуваних накопичувачів та/чи видалення окремих масивів даних.

Актуальність роботи полягає в необхідності забезпечення надійного знищення конфіденційних/чутливих даних (безвідносно типу кінцевих користувачів), що є однією їз важливих складових в загальній системі захисту інформації від несанкціонованого доступу до неї. З розвитком технологій зберігання даних виникає потреба у вдосконаленні існуючих методів знищення даних та розробці нових, які б відповідали сучасним вимогам та особливостям використовуваних апаратних засобів.

Основна мета роботи пов'язана з аналізом відомих технологій видалення інформації та дослідження властивостей найбільш поширеного ПЗ, що реалізують різні підходи при реалізації відповідної задачі. Для досягнення цієї мети використовується метод комплексного аналізу і порівняння, який поєднує вивчення основних теоретичних аспектів, експериментальне тестування та узагальнення отриманих результатів.

1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ФАЙЛОВИХ СИСТЕМ ТА МЕТОДІВ УТИЛІЗАЦІЇ ДАНИХ НА РІЗНИХ ТИПАХ НОСІЇВ

1.1 Огляд теоретичних засад

Огляд теоретичних засад дозволить отримати глибше розуміння основних концепцій, що лежать в основі файлових систем та методів утилізації даних на різних типах носіїв. Цей огляд стане основою для подальшого аналізу та дослідження в цій області, допоможе визначити ключові аспекти та визначити оптимальні підходи до роботи з даними.

Поняття файлової системи є ключовим для розуміння організації та функціонування сучасних операційних систем (ОС) і збереження даних. Файлова система – це спосіб організації та збереження даних на носії інформації, такому як жорсткий диск (HDD), твердотілий накопичувач (SSD), USB-накопичувач тощо. Вона визначає структуру даних, способи доступу до них та механізми управління цими даними [1].

Основні компоненти файлової системи включають:

- Основна одиниця збереження інформації. Файли можуть бути текстовими, відео, аудіо, програмами тощо.
- Структура, яка організовує файли у логічні групи. Каталоги можуть містити підкаталоги та файли.
- Метадані, які описують кожен файл, такі як ім'я, розмір, дата створення, дозволи доступу тощо.

Файлова система також включає в себе набір правил та процедур, які визначають, які дії можна виконати з файлами та каталогами, як вони організовані на носії даних та як вони захищені від несанкціонованого доступу або втрати.

Основні функції файлової системи включають:

- Створення, збереження та видалення файлів та каталогів.

- Управління доступом до файлів та каталогів за допомогою прав доступу.
- Організація файлів та каталогів у структури з урахуванням ієрархії та логічних відносин.
- Забезпечення ефективного використання дискового простору та оптимізація доступу до даних.

Поняття файлової системи є важливим як для користувачів, які взаємодіють з файлами у їх повсякденній роботі, так і для розробників, які створюють операційні системи та програмне забезпечення (ПЗ) для роботи з даними.

Принципи організації файлових систем визначають способи, за якими дані зберігаються, організовані та керуються на зберіжних пристроях.

Файлові системи зазвичай використовують ієрархічну структуру для організації файлів та каталогів. Це означає, що файли розміщені в каталогах, які можуть містити інші каталоги або файли. Ієрархічна структура дозволяє легко організовувати та керувати великими обсягами даних.

Файлові системи мають механізми для відстеження вільного простору на диску. Це дозволяє оптимізувати розміщення нових файлів на диску та уникнути фрагментації даних [2].

Кожен файл та каталог у файловій системі має унікальний ідентифікатор або адресу, який дозволяє системі знаходити та керувати ними.

Операційна система забезпечує набір функцій для роботи з файловою системою, таких як створення, відкриття, закриття, зміна та видалення файлів та каталогів.

Сучасні операційні системи зазвичай підтримують різні типи файлових систем, такі як FAT (File Allocation Table), NTFS (New technology file system), ext (Extended file system) тощо. Це дозволяє користувачам вибирати найбільш підходящий тип файлової системи залежно від їх потреб та вимог.

Принципи, розглянуті вище, допомагають створити структуровану, ефективну та надійну систему для зберігання та управління даними на різних типах носіїв.

Загальною характеристикою файлових систем є їх функціональність та продуктивність, що визначаються швидкодією доступу до даних, максимальним обсягом файлів та розміром файлової системи, підтримкою різних операційних систем, системою прав доступу та шифруванням даних, а також стійкістю до пошкоджень та можливістю відновлення даних. Важливо враховувати ці характеристики при виборі файлової системи, оскільки вони визначають її придатність для конкретного використання та забезпечують оптимальну роботу з даними.

1.2 Принципи розмітки дискового простору

Під час партіціонування фізичний диск розділяється на логічні сегменти, відомі як партіції, що дозволяє виділити окремі області диска для різних цілей, таких як зберігання операційної системи, програм та користувацьких даних.

Форматування включає створення файлової системи на кожній партіції. Під час цього процесу визначаються параметри файлової системи, такі як тип (наприклад, FAT32, NTFS, ext4), розмір блоку та таблиця файлів.

Після форматування партіцій диск поділяється на логічні сегменти або блоки. Кожен сегмент має унікальну адресу та може містити певну кількість даних.

Файлові системи включають механізми відстеження вільного простору на диску та управління ним, що дозволяє оптимізувати розміщення нових файлів та уникнути фрагментації даних.

Для забезпечення безпеки даних використовуються стратегії захисту, такі як резервне копіювання та розміщення файлів на різних ділянках диска, що допомагає уникнути втрати даних у разі пошкодження або втрати диска.

1.3 Нормативні вимоги щодо знищення даних

Нормативні вимоги щодо знищення даних визначають правила та процедури, які повинні дотримуватися при видаленні або знищенні інформації на різних типах носіїв даних. Ці вимоги можуть включати в себе рекомендації щодо застосування спеціальних програмних засобів для безпечного видалення інформації, вимоги щодо фізичного знищення носіїв даних та вимоги до забезпечення конфіденційності та безпеки під час процесу утилізації. Дотримання цих вимог є важливим для запобігання витоку конфіденційної інформації та забезпечення відповідності вимогам законодавства щодо захисту даних [3].

Державні стандарти України (ДСТУ). Аналіз національних стандартів, зокрема (ДСТУ), з огляду на вимоги щодо управління та захисту даних на різних типах носіїв [4]:

1) Аналіз вимог до безпеки даних:

- Перевірка стандартів на наявність вимог до шифрування даних на носіях, контролю доступу та аудиту безпеки.
- Визначення рівня деталізації вимог та їх відповідність сучасним практикам забезпечення безпеки.

2) Аналіз стандартів щодо видалення даних:

- Вивчення методів та процедур видалення даних, що включені у стандарти, та їх відповідність сучасним методам управління даними.
- Оцінка вимог до безпеки процедур видалення даних та їх можливого впливу на ефективність знищення інформації.

3) Аналіз вимог до резервного копіювання та відновлення даних:

- Огляд вимог до процедур резервного копіювання та відновлення даних, включених у стандарти, та їх відповідність сучасним методам управління даними.
- Визначення рекомендацій щодо забезпечення надійності та доступності даних під час відновлення.

4) Аналіз норм щодо файлових систем:

- Перевірка наявних вимог до підтримки різних типів файлових систем та їх відповідність сучасним стандартам та практикам.
- Оцінка вимог щодо безпеки файлових систем та їх відповідність сучасним вимогам до захисту даних.

5) Аналіз вимог до апаратних засобів знищення інформації:

- Вивчення вимог до апаратних засобів знищення інформації на носіях даних та їх відповідність сучасним технологіям та методам знищення.
- Оцінка рівня деталізації вимог та їх відповідність здатності забезпечити ефективне та безпечне знищення даних.

Аналіз нормативних вимог дозволяє з'ясувати, наскільки національні стандарти відповідають сучасним потребам управління та захисту даних на різних типах носіїв.

Міжнародні стандарти (ISO). Стандарти ISO, зокрема ISO/IEC 27001, містять вимоги до систем управління інформаційною безпекою. Ці вимоги охоплюють такі аспекти, як розробка політик безпеки, встановлення контролю доступу, впровадження криптографічного захисту тощо [5].

ISO/IEC 27002 надає рекомендації щодо захисту даних, включаючи вимоги до фізичного та логічного контролю доступу, захисту від зловживання, захисту даних під час їх передачі тощо.

ISO/IEC 27035 надає рекомендації щодо управління інцидентами безпеки, включаючи процедури реагування на інциденти, їх аналіз та запобігання подібним інцидентам у майбутньому.

ISO 8000 спрямовані на управління якістю даних та містять рекомендації щодо процедур контролю та покращення якості даних.

Вимоги щодо знищення даних на різних типах носіїв. Більшість міжнародних стандартів ISO, таких як ISO/IEC 27001, містять вимоги до видалення даних як складової частини системи управління інформаційною

безпекою. Однак, конкретні методи та процедури видалення можуть визначатися окремими стандартами або рекомендаціями.

Вимоги до методів знищення даних на різних типах носіїв можуть бути різними в залежності від чутливості інформації та ступеня захищеності. Наприклад, для HDD може рекомендуватися багатократне перезаписання даних, а для SSD - фізичне руйнування носія [6].

Стандарти ISO/IEC 27001 та ISO/IEC 27002 містять вимоги до забезпечення безпеки процедур утилізації даних, включаючи контроль доступу до пристроїв, що використовуються для знищення, аудит процесу утилізації та забезпечення конфіденційності інформації.

Різні країни мають власне законодавство та регулятивні вимоги щодо утилізації даних, зокрема вимоги щодо захисту персональних даних та конфіденційної інформації. Наприклад, у Європейському Союзі застосовується Загальний регламент з захисту даних (GDPR).

Наявність стандартизованих процедур утилізації даних може варіюватися в залежності від галузі або регіону. Наприклад, стандартизовані методи можуть бути розроблені організаціями, що спеціалізуються на захисті даних або управлінні ризиками.

1.4 Апаратні та програмні засоби знищення інформації на SSD та HDD

В сучасному світі захист конфіденційної інформації на комп'ютерних носіях є критично важливим завданням. На щастя, існує кілька ефективних методів знищення даних на HDD та SSD, які дозволяють забезпечити надійний захист інформації від несанкціонованого доступу.

Один з найбільш ефективних способів знищення даних на HDD та SSD полягає у їх фізичному руйнуванні. Для HDD це може включати буртування, подрібнення або інше механічне знищення диска. Для SSD можна використовувати спеціалізовані пристрої для механічного руйнування чипів пам'яті.

Електромагнітна дегаусація - метод полягає у використанні сильного магнітного поля для знищення даних на HDD. Однак для SSD цей метод зазвичай не ефективний через особливості технології зберігання даних на напівпровідниках.

Перезаписання даних - метод включає в себе многократне перезаписання даних на носіях, що може зробити їх відновлення неможливим. Однак для SSD цей метод може бути менш ефективним через специфічність технології зберігання даних.

Шредери даних - це спеціалізовані пристрої, призначені для безпечного руйнування носіїв, включаючи HDD та SSD. Вони можуть подрібнювати диски на маленькі частинки, що робить відновлення даних неможливим.

Деякі програмні засоби можуть бути використані для знищення даних на HDD та SSD шляхом перезаписання або шифрування інформації. Однак їх ефективність може залежати від конкретної моделі носія та технології зберігання даних [7].

Узагальнюючи, апаратні засоби знищення інформації на SSD та HDD відіграють важливу роль у забезпеченні безпеки та конфіденційності даних. Вибір конкретного методу залежить від потреб користувача та специфіки використання носіїв.

Жорсткий диск (HDD) і твердотілий накопичувач (SSD) - це два основних типи носіїв даних, які використовуються для зберігання і обробки інформації в комп'ютерних системах. Хоча вони служать одній меті - зберіганню даних, їхні принципи роботи значно відрізняються.

HDD використовує механічні рухомі частини для зчитування і запису даних. Основні компоненти HDD включаються:

1) Магнітні диски. Вони зазвичай складаються з одного або більше покритих магнітним шаром дисків, які обертаються зі сталевою віссю в центрі.

2) Головки зчитування/запису. Ці головки, розташовані на рухомому гвинті, переміщуються над поверхнею диска для зчитування та записування даних.
3) Шпиндель. Шпиндель відповідає за обертання дисків з магнітним шаром з високою швидкістю.

Дані зберігаються на HDD у вигляді магнітних змін, що відображають біти інформації. Головки зчитують ці зміни, коли диск обертається. Один з недоліків HDD полягає в тому, що вони мають механічні частини, які можуть вийти з ладу в результаті ударів або пошкоджень [8].

SSD використовує мікросхеми пам'яті для зберігання даних без жодних рухомих частин. Основні компоненти SSD включаються:

1) Флеш-пам'ять. Використовується для зберігання даних у вигляді електричних зарядів. Вона може бути представлена у вигляді NAND або NOR пам'яті.
2) Керуючий контролер. Відповідає за керування операціями зчитування, запису та видалення даних, а також за забезпечення надійності та довговічності SSD.

SSD не має рухомих частин, що робить їх менш схильними до втрати через механічні пошкодження. Вони також мають значно швидший час доступу до даних порівняно з HDD. Однак, вони можуть мати обмежену кількість циклів запису, що може призвести до зношування пам'яті з часом.

Узагальнюючи, як HDD, так і SSD мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб користувача.

Жорсткий диск (HDD) є одним з найпоширеніших носіїв даних, і знищення інформації на ньому може бути важливим для забезпечення безпеки та конфіденційності. Існує кілька методів знищення даних на HDD, які можуть бути використані залежно від рівня захисту, який необхідно досягти.

Механічне знищення диска шляхом подрібнення, буртування або іншого фізичного пошкодження. Цей метод надає найвищий рівень безпеки, але вимагає фізичного доступу до носія.

Використання дегаусера для зміни магнітної орієнтації частинок на диску, що призводить до втрати даних. Цей метод ефективний, але може залежати від типу диска.

Багатократне перезаписання даних на диску, що робить відновлення інформації неможливим. Цей метод вимагає часу, але надає високий рівень захисту.

Комбінація дегаусації або перезаписування з подальшим фізичним знищенням диска. Цей метод забезпечує додатковий рівень безпеки.

Шифрування даних перед знищенням, що робить їх незрозумілими без відповідного ключа. Після цього диск може бути фізично знищений або перезаписаний.

Ці методи можуть бути використані окремо або в комбінації, залежно від потреб безпеки та конфіденційності даних.

SSD (твердотільний накопичувач) - це носій даних, який використовується для зберігання і обробки інформації в комп'ютерних системах. Знищення даних на SSD може бути складнішим завданням порівняно з HDD через особливості їхньої структури і робочих принципів.

Однак існують деякі методи, які можна використовувати для ефективного знищення даних на SSD.

Опишимо декількох з них:

Перезаписання даних. Метод полягає в многократному перезаписанні даних на SSD за допомогою спеціального програмного забезпечення. Це може бути здійснено за допомогою інструментів, які здатні здійснювати многократні перезаписи кожного блоку пам'яті SSD, що робить відновлення даних майже неможливим.

Шифрування даних. Перед знищенням даних їх можна зашифрувати з використанням надійного шифрування. Після цього SSD може бути фізично

знищений або перезаписаний. Шифрування забезпечує додатковий рівень безпеки, оскільки навіть у випадку недостатнього ефекту перезапису, дані залишаються незрозумілими без відповідного ключа.

Фізичне знищення. Цей метод передбачає фізичне пошкодження SSD шляхом подрібнення, розрізання або іншого ушкодження. Фізичне знищення може бути надійним методом знищення даних, але вимагає фізичного доступу до носія.

Використання вбудованих функцій. Деякі виробники SSD надають вбудовані функції, що дозволяють знищувати дані на накопичувачі. Ці функції можуть включати в себе функцію самознищення (Secure Erase), яка перезаписує всі дані на SSD інформацією-сміттям, що робить відновлення даних практично неможливим.

Кожен з цих методів має свої переваги та недоліки, і вибір конкретного методу залежить від вимог до безпеки і конфіденційності даних, а також від можливостей і доступності використання.

Порівняємо ефективність методів знищення даних на різних типах накопичувачів, таких як HDD і SSD. Оскільки структура та принцип роботи цих накопичувачів відрізняються, методи їхнього знищення можуть мати різну ефективність. Оглянемо ключові аспекти порівняння ефективності методів знищення [9]:

1) Методи знищення даних на HDD

- Фізичне руйнування. Надає найвищий рівень безпеки, оскільки відновлення даних практично неможливе.
- Дегаусація. Ефективний метод, але його ефективність може залежати від типу і конфігурації диска.
- Перезаписання даних. Забезпечує високий рівень безпеки, але може вимагати більше часу і ресурсів.
- Фізичне знищення після дегаусації або перезаписування: Комбінація дегаусації або перезаписування з подальшим фізичним знищенням диска забезпечує додатковий рівень безпеки.

2) Методи знищення даних на SSD

- Перезаписання даних. Метод перезаписання даних може бути менш ефективним на SSD через особливості їхньої структури.
- Шифрування даних. Забезпечує додатковий рівень безпеки, але вимагає відповідного ключа для розшифрування даних.
- Фізичне знищення. Цей метод може бути ефективним, але вимагає доступу до носія і може бути часо- та ресурсозатратним.

3) Порівняння ефективності

- Фізичне руйнування може бути найбільш ефективним методом для обох типів накопичувачів.
- Для HDD методи, які використовують магнітні властивості диска, такі як дегаусація, можуть бути досить ефективними.
- Для SSD методи, які залежать від перезаписування даних, можуть бути менш ефективними через особливості їхньої структури.

У загальному, вибір конкретного методу знищення даних на HDD або SSD повинен здійснюватися з урахуванням конкретних обставин, вимог до безпеки і конфіденційності, а також доступності та можливостей використання методу.

Висновки за Розділом.

У першому розділі дипломної роботи було детально розглянуто питання файлових систем, принципів їх організації та розмітки дискового простору, а також аналізовано нормативні вимоги щодо утилізації даних на різних типах носіїв.

Було розглянуто основні поняття файлових систем, їхню структуру та принципи роботи. Виявлено, що кожна операційна система має свою власну файлову систему з унікальними особливостями та можливостями.

Досліджено принципи організації та розмітки дискового простору на носіях. Було виявлено, що правильна розмітка диска дозволяє оптимально використовувати його потенційні можливості та забезпечує ефективне управління даними.

Аналіз національних та міжнародних стандартів показав, що існують чіткі вимоги щодо утилізації даних на різних типах носіїв. Дотримання цих вимог є важливим для забезпечення конфіденційності та безпеки інформації.

Таким чином у 1-му розділі роботи розглянуто основні аспекти, які притаманні до найбільш поширених файлових систем, принципи їх організації та вимоги, щодо утилізації даних на різних типах носіїв. Ця інформація буде корисною для виконання подальших досліджень в межах циклу тестувань відповідного спеціалізованого ПЗ (нижче).

2 ДОСЛІДЖЕННЯ ВІДОМИХ СТАНДАРТІВ І МЕТОДІВ ЗНИЩЕННЯ ДАНИХ ТА СТИСЛИЙ ОГЛЯД ТИПОВИХ ЗРАЗКІВ ПЗ

2.1 Методи знищення даних за допомогою програмних засобів

На даний момент відомо безліч методів безпечного видалення інформації, стандартизованих практично у всіх провідних державах, а також публікуються національні стандарти, норми і правила, що регулюють використання програмних засобів для знищення інформації і описують механізми їх застосування [10].

Найбільш відомими є наступні міжнародні стандарти:

- Алгоритм Пітера Гутмана – алгоритм знищення даних розроблений у 1996 році Пітером Гутманом, який включає 35 циклів перезапису даних різними шаблонами.
- RCMP TSSIT OPS-II – алгоритм перезаписування даних нулями, Раніше цей метод був державним стандартом Канади, котрий включає 7 циклів перезапису даних: 1, 3 та 5 цикли – перезапис даних нулями, 2, 4 та 6 – одиницями та 7 цикл – випадковими символами.
- Алгоритм Брюса Шнайєра – метод знищення даних розроблений Брюсом Шнайєром, котрий включає 7 циклів перезапису даних нулями, одиницями та випадковими символами.
- US DoD 5220.22-M (8-306./E, C & E) – метод перезаписування даних випадковими символами, визначений Міністерством оборони Сполучених Штатів, котрий включає 7 циклів перезапису даних.
- Американський стандарт NAVSO P-5239-26 — алгоритм знищення даних, який застосовується Військово-морськими силами США та включає 3 цикли перезапису даних: спочатку випадковими значеннями, а потім специфічними шаблонами.

- Німецький VSITR – стандарт знищення даних розроблений для Федерального відомства з інформаційної безпеки Німеччини, але більше не використовується цим урядом. Алгоритм складає 7 циклів перезапису даних, котрі включають використання наступних шаблонів: 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, 0xAA.

Більше методів безпечного видалення даних розглянуто у Додатку А.

Проаналізувавши методи знищення даних, можна сформувати таблицю (Табл. 2.1) з короткою характеристикою кожного з них.

Таблиця 2.1 – Порівняльна характеристика методів знищення даних

Назва стандарту/методу	Кількість циклів	Переваги	Недоліки
Метод Пітера Гутмана	35	Вважається найнадійнішим методом	Часозатратний
RCMP TSSIT OPS-II	7	Надійний, виконує перевірку в кінці	Відносно довгий процес
Алгоритм Брюса Шнайєра	7	Ефективний, широко розповсюджений	Низька надійність знищення даних
US DoD 5220.22-M (8-306./E, C & E)	7	Стандарт військового рівня, більш надійний за NAVSO P-5239-26 та US Air Force 5020, котрі включають всього 3 цикли перезапису даних	Низька надійність знищення даних на сучасних SSD-дисках
Американський стандарт NAVSO P-5239-26	3	Швидкий та досить надійний метод	Не завжди ефективний через малу кількість циклів
VSITR (Німеччина)	7	Високий рівень безпеки, рекомендований німецьким урядом	Відносно довгий процес видалення даних

Серед переглянутих методів найбільш ефективним вважається метод Пітера Гутмана, але він також є найбільш часозатратним методом. Найшвидшими алгоритмами є Американський стандарт NAVSO P-5239-26 та US Air Force 5020, але їх ефективність безпечного знищення даних може бути не надто надійною. Переглянуті стандарти і методи знищення даних використовуються в різних програмних засобах для повного та безпечного видалення файлів. Деякі з програмних засобів також включають в собі власні алгоритми знищення даних. Кожна з описаних нижче програм відрізняється своїм інтерфейсом, можливостями і функціональністю [10].

1) “Eraser” – програмне забезпечення для безпечного видалення окремих файлів, каталогів та їх попередньо видалені копії, а також цілі диски чи розділи та невикористаний простір на диску. Воно працює на операційних системах Windows XP (з пакетом оновлень 3), Windows Server 2003 (з пакетом оновлень 2), Windows Vista, Windows Server 2008, Windows 7,8,10 і Windows Server 2012. Windows 98, ME, NT, 2000 [11].

“Eraser” є безкоштовним програмним забезпеченням і публікується під загальною публічною ліцензією GNU.

“Eraser” підтримує низку найпопулярніших стандартів утилізації даних опубліковних різними країнами за останні декілька десятиліть. Основна ідея полягає в перезаписі місця на диску, де зберігалися файли, використовуючи різні шаблони таким чином, щоб відновлення даних було складним чи неможливим. Також є можливість налаштування різних завдань, які будуть виконуватися вручну після кожного запуску Windows або за розкладом.

Стандарти знищення даних, які підтримуються “Eraser” [12]:

- Метод Пітера Гутмана
- US DoD 5220.22-M (8-306./E, C & E)
- RCMP TSSIT OPS-II
- Алгоритм Брюса Шнайєра
- Німецький VSITR
- US DoD 5220.22-M (8-306./E)

- Британський HMG IS5 (розширений)
- US Air Force 5020
- Армія США AR380-19
- Російський ГОСТ Р50739-95
- Британський HMG IS5 (базова лінія)
- Псевдовипадкові дані – це метод швидкого очищення, який перезаписує наявні дані випадковими символами.
- Стирання перших/останніх 16 КБ – швидкий і простий спосіб ускладнити пошук/відновлення файлів. Якщо розмір файлу перевищує 32 Кбайт, дані залишаться на диску.

Переваги:

- Зручний інтерфейс;
- Підтримка багатьох стандартів знищення даних;
- Можливість видалення окремих файлів, цілих каталогів або дисків;
- Можливість планування завдань на регулярній основі;
- Інтегрований з оболонкою Windows, що дозволяє легко видаляти файли та папки безпосередньо з контекстного меню.

Недоліки:

- Тільки для Windows;
- Знищення даних може бути досить часозатратним;
- Можливі випадкові збої під час процесу видалення даних.

2) “File Shredder” – безкоштовне програмне забезпечення, яке було випущено за ліцензією GNU, для швидкого, безпечного та надійного знищення даних. У “File Shredder” є можливість обрати між 5-ма різними алгоритмами перезапису даних, а також має функцію очищення диска для видалення невикористаного дискового простору [13].

“File Shredder” працює на операційних системах Windows NT, Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 7,8,10.

Алгоритми знищення даних, які підтримуються “File Shredder”:

- Простий (1 цикл) – швидкий, але менш безпечний метод перезапису даних випадковими даними.
- Простий (2 цикли) – перезаписує дані двічі: спочатку нулями, а потім одиницями
- US DoD 5220.22-M
- Безпечний алгоритм знищення даних (7 циклів) – перезапис даних з використанням комбінацій нулів, одиниць та випадкових даних для збільшення надійності знищення даних
- Метод Пітера Гутмана

Переваги “File Shredder”:

- Простий у використані;
- Підтримка 5-ти різних алгоритмів знищення даних;
- Інтегрований з оболонкою Windows, що дозволяє легко видаляти файли та папки безпосередньо з контекстного меню;
- Швидке видалення файлів.

Недоліки:

- Тільки для Windows;
- Немає можливості стирання даних на цілому диску;
- Відсутність підтримки при виникненні технічних питань.

3) “Secure Eraser” – це безкоштовне програмне забезпечення з можливістю придбання платної версії з розширеним функціоналом та відсутньою рекламою. За допомогою “Secure Eraser” можна безпечно видаляти файли, папки та диски, видаляти вільний простір на диску, очищувати реєстр та систему. Програмне забезпечення підтримує наступні версії Windows: Server 2003, Server 2008, Server 2012, Server 2016, Server 2019, 7, 8, 8.1, 10 і Windows 11 [15].

“Secure Eraser” просте у використанні програмне забезпечення, яке перезаписує дані до 35 разів та має такі методи та стандарти знищення даних:

- Перезапис випадковими значеннями

- US DoD 5220.22-M E
- Німецький VSITR
- US DoD 5220.22-M (8-306./E, C & E)
- Метод Пітера Гутмана

Переваги “Secure Eraser”:

- Простий у використані;
- Інтегрований з оболонкою Windows, що дозволяє легко видаляти файли та папки безпосередньо з контекстного меню;
- Доступна безкоштовна версія;
- Різноманітні стандарти та методи знищення даних.

Недоліки:

- Тільки для Windows;
- Наявність реклами у безкоштовній версії.

4) “PrivaZer” – також безкоштовне програмне забезпечення для безпечного видалення даних з можливістю придбання платної версії з розширеним функціоналом. За допомогою програми “PrivaZer” можна виявляти та видаляти залишкові сліди, що залишились у вільному просторі від старих файлів, безпечно видаляти дані за допомогою методів перезапису, видаляти сліди активності в Інтернеті [14].

“PrivaZer” працює на операційних системах Windows 11, Windows 10, Windows 8, Windows 7, Windows Vista та Windows XP.

“PrivaZer” включає такі методи та стандарти знищення даних для магнітних дисків:

- Перезапис нулями
- Британський HMG IS5 (базова лінія)
- Британський HMG IS5 (розширений)
- USA-AF AFSSI 5020
- Російський ГОСТ Р50739-95
- Німецький VSITR

- NAVSO ВМС США P-5239-26
- US DoD 5220.22-M
- Канадська служба безпеки зв’язку ITSG-06
- NISPOMSUP Chap 8, Sect. 8-501
- NSA Manual 130-2
- IREC (IRIG) 106
- Армія США AR380-19
- Німецький VSITR
- Алгоритм Брюса Шнайєра
- RCMP TSSIT OPS-II
- Метод Пітера Гутмана

Переваги “PrivaZer”:

- Віртуалізація результатів про знайдені залишки та потенційні ризики;
- Наявність портативної версії;
- Доступна безкоштовна версія;
- Різноманітні стандарти та методи знищення даних;
- Видалення слідів активності в Інтернеті та залишкових слідів від файлів.

Недоліки:

- Тільки для Windows;
- Потреба в регулярних оновленнях;
- Може бути досить часозатратним.

5) “Hardwipe” – безкоштовне та просте у використані програмне забезпечення для безпечного видалення файлів, як окремих, так і каталогів та дисків, а також з можливістю очищення вільного простору на диску. “Hardwipe” працює на операційних системах Windows 10, Windows 8.1, Windows 8 та Windows 7 [16].

“Hardwipe” включає такі методи та стандарти знищення даних:

- Перезапис нулями

- Перезапис випадковими значеннями
- Російський ГОСТ Р50739-95
- US DoD 5220.22-M
- RAZER, RAZER+, RAZER++
- Німецький VSITR
- Алгоритм Брюса Шнайєра
- Метод Пітера Гутмана

Переваги “Hardwipe”:

- Простий та зрозумілий інтерфейс;
- Наявність портативної версії;
- Інтегрований з оболонкою Windows, що дозволяє легко видаляти файли та папки безпосередньо з контекстного меню;
- Різноманітні стандарти та методи знищення даних;
- Наявність безкоштовної версії.

Недоліки:

- Тільки для Windows;
- Знищення даних може бути досить часозатратним.

6) “BitKiller” – безкоштовне портативне програмне забезпечення, яке було випущено за ліцензією GNU, для безпечного та надійного знищення даних, як окремих файлів, так і каталогів, використовуючи різноманітні методи перезапису даних, а також заміну імені файлів для того, щоб їх було важче знайти. “BitKiller” працює на операційній системі Windows 2000 та новіших версіях Windows [17].

“BitKiller” включає такі методи та стандарти знищення даних:

- Перезапис даних нулями
- Перезапис даних випадковими даними
- US DoD 5220.22-M (8-306./E)
- US DoD 5220.22-M (8-306./E, C & E)
- Метод Пітера Гутмана

Переваги “BitKiller”:

- Простий у використані;
- Не потребує установлення;
- Швидке видалення даних;
- Різноманітні стандарти та методи знищення даних.

Недоліки:

- Тільки для Windows;
- Обмежені функціональні можливості.

2.2 Аналіз відгуків про програмні забезпечення знищення даних

Узагальнимо відгуки користувачів про програмні засоби, які були наведені раніше, у формі таблиці (Табл. 2.2), яка включає позитивні та негативні відгуки, а також технічні проблеми з якими зіткнулися користувачі [18-30].

Таблиця 2.2 – Узагальнення відгуків про програмні засоби знищення даних

Програмне забезпечення	Позитивні відгуки	Негативні відгуки	Технічні проблеми
1	*2*	*3*	*4*
Eraser	Підтримка різних методів знищення, включаючи DoD 5220-22.M і Gutmann; простота використання; підтримка видалення файлів, вільного простору і цілих дисків; опції для налаштувань задач.	Програма може бути ненадійною, повільною; часті збої та помилки під час роботи; вимога до .NET для установки; відсутність паралельної обробки декількох дисків.	Проблеми з установкою на певних операційних системах; проблеми з видаленням даних на SSD через особливості цих накопичувачів.
File Shredder	Простота у використані; швидке видалення файлів; безпечне видалення файлів; підтримка різних форматів дисків.	Проблеми з установкою.	Помилки при видаленні даних з дисків; відсутність очікуваних функцій; проблеми з підтримкою та оновленнями.

Продовження Таблиці 2.2

1	*2*	*3*	*4*
Secure Eraser	Простота у використані; надійне видалення даних; швидкість роботи програми.	Спливаючі вікна з рекламою; обмежені функції у безкоштовній версії; нав'язування покупки платної версії.	Проблеми з видаленням великої кількості файлів; помилки при роботі на певних ОС.
PrivaZer	Простота інтерфейсу та легкість використання; ефективність очищення; швидка підтримка.	Технічні проблеми з певними функціями; повільність деяких процесів.	Проблеми з використанням дискового простору; проблеми з підтримкою.
Hardwipe	Ефективне стирання даних; простота використання; гнучкість налаштувань.	Неможливість стирання основного диска; проблеми з стиранням посилань (.lnk файлів).	Проблеми з портативною версією.
BitKiller	Простота у використані, швидка установка; можливість вибору методів знищення даних.	Проблеми з швидкодією, обмежені функціональні можливості, відсутність додаткових опцій.	Періодичні збої програми; проблеми зі стабільністю на деяких версіях Windows.

Аналізуючи відгуки користувачів різних програм для безпечного видалення даних, таких як “Eraser”, “File Shredder”, “Secure Eraser”, “PrivaZer” можна побачити, що більшість користувачів цінують їх за простоту використання, тому що інтерфейси цих програм зазвичай інтуїтивно зрозумілі, що дозволяє швидко освоїти їх функціонал, також великий вибір різноманітних методів безпечного видалення даних є ще однією важливою перевагою.

Однак, також є часті технічні проблеми при використанні цих програмних засобів, як, наприклад, помилки при встановленні, нестабільна робота та обмежені можливості в безкоштовних версіях. “Eraser” та “Secure Eraser”, попри їх високу ефективність і налаштовуваність, користувачі часто незадоволені від помилок на певних операційних системах і надмірної кількості спливаючих вікон і реклами.

“File Shredder” швидко виконує свої завдання, але є також проблеми з технічними збоями програмного забезпечння та відсутністю підтримки новіших операційних систем. “PrivaZer” подобається користувачам своєю здатністю до глибокого очищення, проте повільне виконання та технічні проблеми зі слів користувачів є одними з основних недоліків цього програмного забезпечення.

Отже, програмні забезпечення, описані вище, часто обмежені у своїй повній ефективності через технічні недоліки та нестабільність у роботі. Це підкреслює необхідність подальших покращень у стабільності та функціональності від розробників, щоб підвищити загальну якість продуктів.

Висновки за Розділом.

У цьому розділі дипломної роботи було проведено детальний аналіз методів та стандартів знищення даних, а також зроблено короткий огляд програмних засобів знищення даних.

Детальний аналіз методів та стандартів знищення даних показав, що найбільш надійним, але й часозатратним методом є алгоритм Пітера Гутмана, який включає 35 циклів перезапису,а менш часозатратними методами є NAVSO P-5239-26 та US Air Force 5020, хоча вони можуть бути менш ефективними, особливо для сучасних SSD-дисків. Всі алгоритми знищення даних відрізняються кількістю циклів перезапису, що впливає на їх ефективність та тривалість процесу знищення даних.

Були розглянуті різне ПЗ, такі як: “Eraser”, “File Shredder”, “Secure Eraser”, “PrivaZer”, “Hardwipe” та “BitKiller”. Кожне рішення має свої особливості, можливості та обмеження. Основними критеріями вибору ПЗ є підтримка різноманітних стандартів знищення даних, зручність інтерфейсу, швидкість роботи та надійність. Аналіз відгуків користувачів показав, що більшість програмних засобів мають позитивні відгуки щодо зручності використання та ефективності, проте часто стикаються з технічними проблемами, що підкреслює необхідність подальших покращень у стабільності та функціональності цього ПЗ.

3 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВІДНОВЛЕННЯ ДАНИХ

3.1 Методи та засоби відновлення даних

Відновлення даних – це процес отримання інформації, доступ до якої неможливо отримати стандартними способами через попереднє видалення або пошкодження цифрових носіїв [31].

Серед усіх способів відновлення даних можна виділити кілька основних категорій:

- програмне забезпечення відновлення даних;
- апаратні засоби відновлення даних.

Програмне забезпечення відновлення даних включає сканування та відновлення файлів, які були втрачені або видалені [32].

Відновлення даних за допомогою програмних засобів можливе за таких обставин [33]:

- видалені дані не були перезаписані новими даними;
- втрачені дані на SSD-дисках не були видалені командою TRIM;
- для видалення файлів не використовувались програмні засоби безпечного знищення даних;
- носії інформації фізично неушкоджені.

На цей момент існує два основних метода відновлення даних за допомогою програмного забезпечення, які використовуються майже у всіх програмних засобах поодиночно, або в комбінації [34]:

- аналіз метаданих;
- пошук даних по сигнатурам (сканування файлів відомих типів).

Метадані включають інформацію про розміщення даних, їх властивості та інше. Метод аналізу метаданих дозволяє програмі знайти основні структури у сховищі, відтворюючи пошкоджену файлову систему. Цей метод дозволяє повністю відновити структуру втрачених даних, але тільки якщо

метадані не серйозно пошкоджені. В інакшому випадку, метод аналізу метаданих не буде дієвим для відновлення даних [31].

Якщо програмне забезпечення не відновило дані за допомогою методу аналізу метаданих, то тоді може застосовуватись метод пошуку даних по сигнатурам, який базується на пошуку файлів за їх відомим вмістом. У цьому випадку програма шукає послідовності неопрацьованих даних, характерні для файлів певного формату, що допомагає визначити початок або кінець файлу. Файли, відновлені таким чином, отримують нові імена та розширення на основі знайдених сигнатур і розміщуються в окремих папках для різних типів файлів. Основне обмеження цього методу – деякі файли можуть не мати упізнаваних сигнатур або мати сигнатури лише на початку файлу, що ускладнює визначення їх кінця, особливо якщо частини файлу не зберігаються послідовно [31].

Проаналізувавши методи відновлення даних, можна створити порівняльну таблицю (Табл. 3.1) недоліків та переваг обох методів.

Таблиця 3.1 – Порівняльна таблиця методів відновлення даних

Назва методу	**Переваги**	**Недоліки**
Метод аналізу метаданих	Можливе повне відновлення структури втрачених даних; швидкість процесу відновлення; можливе відовлення фрагментованих даних.	Можливе відновлення тільки якщо метадані несерйозно пошкоджені.
Метод пошуку даних по сигнатурам	Можливе відновлення даних, якщо дані були давно видалені та у випадках, коли метадані пошкоджені або відсутні.	Повільність процесу, втрата оригінальної структури, обмежена підтримка форматів.

Сучасні програми для відновлення даних часто застосовують гібридний підхід, прагнучи максимально зчитати інформацію з файлової системи та вдаючись до сигнатурного аналізу лише в крайніх випадках, коли файлова система пошкоджена або відсутня, а також для пошуку файлів, які були видалені давно [34].

Апаратні засоби відновлення даних включають використання спеціалізованого обладнання. За допомогою цього обладнання можна читати та відновлювати дані з ушкоджених носіїв інформації.

Також, в деяких випадках, використовується комбінація апаратних та програмних методів відновлення даних. Це корисно, наприклад, коли жорсткий магнітний диск фізично пошкоджений, але при цьому файлова система не має несправностей.

Розглянемо деякі широко розповсюджені програмні засоби відновлення даних:

1) “Recuva” – безкоштовний програмний засіб для сканування пошкоджених або видалених даних для будь-якого носія інформації (SSD-диски, HDD-диски, флеш-карти та інші), підтримує такі файлові системи, як: NTFS, FAT32, EXT3, EXT4 та exFAT. Також є платна версія з розширеним функціоналом [35].

Переваги:

- простий у використані;
- наявність безкоштовної та портативної версії;
- інтеграція в операційну систему;
- можливість безпечного видалення даних;
- відновлення даних на пошкоджених носіях інформації;
- наявність продвинутого режиму сканування;
- можливість глибокого сканування.

Недоліки:

- тільки для Windows;
- повільна швидкість глибокого сканування;
- відсутня технічна підтримка пробної версії.

2) “Disk Drill” – багатофукціональне програмне забезпечення відновлення втрачених або видалених даних. Працює на операційних системах Windows та macOS, підтримує такі файлові системи, як: FAT,

exFAT, EXT3, EXT4, NTFS, APFS (Apple File System), HFS (Hierarchical File System).

Переваги:

- наявність безкоштовної пробної версії;
- наявність функції захисту даних Recovery Vault;
- можливість відновлення з різних носіїв;
- наявність глибокого сканування;
- можливість створення резервної копії дисків та розділів;
- підтримка різноманітних файлових систем.

Недоліки:

- висока вартість;
- обмеження безкоштовної версії;
- повільна швидкість глибокого сканування;
- програмне забезпечення може вимагати значні ресурси системи.

Проаналізувавши відгуки користувачів про програмне забезпечення, котре було описане вище, можна сформувати таблицю (Табл. 3.2) переваг та недоліків цих програм, а також технічні проблеми, з котрими зіткнулися користувачі [36-40].

Таблиця 3.2 – Узагальнення відгуків про програмні засоби відновлення даних

Програмне забезпечення	**Позитивні відгуки**	**Негативні відгуки**	**Технічні проблеми**
1	2	3	4
Recuva	Легкість використання; безкоштовна версія; попередній перегляд файлів перед відновленням; глибоке сканування; підтримка різних носіїв даних.	Погане відновлення даних; встановлення небажаного програмного забезпечення; не завжди ефективне відновлення файлів; деякі файли можуть бути пошкоджені або неповністю відновлені.	Може встановлювати небажане програмне забезпечення; нестабільність при роботі з великими дисками; тривалий час сканування; проблеми з розпізнаванням певних носіїв.

Продовження Таблиці 3.2

1	2	3	4
Disk Drill	Ефективність відновлення; можливість відновлення даних з різних типів носіїв; легкість використання; швидка та корисна підтримка користувачів; наявність додаткових функцій, як, наприклад, очищення дисків, пошук дублікатів файлів та захист даних.	Програма не змогла відновити файли, або відновила лише пошкоджені чи непридатні файли; оманлива реклама; купівля повної версії не гарантує 100% відновлення файлів; відмови у поверненні коштів та довгий час відповіді від розробників.	Проблеми з роботою на певних операційних системах, особливо на Mac з SSD; збої під час роботи програми, особливо під час глибокого сканування або відновлення великих обсягів даних; програма не завжди правильно попередньо переглядає файли, що ускладнює оцінку їх придатності до відновлення.

Проаналізувавши таблицю, можна зробити висновки, що обидва програмні засоби мають свої переваги та недоліки. “Recuva” підходить для простих завдань, але може бути ненадійною при роботі з великими обсягами даних або складними випадками відновлення, а програмне забезпечення “Disk Drill” пропонує більше функцій і кращу підтримку користувачів, але також має свої недоліки, включаючи технічні проблеми та випадки невдалого відновлення даних. Користувачі обох програм можуть зіткнутися з проблемами на різних операційних системах і носіях, що варто враховувати при виборі відповідного інструменту для відновлення даних.

На діаграмі (Рис. 3.1) представлено полярність відгуків про програмні забезпечення “Recuva” та “Disk Drill” по країнах (США, Великобританія, Індія, Германія, Канада). Для кожної країни показано кількість позитивних та негативних відгуків [36-40].

На основі цих даних видно, що “Disk Drill” має більше позитивних відгуків порівняно з “Recuva” у всіх зазначених країнах.

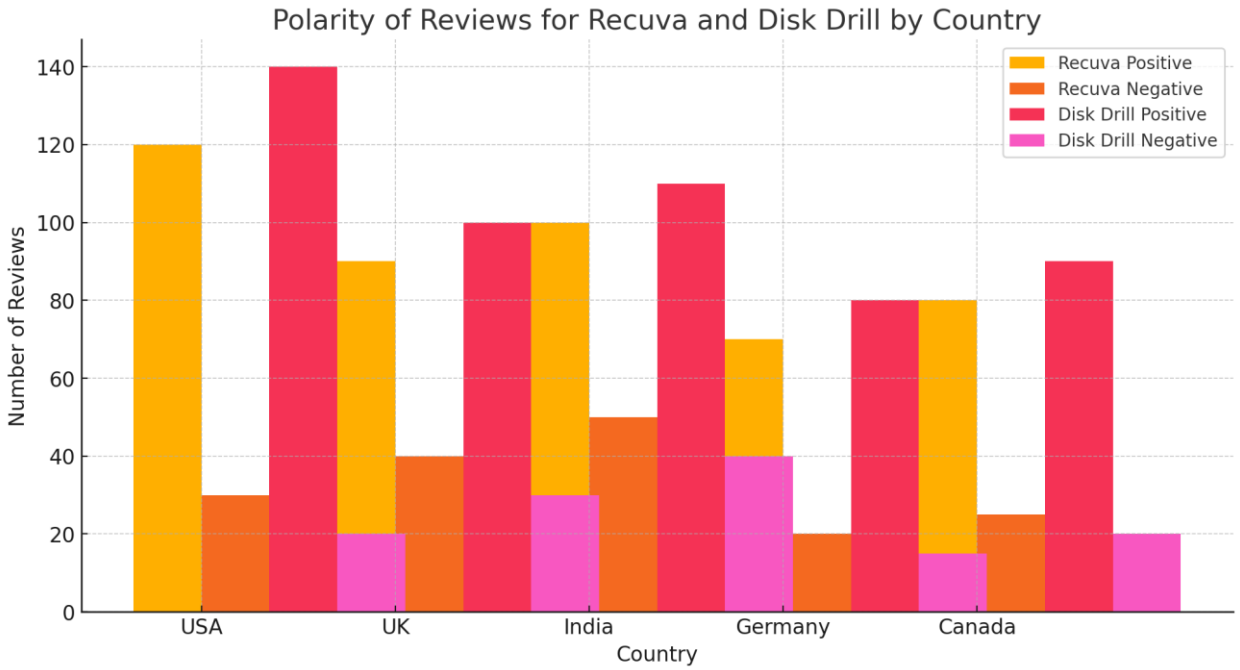

Рис. 3.1 – Популярність програмних забезпечень “Recuva” та “Disk Drill”

Висновки за розділом.

У цьому розділі досліджено методи та засоби відновлення даних, а також програмні засоби для відновлення інформації. Проведено аналіз ефективності різних програмних засобів для відновлення даних.

Розглянуті метод аналізу метаданих та метод пошуку даних по сигнатурам. Виявлено, що метод аналізу метаданих дозволяє повністю відновити структуру втрачених даних за умови, що метадані не були серйозно пошкоджені, а метод пошуку даних по сигнатурам базується на пошуку відомих послідовностей даних і може відновити файли навіть у випадках серйозного пошкодження файлової системи, але він є повільнішим за метод аналізу метаданих і не завжди може відновити початкову структуру файлів (в т.ч. розмітку диску).

Огляд відповідних програмних рішень показав, що ПЗ «Recuva» просте у використанні, має безкоштовну версію та підтримує різні типи носіїв даних, а основні недоліки включають повільність глибокого сканування та встановлення небажаного програмного забезпечення, а ПЗ «Disk Drill» –

ефективна та багатофункціональна програма з підтримкою різних файлових систем, але безкоштовна версія має обмеження.

Було виявлено, що на ефективність відновлення даних впливають тип носія, кількість циклів перезапису (чим більше, тим становиться менша ймовірність відновлення даних), різні алгоритми знищення та відновлення даних мають різну ефективність залежно від типу носія та інших умов.

Аналіз доступної сукупності відгуків інших користувачів показав, що вони в більшій мірі цінують простоту використання та наявність безкоштовних версій описаних програмних забезпечень, але часто стикаються з технічними проблемами та обмеженнями безкоштовних версій.

Враховуючи відгуки стосовно зручності і простоти використання *(тобто юзабіліті від англ. usability)* профільного ПЗ, можна констатувати, що для ефективного відновлення даних слід використовувати комбінований підхід, застосовуючи як метод аналізу метаданих, так і метод пошуку по сигнатурам. Таким чином, вибір програмного забезпечення для відновлення даних повинен базуватися на конкретних потребах, типах носіїв та обставинах (специфіки подій), за яких були втрачені/знищено дані.

4 ТЕСТУВАННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ ПРОЦЕСУ ЗНИЩЕННЯ ДАНИХ

4.1 Вибір інструментів та підготовка до тестування

1) Вибір інструментів для знищення даних.

Для тестування будуть використані наступні програмні засоби для знищення даних:

- Eraser
- File Shredder
- Secure Eraser
- PrivaZer
- Hardwipe
- BitKiller

2) Вибір інструментів для відновлення даних.

Для тестування будуть використані наступні програмні засоби для відновлення даних:

- Recuva
- Disk Drill

3) Підготовка тестових даних.

Для тестування була обрана операційна система Windows 10.

На кожному носії перед кожним тестуванням програмних засобів знищення даних записуються файли різних типів:

- Два текстових документи в форматах «.docx» та «.pdf»
- Два зображення в форматах «.bmp» та «.jpeg»
- Два музичних треків в форматі «.mp3» з бітрейтами у 320 кбіт/с та 128 кбіт/с
- Два відео в форматах «.avi» та «mp4»
- Виконувальний файл у форматі «.exe»

Типи носіїв інформації:

— Жорсткий диск (HDD)

Назва носія: Seagate Barracuda 250 GB

Основні характеристики:

- Модель: ST250DM000
- Ємність: 250 GB
- Інтерфейс: SATA III (Serial ATA)
- Швидкість обертання: 7200 об/хв
- Кеш-пам'ять: 16 МБ
- Форм-фактор: 3.5 дюйма
- Тип файлової системи: NTFS
- Стан носія: Уживаний, без пошкоджень та зношеності

— Твердотільний накопичувач (SSD)

Назва носія: Seagate Barracuda 250 GB

Основні характеристики:

- Модель: SA400S37
- Ємність: 120 GB
- Інтерфейс: SATA III
- Максимальна швидкість читання даних: 550МБ/с
- Максимальна швидкість запису: 350МБ/с
- Форм-фактор: 2.5 дюйма
- Тип файлової системи: NTFS
- Стан носія: Уживаний, без пошкоджень та зношеності

Перед кожним тестуванням нової програми знищення даних, проводиться повне форматування дисків.

4) Налаштування програмних засобів

Налаштування параметрів знищення даних:

- Eraser (Рис. 4.1)

Кількість циклів перезапису: 7

Вибір алгоритму: RCMP TSSIT OPS-II

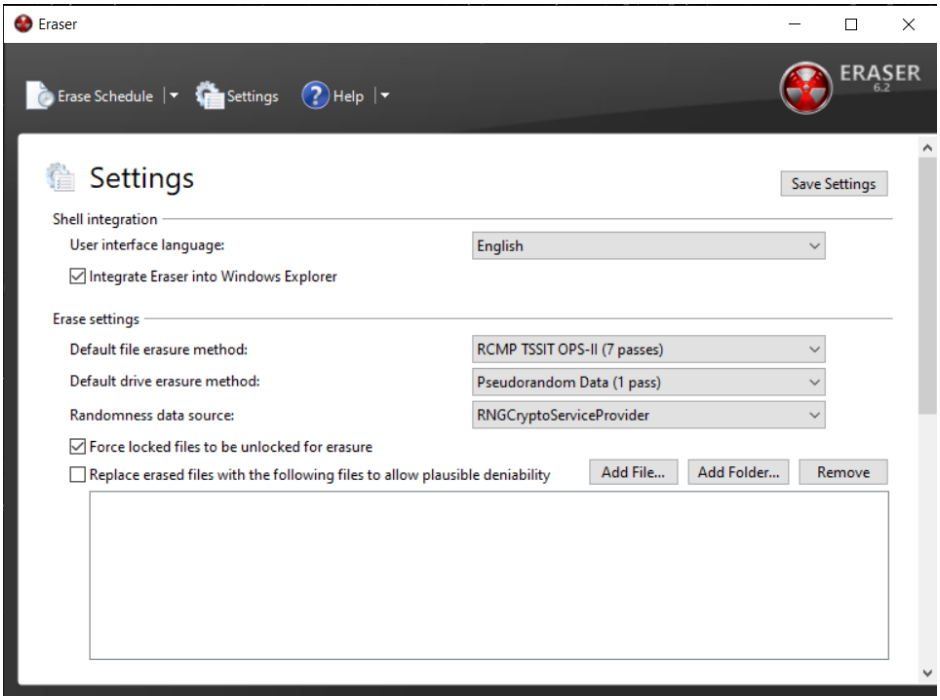

Рисунок 4.1 – Налаштування програмного засобу “Eraser”

- File Shredder (Рис. 4.2)

Кількість циклів перезапису: 35

Вибір алгоритму: Метод Пітера Гутмана

Рисунок 4.2 – Налаштування програмного засобу “ File Shredder”

- Secure Eraser (Рис. 4.3)

Кількість циклів перезапису: 7

Вибір алгоритму: VSITR (Німеччина)

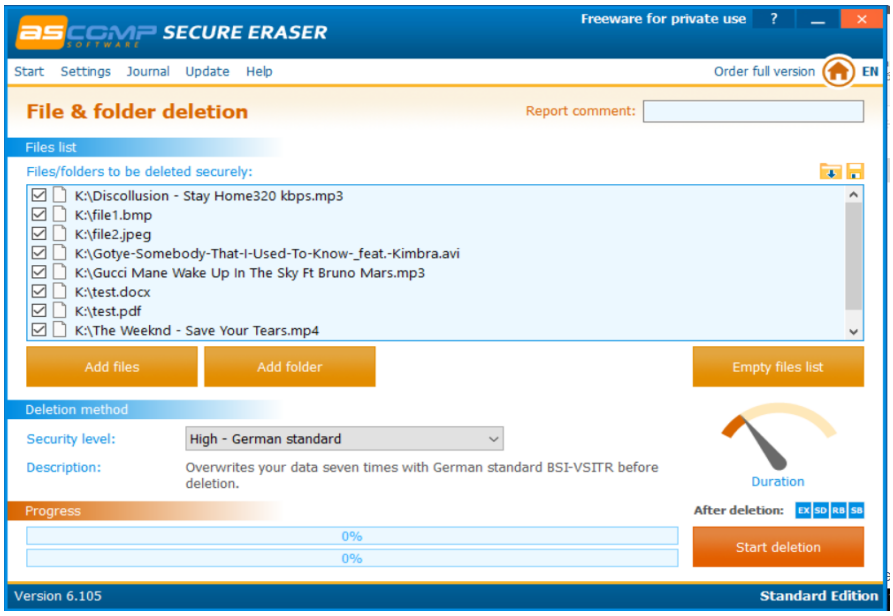

Рисунок 4.3 – Налаштування програмного засобу “ File Shredder”

- PrivaZer (Рис 4.4)

Кількість циклів перезапису: 3

Вибір алгоритму: USA Navy NAVSO

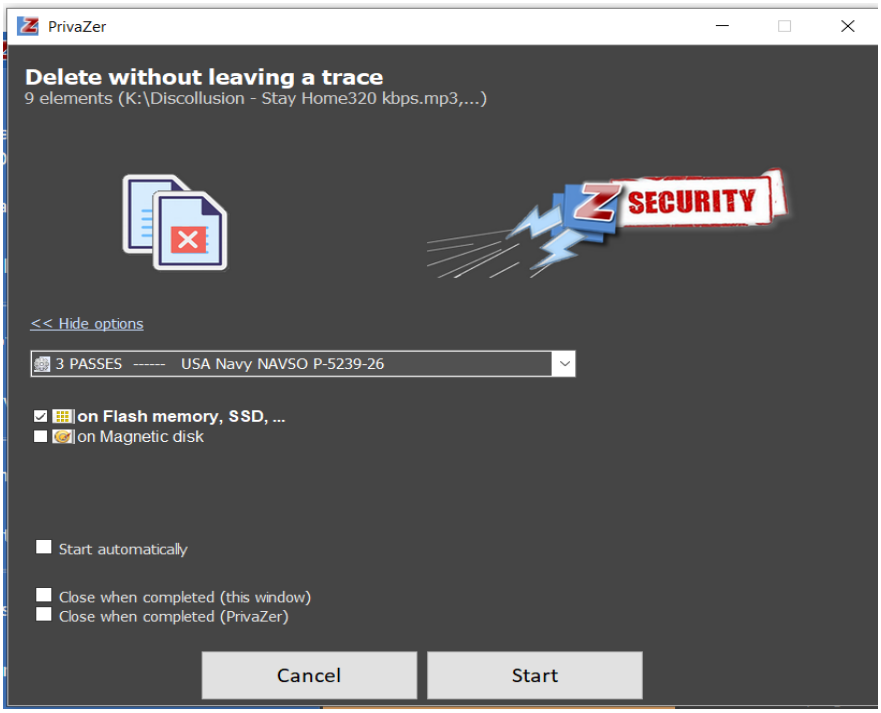

Рисунок 4.4 – Налаштування програмного засобу “ PrivaZer”

- Hardwipe (Рис 4.5)

Кількість циклів перезапису: 7

Вибір алгоритму: Алгоритм Брюса Шнайєра

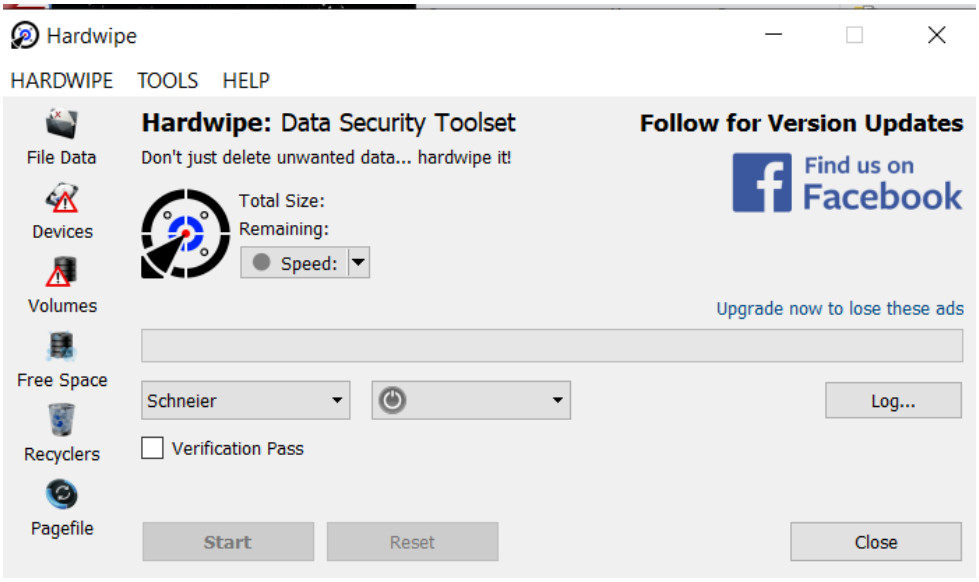

Рисунок 4.5 – Налаштування програмного засобу “ Hardwipe”

- BitKiller (Рис. 4.7)

Кількість циклів перезапису: 7

Вибір алгоритму: US DoD 5220.22-M (8-306./E, C & E)

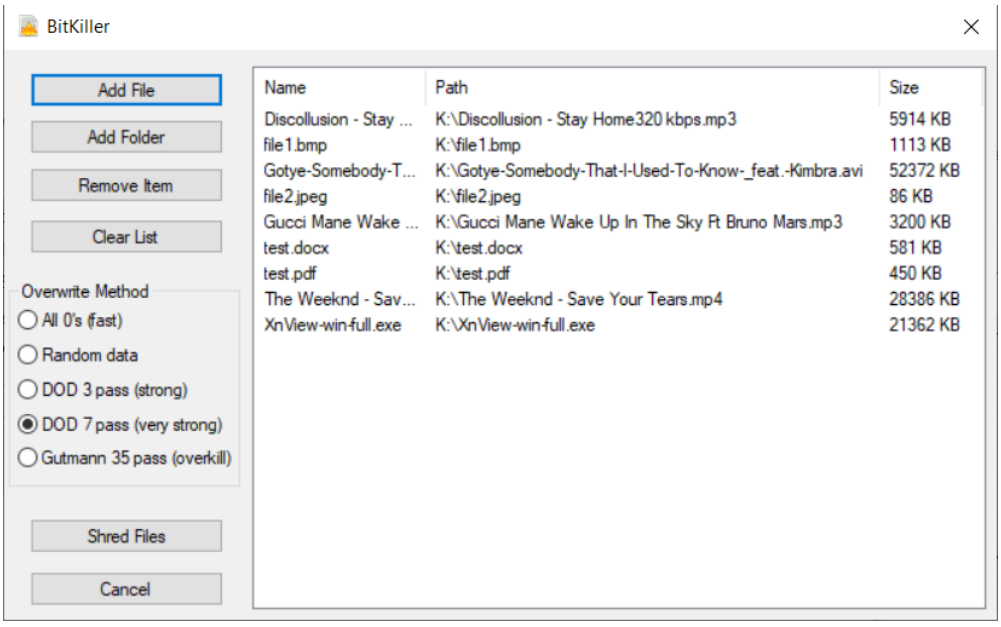

Рисунок 4.6 – Налаштування програмного засобу “BitKiller”

Налаштування параметрів відновлення даних:

Глибоке сканування для максимально ефективного відновлення.

5) Тестовий план

Етапи тестування:

- Повне форматування диску.
- Запис тестового набору даних на диски.
- Знищення даних програмним забезпеченням.
- Відновлення даних після знищення.
- Порівняння результатів для кожного програмного забезпечення та носія.

Критерії оцінки:

- Час, необхідний для знищення даних.
- Час, необхідний для відновлення даних.
- Кількість та якість відновлених файлів.
- Надійність роботи програм.

4.2 Результати тестування програмних засобів знищення даних

На основі проведеного тестування програмних засобів знищення даних, сформуємо таблицю (Табл. 4.1). Процес тестування кожного програмного забезпечення більш детально показано в Додатку Б.

Таблиця 4.1 – Результати тестування програмних засобів знищення даних

Програмний засіб	Носій	Дата і час початку	Дата і час завершення	Загальний час знищення	Повідомлення про помилки
1	2	3	4	5	6
Eraser	SSD	21-05-2024 17:02:32	21-05-2024 17:02:40	8 сек	Відсутні
	HDD	22-05-2024 13:31:05	22-05-2024 13:31:19	14 сек	Відсутні
File Shredder	SSD	21-05-2024 18:49:34	21-05-2024 18:49:51	17 сек	Відсутні
	HDD	22-05-2024 12:13:24	22-05-2024 12:14:22	58 сек	Відсутні

Продовження Таблиці 4.1

1	2	3	4	5	6
Secure Eraser	SSD	22-05-2024 04:40:28	22-05-2024 04:40:40	12 сек	Відсутні
	HDD	22-05-2024 18:07:31	22-05-2024 18:07:40	9 сек	Відсутні
PrivaZer	SSD	22-05-2024 06:15:15	22-05-2024 06:15:21	6 сек	Відсутні
	HDD	23-05-2024 02:03:53	23-05-2024 02:03:58	5 сек	Відсутні
Hardwipe	SSD	22-05-2024 09:05:40	22-05-2024 09:06:38	58 сек	Відсутні
	HDD	22-05-2024 09:05:40	22-05-2024 09:06:30	50 сек	Відсутні
BitKiller	SSD	22-05-2024 10:15:00	22-05-2024 10:15:26	26 сек	Відсутні
	HDD	22-05-2024 10:16:00	22-05-2024 10:16:24	24 сек	Відсутні

4.3 Результати тестування програмних засобів відновлення даних

На основі проведеного тестування програмного забезпечення «Recuva», сформуємо таблицю (Табл. 4.2). Процес тестування відновлення даних більш детально показано в Додатку В.

Таблиця 4.2 – Результати тестування ПЗ «Recuva»

Метод знищення даних	Носій	Глибина сканування	Час виконання сканування	Кількість виявлених файлів	Якість виявлених файлів
1	2	3	4	5	6
RCMP TSSIT OPS-II	SSD	Глибоке сканування	12 хв 40 сек	7	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	34 хв 50 сек	7	Порожні, відновлення не вдалося
Алгоритм Пітера Гутмана	SSD	Глибоке сканування	13 хв 54 сек	7	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	42 хв 50 сек	7	Порожні, відновлення не вдалося
VSITR (Німеччина)	SSD	Глибоке сканування	21 хв 32 сек	0	Відновлення не вдалося
	HDD	Глибоке сканування	51 хв 57 сек	0	Відновлення не вдалося

Продовження Таблиці 4.2

1	2	3	4	5	6
Американський стандарт NAVSO P-5239-26	SSD	Глибоке сканування	14 хв 55 сек	0	Відновлення не вдалося
	HDD	Глибоке сканування	44 хв 12 сек	0	Відновлення не вдалося
Алгоритм Брюса Шнайєра	SSD	Глибоке сканування	12 хв 9 сек	7	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	41 хв 9 сек	8	Порожні, відновлення не вдалося
US DoD 5220.22-M (8-306./E, C & E)	SSD	Глибоке сканування	14 хв	7	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	17 хв 41 сек	8	Порожні, відновлення не вдалося

На основі проведеного тестування програмного забезпечення «Disk Drill», сформуємо таблицю (Табл. 4.3). Процес тестування відновлення даних детально показано в Додатку Г.

Таблиця 4.3 – Результати тестування ПЗ «Disk Drill»

Метод знищення даних	Носій	Глибина сканування	Час виконання сканування	Кількість виявлених файлів	Якість виявлених файлів
1	2	3	4	5	6
RCMP TSSIT OPS-II	SSD	Глибоке сканування	14 хв	12	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	44 хв	24	Порожні, відновлення не вдалося
Алгоритм Пітера Гутмана	SSD	Глибоке сканування	7 хв	22	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	35 хв	24	Порожні, відновлення не вдалося
VSITR (Німеччина)	SSD	Глибоке сканування	8 хв	42	Вдалося відновити метадані, але файли пошкоджені
	HDD	Глибоке сканування	36 хв	21	Вдалося відновити метадані, але файли пошкоджені

Продовження Таблиці 4.3

1	2	3	4	5	6
Американський стандарт NAVSO P-5239-26	SSD	Глибоке сканування	7 хв	24	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	45 хв 23 сек	24	Порожні, відновлення не вдалося
Алгоритм Брюса Шнайєра	SSD	Глибоке сканування	13 хв	24	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	36 хв	12	Порожні, відновлення не вдалося
US DoD 5220.22-M (8-306./E, C & E)	SSD	Глибоке сканування	9 хв	24	Порожні, відновлення не вдалося
	HDD	Глибоке сканування	36 хв	28	Порожні, відновлення не вдалося

4.4 Аналіз результатів тестування

Метою проведеного тестування було визначення ефективності різних програмних засобів для знищення даних та їх здатності запобігати відновленню даних за допомогою популярних інструментів відновлення, таких як “Recuva” та “Disk Drill”. Тестування включало використання різних методів знищення даних на двох типах носіїв інформації: SSD та HDD. Основні параметри оцінки включали час знищення, наявність повідомлень про помилки, кількість виявлених файлів та якість відновлених файлів.

Всі досліджені програмні засоби для знищення даних показали високий рівень ефективності на обох типах носіїв, тому що жоден з методів не залишив відновлюваних файлів, що підтверджується результатами сканування за допомогою “Recuva” та “Disk Drill”. Час знищення даних був різним для кожного програмного засобу. Наприклад, “Eraser” і “PrivaZer” демонстрували найшвидший час знищення, тоді як “Hardwipe” потребував помітно більше часу.

По результатам моделювання можна стверджувати, що попри використання глибокого сканування і складних алгоритмів відновлення, “Recuva” та “Disk Drill” не змогли відновити жодного повного файлу після їх видалення тестовим ПЗ. Єдиним виключення було часткове відновлення метаданих за допомогою “Disk Drill”, що вказує лише на можливість відновлення деякої службової інформації.

Узагальнюючи результати тестувань варто відмітити, що суттєвої різниці в результатах між між SSD та HDD не визначено, що свідчить про надійність сучасних програмних засобів для знищення даних.

В цілому, для забезпечення високих рівнів безпеки при виконанні процедур утилізації накопичувачів та/чи видалення потрібної інформації, слід використовувати перевірені програмні засоби, що підтвердили високу ефективність, стосовно результатів видалення даних та, водночас, всіляко враховувати можливість забезпечення конценсусу процесу видалення за критерієм «час виконання – залучаємі ресурси». В деяких випадках, час гарантованого знищення даних певними методами (комбінацією алгоритмів) може бути занадто надмірним, тому слід обирати іншу модель (спосіб) утилізації даних, виходячи з реальних умов експлуатації інформаційної системи чи її окремих апаратних засобів.

Висновки за Розділом.

У четвертому розділі роботи проведено тестування кількох зразків спеціалізованого ПЗ для знищення і відновлення даних, а також зроблено узагальнення стосовно особливостей застосування й властивостей інтерфейсу користувача для різних варіантів відповідного ПЗ.

Аналіз результатів тестування програмних засобів знищення даних показало, що усі протестовані програмні забезпечення показали високий рівень ефективності у знищенні даних як на SSD, так і на HDD носіях. Жоден з методів знищення даних не залишив неушкоджених файлів, що підтверджується результатами сканування за допомогою “Recuva” та “Disk Drill”, а час, необхідний для знищення даних, варіювався між різними

програмами. На дослідному комплекті даних, найшвидші результати продемонстрували “Eraser” та “PrivaZer” (5-14 сек), тоді як Hardwipe потребував більше часу (до 58 сек), але незважаючи на різницю в часі, усі програми були однаково ефективними у знищенні даних.

Аналіз результатів тестування програм відновлення даних показало, що попри використання глибокого сканування, “Recuva” та “Disk Drill” не змогли відновити жодного повного файлу після їх знищення, а єдиним виключення було часткове відновлення метаданих за допомогою “Disk Drill” (після використання VSITR), що вказує на потенційну можливість відновлення деякої службової інформації, але не самих даних.

В цілому, за результатами тестового моделювання не було виявлено суттєвої різниці в ефективності знищення даних між SSD та HDD носіями. Для забезпечення конфіденційності та безпеки даних слід використовувати перевірені програмні засоби для знищення інформації, які продемонстрували високу ефективність у проведеному тестуванні. В цьому сенсі слід звернути увагу на такі рішення, як “Eraser” та “PrivaZer”, які поєднують високу швидкість знищення з ефективністю.

ВИСНОВКИ

В роботі досліджено існуючі технології і способи знищення даних, що зберігаються на різних типах носіїв інформації та проведено тестові випробування для найбільш характерних зразків відповідного ПЗ. За результатами дослідних тестувань проведено аналіз властивостей спеціалізованих програмних рішень для видалення даних та надано рекомендації, щодо їх використання і можливостей.

Проведений аналіз існуючих файлових систем свідчить про те, що принципи їх побудови, в значній мірі є основою для організації та збереження даних на різних типах носіїв інформації, де вони визначають структуру даних, способи доступу до них та механізми управління цими даними. Звернено увагу, на той факт, що коректна організація і розмітка (тобто, логічний поділ) наявного дискового простору на різних типах носіїв, є критично важливими для ефективного управління даними та їх безпеки (адміністрування доступу, потокового шифрування, кластерной стеганографії тощо).

Проведений аналіз національних і міжнародних стандартів в частині, що стосуються регламентації порядку видалення/знищення даних, свідчить про те, що вони встановлюють достатньо чіткі вимоги, стосовно утилізації даних на різних типах носіїв, а їх дотримання є необхідним для забезпечення конфіденційності та безпеки інформації.

В ході виконання роботи досліджено основні особливості, що притаманні для найбільш поширених методів знищення даних на HDD та SSD накопичувачах, включаючи механічне знищення, багатократне перезаписування даних та ін. Встановлено, що кожен з методів має свої переваги і недоліки, а вибір конкретного алгоритму залежить від цілей та можливостей користувача, та специфіки використання носіїв інформації.

В межах виконання теоретичної частини завдань, проаналізовано основні міжнародні стандарти знищення даних, такі як метод Пітера Гутмана, RCMP TSSIT OPS-II, алгоритм Брюса Шнайєра та інші. Акцентовано увагу на тому, що найбільш ефективним, але, й водночас, ресурсоємним і часозатратним є метод Пітера Гутмана, тоді як інші методи при певних налаштуваннях, можуть бути більш швидшими, але й менш надійними (з точки зору можливостей реновації даних спеціалізованим ПЗ).

Результати проведених тестових досліджень декількох показових спеціалізованих програмних рішень для знищення даних, дозволяють стверджувати, що кожне таке рішення має свої особливості, можливості й обмеження та забезпечують підтримку різних комбінацій алгоритмів (стандартів) видалення даних. Узагальнення результатів власного тестування та відгуків інших (*зовнішних*) користувачів свідчить про те, що більшість відповідного ПЗ, залишає позитивне враження щодо легкості їх використання та ефективності, проте існують і певні технічни проблеми, що зумовлені функціональною обмеженістю *(наприклад, відсутністю можливостей складання власних шаблонів/масок обробки і неможливістю врахування ресурсних обмежень для використовуваних платформ/засобів та ін.)* та складнощами в питаннях сумісності з різними типами операційних системам (кросплатформність) й апаратними платформами *(в т.ч. мобільними гаджетами)*.

Дослідження процесу відновлення даних показало, що воно можливе за допомогою відповідних програмних та апаратних засобів. При цьому, в переважній більшості ПЗ, основними методами відновлення даних є аналіз метаданих та пошук даних по їх сигнатурам. ПЗ для відновлення даних, зазвичай, використовує різні комбінації вказаних методів, проте це помітно впливає на час виконуваних процедур та не надає однозначного фактажу щодо очікуваного результату цільового процесу *(тобто, присутня значна невизначеність у результатах відновлення даних)*.

В межах проведених циклів тестування по знищенню та відновленню даних різного типу (форматів представлення та обсягів) встановлено, що використовувани алгоритми знищення даних є достатньо ефективними та відновлення інформації, після їх застосування часто неможливе.

При використанні програмних засобів видалення інформації для забезпечення максимального рівня безпеки, можна рекомендувати поетапне комбінування різних методів/алгоритмів перезапису дпаних. Поетапна обробка носіїв та руйнування їх файлової системи, включаючи фінішну «обробку» завантажувального сектора накопичувача, дозволяє досягнути досить хороших результатів, проте потребує певного часу. В цілому, для запобігання несанкціонованого витоку та/чи інсайду конфіденційної інформації з використовуваних накопичувачів, важливо дотримуватись вимог національних й міжнародних стандартів з питань знищення даних, та регулярно оновлювати відповідне спеціалізоване ПЗ. При цьому, процедури утилізації накопичувачів корпоративних даних і знищення «чутливої» інформації в ході виконання основних бізнес-процедур, повинні носити плановий (регулярний) характер та бути чітко регламентовани діючою версією корпоративниї політики інформаційної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tanenbaum, A. S., & Woodhull, A. S. (2014). Operating systems: Design and implementation. Pearson Education India. (дата звернення: 05.04.2024)
2. Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating system concepts. John Wiley & Sons (дата звернення: 20.03.2024)
3. Stallings, W. (2014). Operating systems: Internals and design principles. Pearson Education (дата звернення: 20.03.2024)
4. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements (дата звернення: 21.03.2024)
5. ДСТУ ISO/IEC 27001:2014 "Інформаційні технології. Методи та засоби забезпечення безпеки інформації. Системи управління інформаційною безпекою. Вимоги" (дата звернення: 13.04.2024)
6. NIST Special Publication 800-88 Rev. 1 "Guidelines for Media Sanitization" (дата звернення: 18.04.2024)
7. Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. Proceedings of the Sixth USENIX Security Symposium, 77-88 (дата звернення: 19.04.2024)
8. SANS Security Essentials - Cleaning Data Storage Media. | SANS Institute [Елекронний ресурс] // SANS Institute – Режим доступу: https://www.sans.org/cyber-security-courses/advanced-security-essentials-enterprise-defender/ (дата звернення: 21.04.2024)
9. Schneier, B. (1996). Applied cryptography: protocols, algorithms, and source code in C. Wiley (дата звернення: 26.04.2024)
10. Сапожнік Т. Метод гарантованого знищення даних. [Елекронний ресурс] // В. Кінзерявий, Т. Сапожнік // Актуальні питання забезпечення кібербезпеки та захисту інформації – 2018. – С. 46-51. (дата звернення: 27.04.2024)

11. Why use eraser? | Eraser [Електронний ресурс] // Eraser. – Режим доступу: https://eraser.heidi.ie/ (дата звернення: 27.04.2024)
12. Eraser, the Open Source File Deletion Power Tool | Blokt [Електронний ресурс] // Blokt. – Режим доступу: https://blokt.com/guides/eraser-the-open-source-file-deletion-power-tool (дата звернення: 27.04.2024)
13. File Shredder is free desktop application for shredding (destroying) unwanted files beyond recovery | File Shredder [Електронний ресурс] // File Shredder. – Режим доступу: https://www.fileshredder.org/index.php (дата звернення: 29.04.2024)
14. Free PC cleaner & Privacy tool | PrivaZer [Електронний ресурс] // PrivaZer. – Режим доступу: https://privazer.com/en/index.php (дата звернення: 01.05.2024)
15. Secure Eraser: Secure Data Deletion and Destruction | Ascompsoftware [Електронний ресурс] // Ascompsoftware. – Режим доступу: https://www.ascompsoftware.com/en/products/secureeraser/tab/description (дата звернення: 03.05.2024)
16. Want to Wipe Hard Drive completely? | Wipedisk [Електронний ресурс] // Wipedisk. – Режим доступу: https://www.wipedisk.net/ (дата звернення: 04.05.2024)
17. BitKiller | Source Forge [Електронний ресурс] // Source Forge. – Режим доступу: https://sourceforge.net/projects/bitkiller/ (дата звернення: 04.05.2024)
18. BitKiller | Softpedia [Електронний ресурс] // Softpedia. – Режим доступу: https://www.softpedia.com/get/Security/Secure-cleaning/BitKiller.shtml (дата звернення: 04.05.2024)
19. BitKiller 2.0 | Download Crew [Електронний ресурс] // Download Crew. – Режим доступу: https://www.downloadcrew.com/article/31606/bitkiller (дата звернення: 04.05.2024)
20. PrivaZer User Reviews | Snap Files [Електронний ресурс] // Snap Files. – Режим доступу:

https://www.snapfiles.com/userreviews/113154/privazer.html (дата звернення: 04.05.2024)

21. PrivaZer | Trust Pilot [Електронний ресурс] // Trust Pilot. – Режим доступу: https://ie.trustpilot.com/review/privazer.com?page=2 (дата звернення: 04.05.2024)
22. Review: Eraser removes files safely and permanently | Pcworld [Електронний ресурс] // Pcworld. – Режим доступу: https://www.pcworld.com/article/456337/review-eraser-removes-files-safely-and-permanently.html (дата звернення: 04.05.2024)
23. Is Eraser secure and efficient? | Security Stack Exchange [Електронний ресурс] // Security Stack Exchange. – Режим доступу: https://security.stackexchange.com/questions/241894/is-eraser-secure-and-efficient (дата звернення: 04.05.2024)
24. Eraser Reviews | Sourceforge [Електронний ресурс] // Sourceforge. – Режим доступу: https://sourceforge.net/projects/eraser/reviews/ (дата звернення: 04.05.2024)
25. File Shredder for Windows | Download.cnet [Електронний ресурс] // Download.cnet. – Режим доступу: https://download.cnet.com/file-shredder/3000-2144_4-10662831.html (дата звернення: 06.05.2024)
26. File Shredder User Reviews | Snapfiles [Електронний ресурс] // Snapfiles. – Режим доступу: https://www.snapfiles.com/userreviews/110746/fileshredder2.html (дата звернення: 06.05.2024)
27. BitKiller | Findmysoft [Електронний ресурс] // Findmysoft. – Режим доступу: https://bitkiller.findmysoft.com/ (дата звернення: 06.05.2024)
28. Hardwipe for Windows | Download.cnet [Електронний ресурс] // Download.cnet. Режим доступу: https://download.cnet.com/hardwipe/3000-2248_4-75532060.html (дата звернення: 06.05.2024)
29. Hardwipe User Reviews | Snapfiles [Електронний ресурс] // Snapfiles. – Режим доступу:

https://www.snapfiles.com/userreviews/112884/hardwipe.html (дата звернення: 06.05.2024)

30. Hardwipe | Hardwipe [Електронний ресурс] // Hardwipe. – Режим доступу: https://hardwipe.en.lo4d.com/windows (дата звернення: 06.05.2024)
31. Що таке відновлення даних? | Ufsexplorer [Електронний ресурс] // Ufsexplorer. – Режим доступу: https://www.ufsexplorer.com/uk/articles/what-is-data-recovery/ (дата звернення: 13.05.2024)
32. Восстановление данных с устройств хранения информации? | Pomogator [Електронний ресурс] // Pomogator. – Режим доступу: https://pomogator.com.ua/vosstanovlenie-dannyx/ (дата звернення: 13.05.2024)
33. Основи відновлення даних | Raisedr [Електронний ресурс] // Raisedr. – Режим доступу: https://www.raisedr.com/uk/resources/general/data-recovery-basics/
34. Коваленко Е. ПРИНЦИПЫ ВОССТАНОВЛЕНИЯ ПОТЕРЯННЫХ ДАННЫХ | Е.А. Коваленко, А.Б. Лачихіна [Електронний ресурс] // Е.А. Коваленко, А.Б. Лачихіна. – Режим доступу: https://nto-journal.ru/catalog/informacionnye-texnologii/284/ (дата звернення: 15.05.2024)
35. Recuva — бесплатная программа для восстановления удаленных файлов | Recuva [Електронний ресурс] // Recuva. – Режим доступу: https://recuva.su/ (дата звернення: 15.05.2024)
36. Recuva for Windows | Download.cnet [Електронний ресурс] // Download.cnet. – Режим доступу: https://download.cnet.com/recuva/3000-2242_4-10753287.html (дата звернення: 15.05.2024)
37. User comments for Recuva | Softonic [Електронний ресурс] // Softonic. – Режим доступу: https://recuva.en.softonic.com/comments (дата звернення: 18.05.2024)

38. Recuva | Mouthshut [Електронний ресурс] // Mouthshut. – Режим доступу: https://www.mouthshut.com/software/Recuva-reviews-925840394#dvreview-listing (дата звернення: 19.05.2024)
39. Diskdrill | Trustpilot [Електронний ресурс] // Trustpilot. – Режим доступу: https://www.trustpilot.com/review/diskdrill.com (дата звернення: 20.05.2024)
40. Disk Drill for Windows | Cnet [Електронний ресурс] // Cnet. – Режим доступу: https://download.cnet.com/disk-drill/3000-2248_4-76277044.html (дата звернення: 20.05.2024)

ДОДАТОК А

Методи та стандарти знищення даних

Британський HMG IS5 (розширений) – алгоритм знищення даних, розроблений у Великобританії, який включає 3 цикли перезапису даних нулями, одиницями та випадковими символами, також включає перевірку.

US Air Force 5020 – алгоритм знищення даних, розроблений ВПС США, включає 3 цикли перезапису даних нулями, одиницями та псевдовипадковими значеннями.

Армія США AR380-19 – метод перезапису даних випадковими символами, розроблений армією США, включає 3 цикли.

Російський ГОСТ Р50739-95 – 2 цикли перезапису даних нулями та випадковими значеннями, стандарт був визначений Росією.

Британський HMG IS5 (базова лінія) – метод перезапису даних нулями, включає один цикл.

RAZER, RAZER+, RAZER++ — власні алгоритми програмного забезпечення Hardwipe.

USA-AF AFSSI 5020 — включає один цикл перезапису даних випадковими значеннями та один цикл для перевірки, використовується Повітряними силами США.

Канадська служба безпеки зв’язку ITSG-06 — включає 3 цикли перезапису даних за допомогою специфічних та випадкових шаблонів.

NISPOMSUP Chap 8, Sect. 8-501 — включає 3 цикли з перезаписом даних випадковими та специфічними шаблонами.

NSA Manual 130-2 — включає більш складну послідовність перезаписів для забезпечення кращого знищення даних.

IREC (IRIG) 106 — включає перезапис даних за допомогою послідовних перезаписів зі змінними шаблонами, застосовується у військовій аерокосмічній сфері.

ДОДАТОК Б

Тестування програмних засобів знищення даних

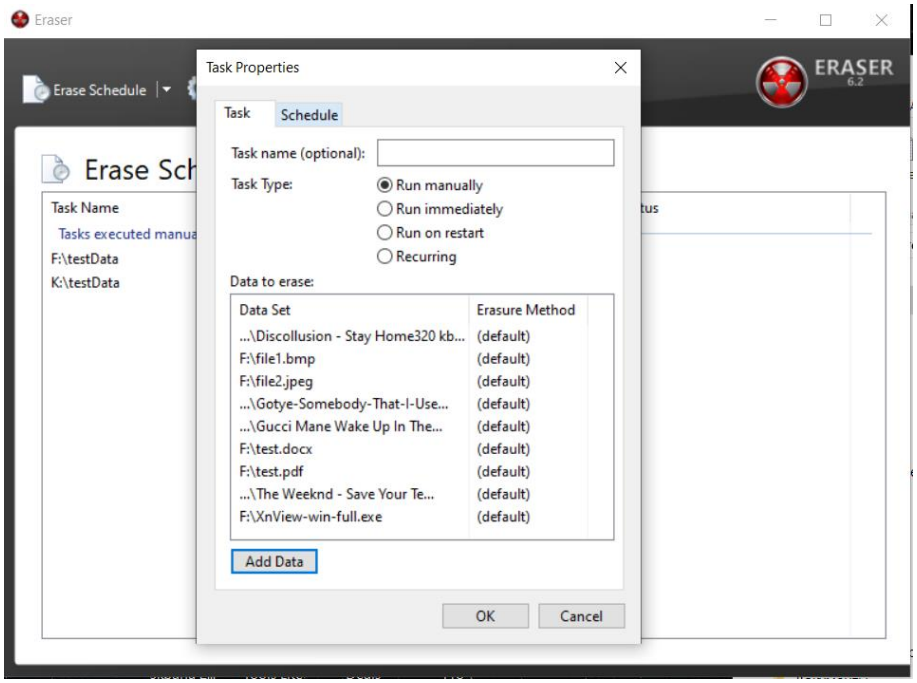

Рисунок Б.1 – Додавання файлів для знищення з HDD-диску за допомогою програми “Eraser”

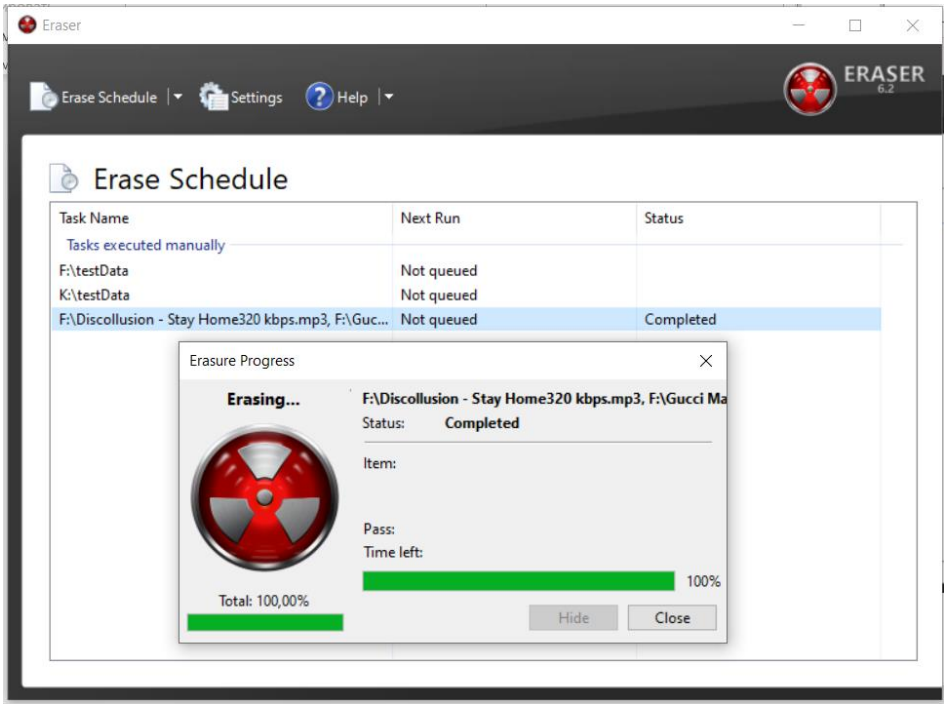

Рисунок Б.2 – Завершення знищення файлів з HDD-диску за допомогою програми “Eraser”

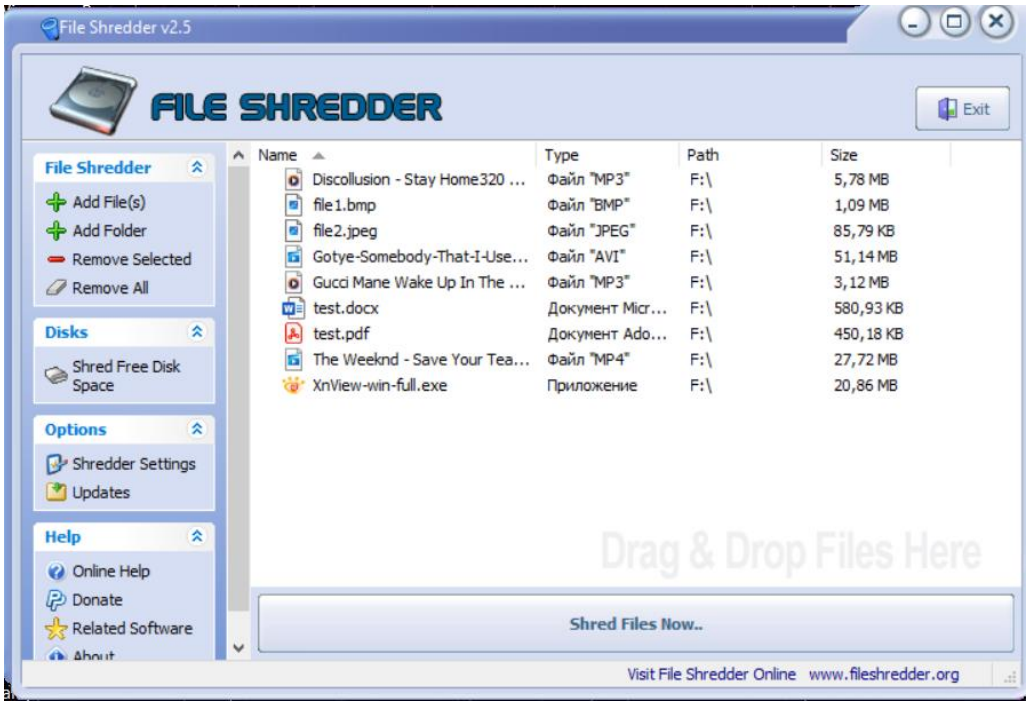

Рисунок Б.3 – Додавання файлів для знищення з HDD-диску за допомогою програми “File Shredder”

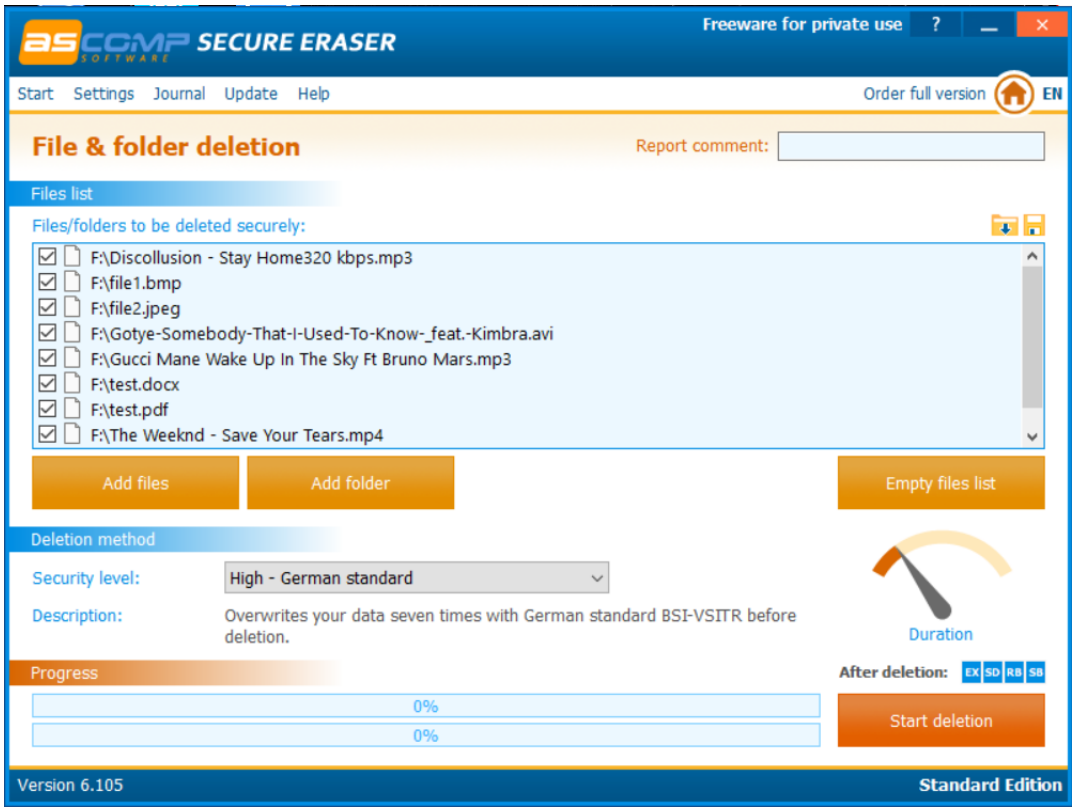

Рисунок Б.4 – Додавання файлів для знищення з HDD-диску за допомогою програми “Secure Eraser”

Secure Eraser

General information

Program version	**6.105**
Computer	**DESKTOP-BT07V55**
User	**Наталія**
Deletion type	**File & folder deletion**
Deletion method	**High - German standard**
Comment	
Started	**22.05.2024 18:07:29**
Finished	**22.05.2024 18:07:40**
State	**completed**
Errors	**0**

Occurred errors (0)

Type	Description	Time

Successfully deleted (9)

Object	Action	Time
F:\XnView-win-full.exe	deleted [High - German standard]	22.05.2024 18:07:31
F:\The Weeknd - Save Your Tears.mp4	deleted [High - German standard]	22.05.2024 18:07:33
F:\test.pdf	deleted [High - German standard]	22.05.2024 18:07:33
F:\test.docx	deleted [High - German standard]	22.05.2024 18:07:34
F:\Gucci Mane Wake Up In The Sky Ft Bruno Mars.mp3	deleted [High - German standard]	22.05.2024 18:07:34
F:\Gotye-Somebody-That-I-Used-To-Know-_feat.-Kimbra.avi	deleted [High - German standard]	22.05.2024 18:07:38
F:\file2.jpeg	deleted [High - German standard]	22.05.2024 18:07:39
F:\file1.bmp	deleted [High - German standard]	22.05.2024 18:07:39
F:\Discollusion - Stay Home320 kbps.mp3	deleted [High - German standard]	22.05.2024 18:07:40

Рисунок Б.5 – Деталі безпечного видалення даних з HDD-диску за допомогою програми “Secure Eraser”

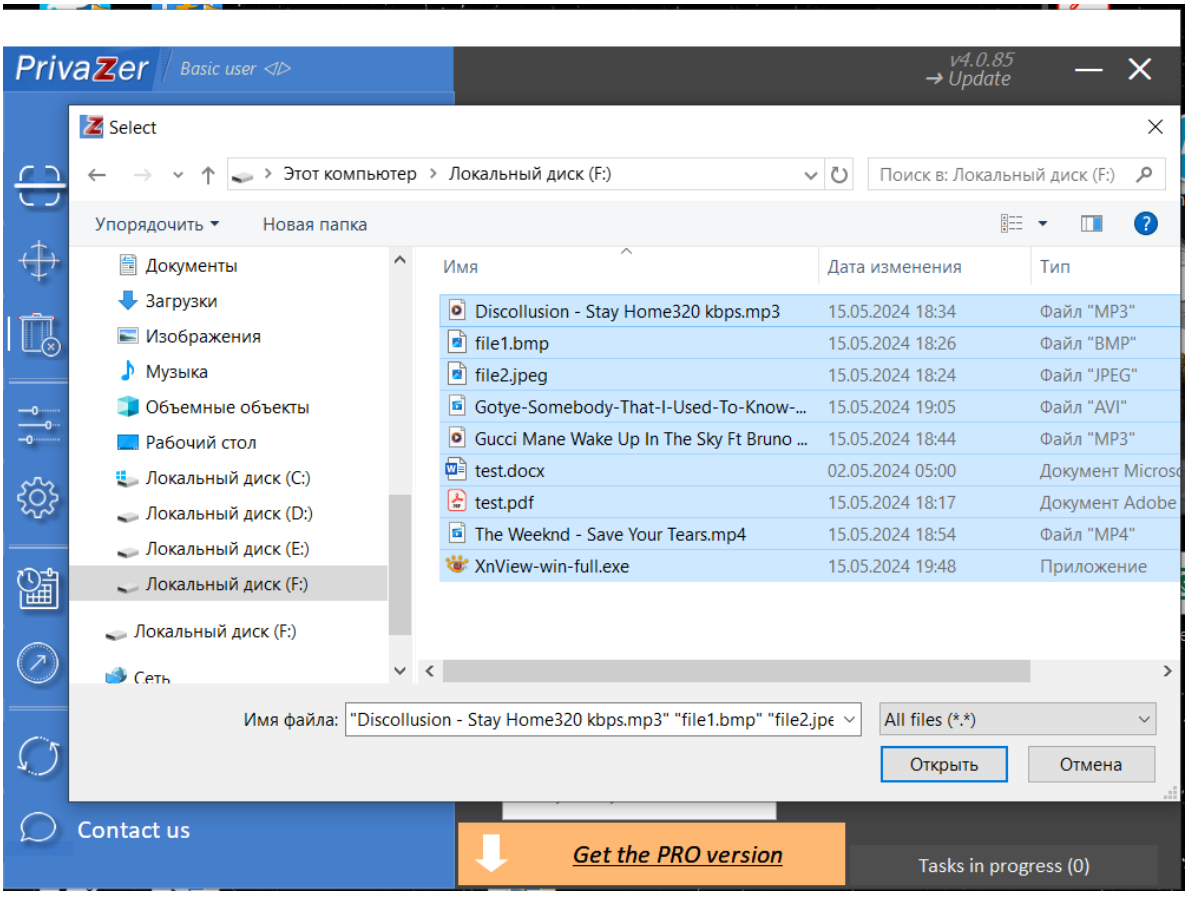

Рисунок Б.6– Додавання файлів для знищення з HDD-диску за допомогою програми “PrivaZer”

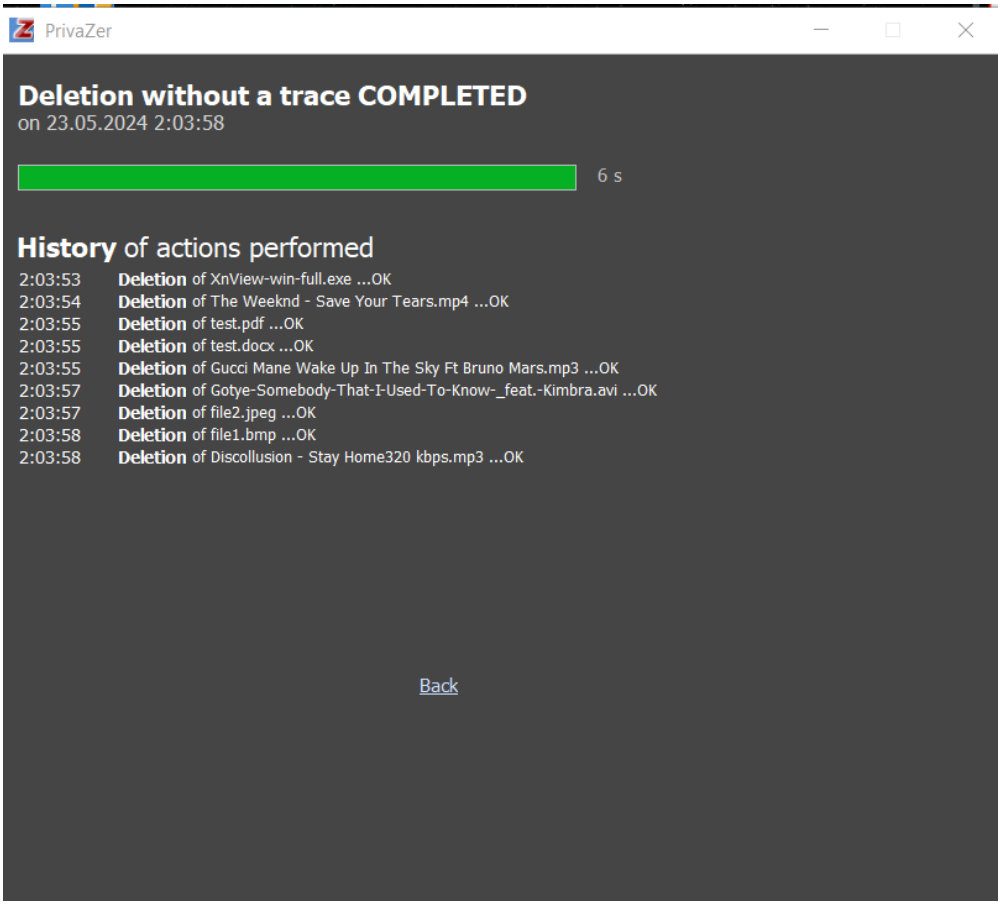

Рисунок Б.7 – Деталі безпечного видалення даних з HDD-диску за допомогою програми “PrivaZer”

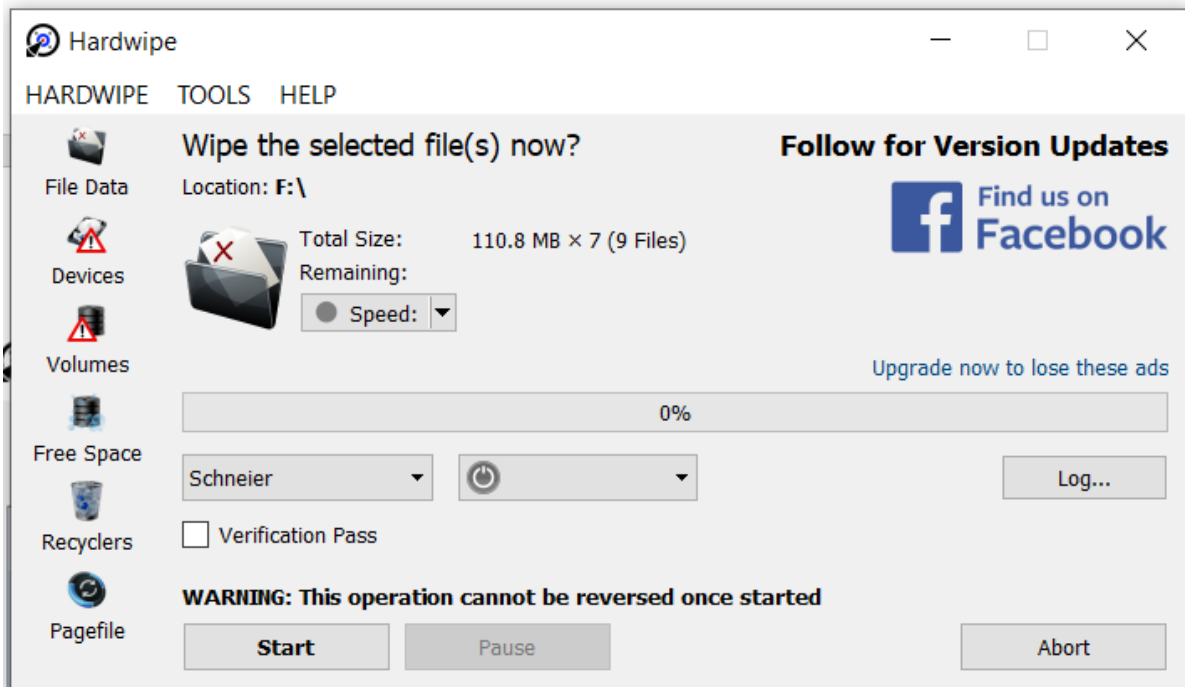

Рисунок Б.8 – Додавання файлів для знищення з HDD-диску за допомогою програми “Hardwipe”

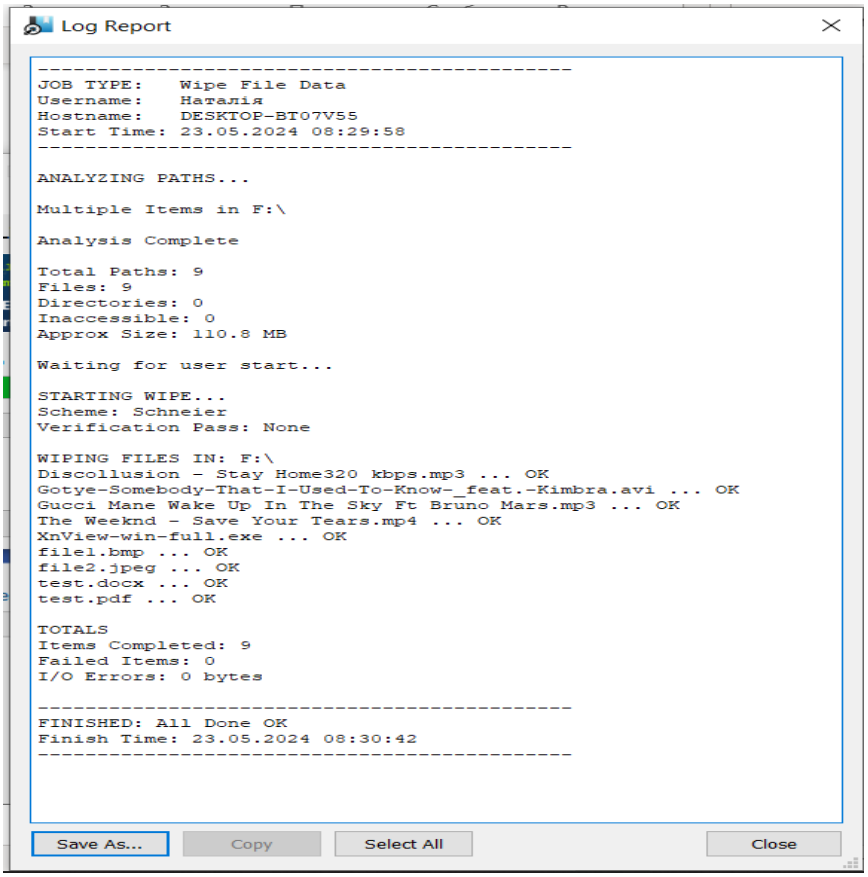

Рисунок. Б.9 – Деталі знищення даних з HDD-диску за допомогою програми “Hardwipe”

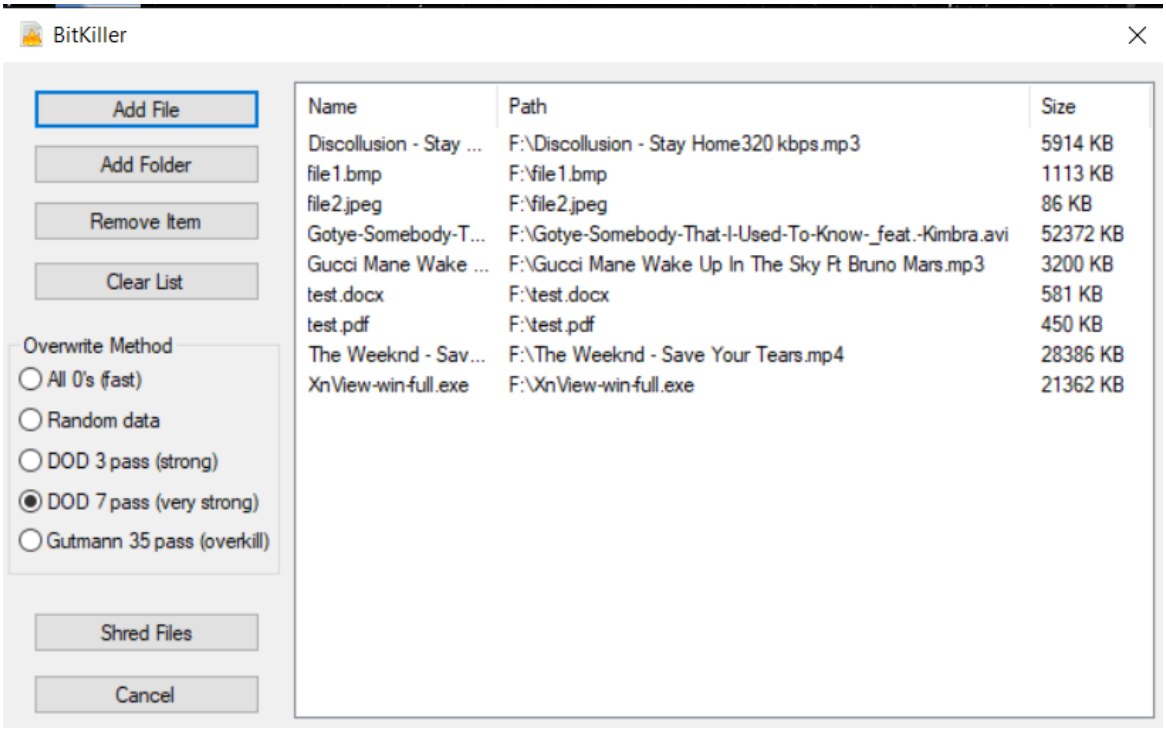

Рисунок Б.10 – Додавання файлів для знищення з HDD-диску за допомогою програми “BitKiller”

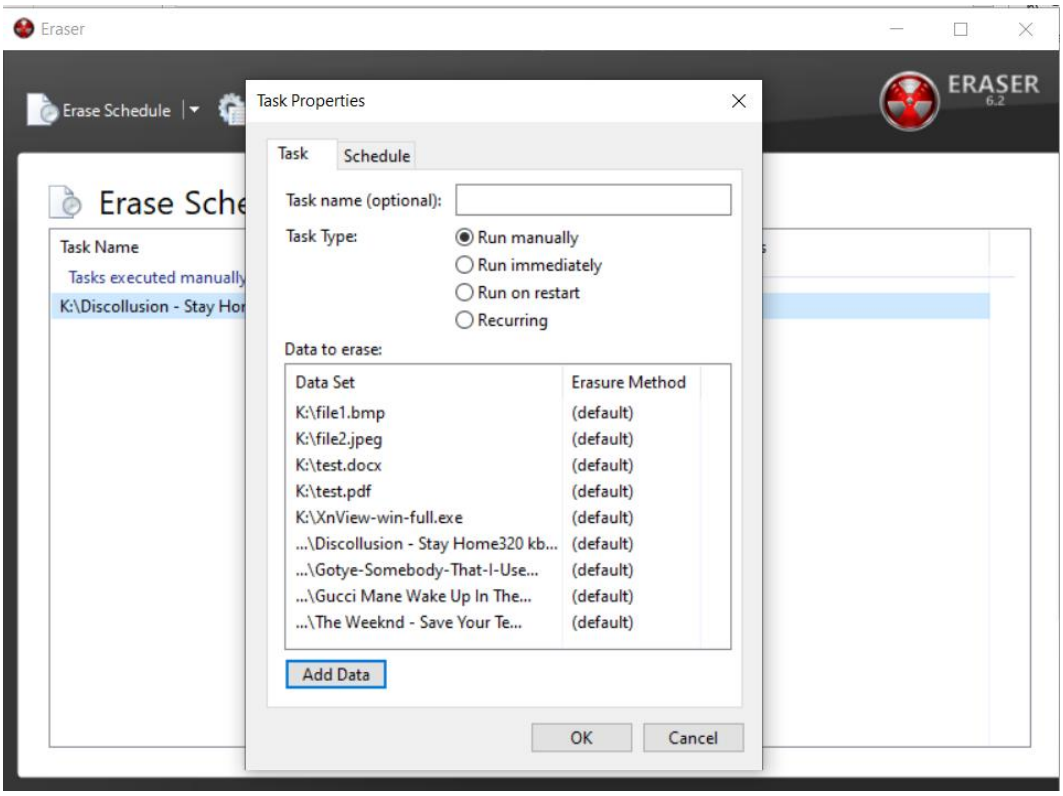

Рисунок Б.11 – Додавання файлів для знищення з SSD-диску за допомогою програми “Eraser”

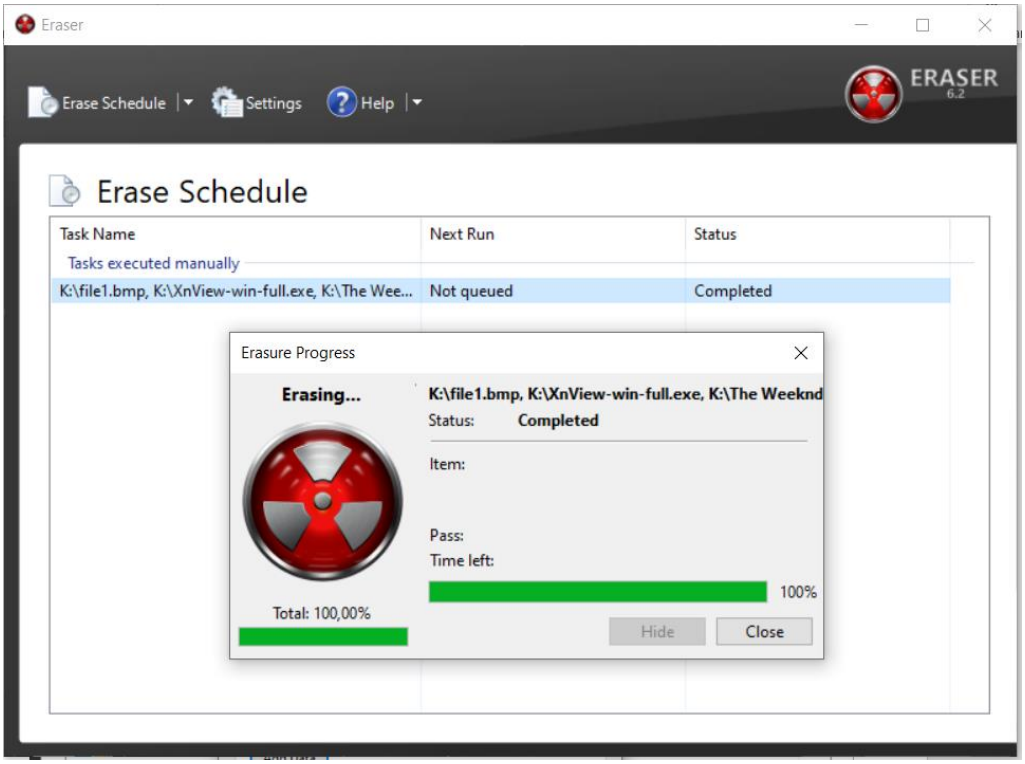

Рисунок Б.12 – Успішне завершення знищення файлів з SSD-диску за допомогою програми “Eraser”

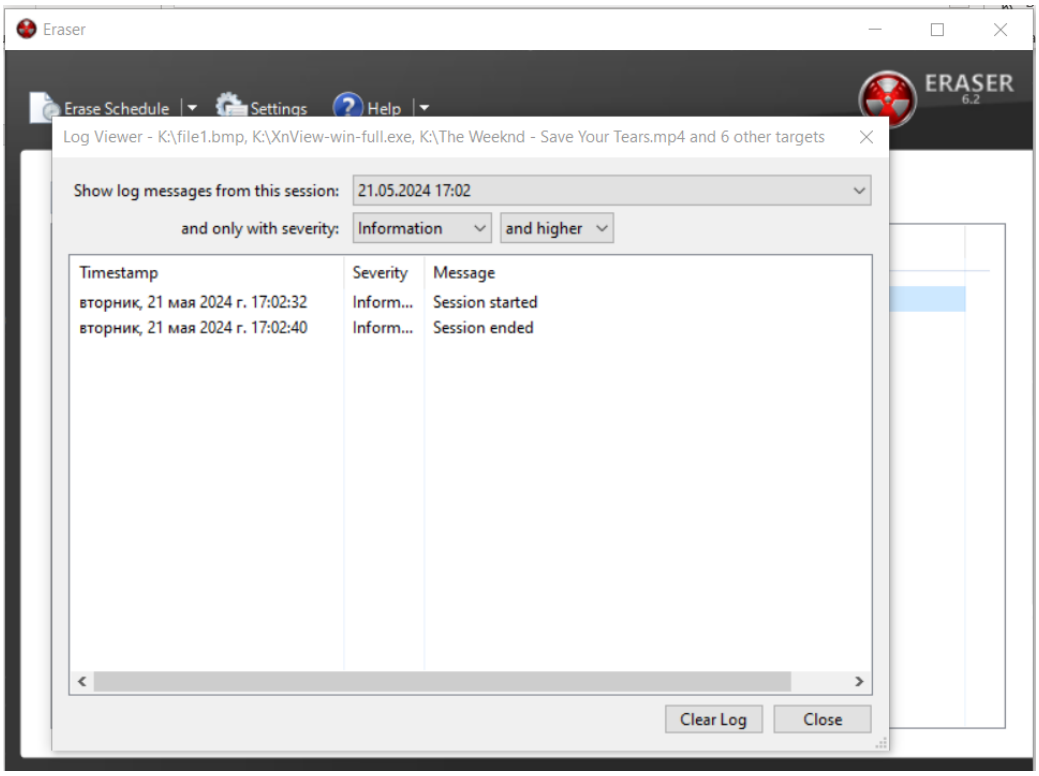

Рисунок Б.13 – Опис знищення файлів з SSD-диску за допомогою “Eraser”

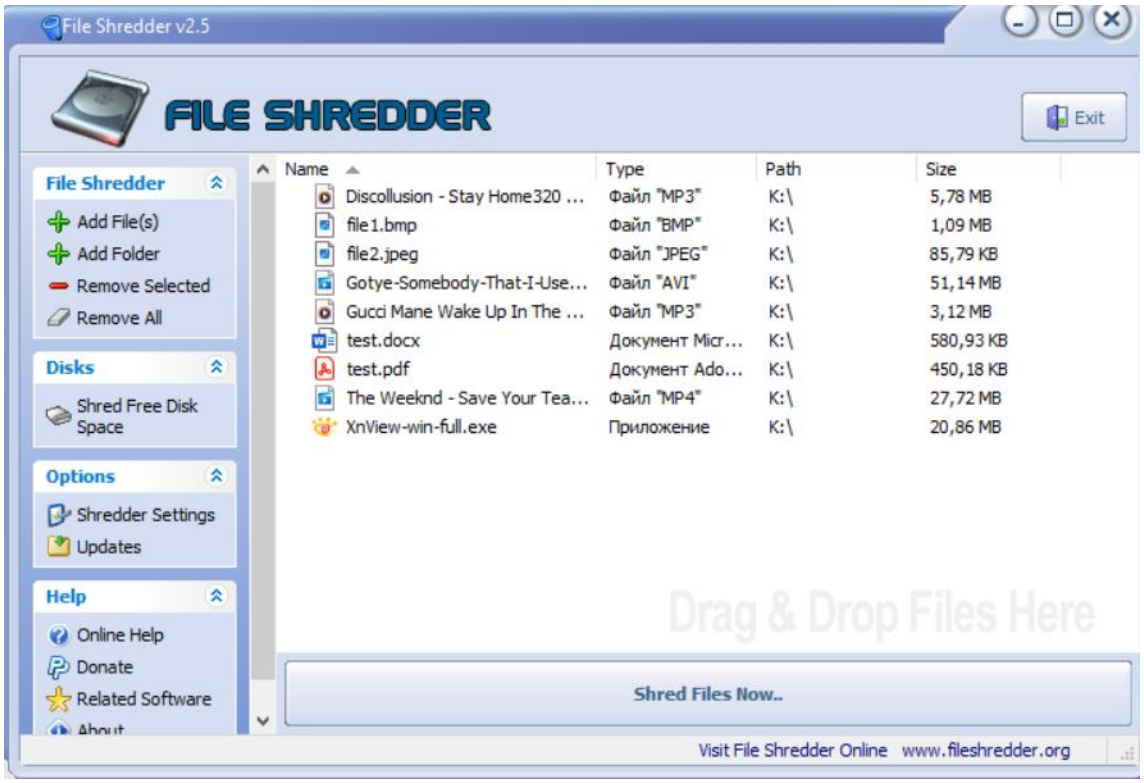

Рисунок Б.14 – Додавання файлів для знищення з SSD-диску за допомогою програми “File Shredder”

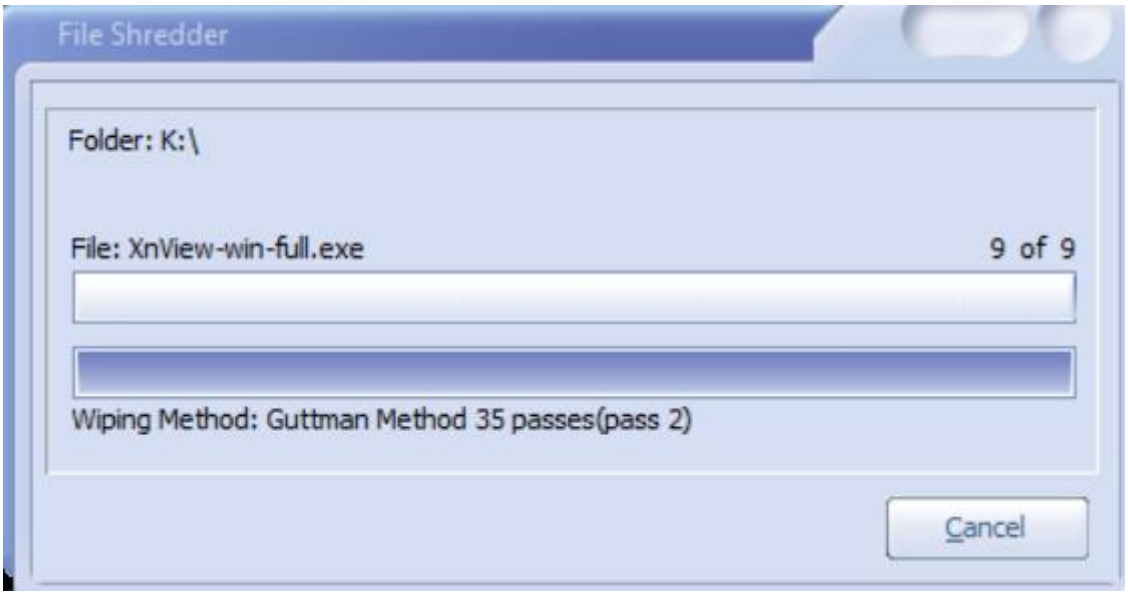

Рисунок Б.15 – Процес знищення файлів з SSD-диску за допомогою програми “File Shredder”

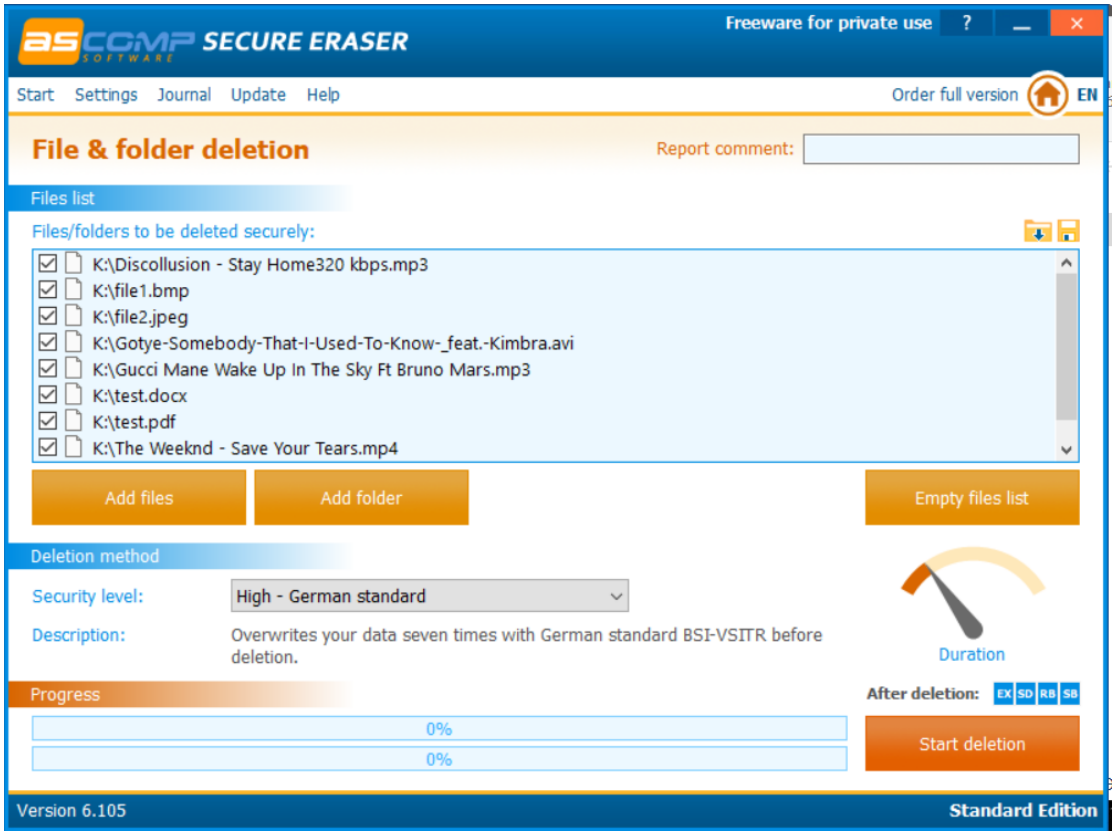

Рисунок Б.16 – Додавання файлів для знищення з SSD-диску за допомогою програми “Secure Eraser”

Secure Eraser

General information

Program version	**6.105**
Computer	**DESKTOP-BT07V55**
User	**Наталія**
Deletion type	**File & folder deletion**
Deletion method	**High - German standard**
Comment	
Started	**22.05.2024 04:40:27**
Finished	**22.05.2024 04:40:40**
State	**completed**
Errors	**0**

Occurred errors (0)

Type	Description	Time

Successfully deleted (9)

Object	Action	Time
K:\XnView-win-full.exe	deleted [High - German standard]	22.05.2024 04:40:28
K:\The Weeknd - Save Your Tears.mp4	deleted [High - German standard]	22.05.2024 04:40:29
K:\test.pdf	deleted [High - German standard]	22.05.2024 04:40:29
K:\test.docx	deleted [High - German standard]	22.05.2024 04:40:29
K:\Gucci Mane Wake Up In The Sky Ft Bruno Mars.mp3	deleted [High - German standard]	22.05.2024 04:40:29
K:\Gotye-Somebody-That-I-Used-To-Know-_feat.-Kimbra.avi	deleted [High - German standard]	22.05.2024 04:40:39
K:\file2.jpeg	deleted [High - German standard]	22.05.2024 04:40:39
K:\file1.bmp	deleted [High - German standard]	22.05.2024 04:40:40
K:\Discollusion - Stay Home320 kbps.mp3	deleted [High - German standard]	22.05.2024 04:40:40

Рисунок Б.17 – Деталі процесу знищення файлів з SSD-диску за допомогою програми “Secure Eraser”

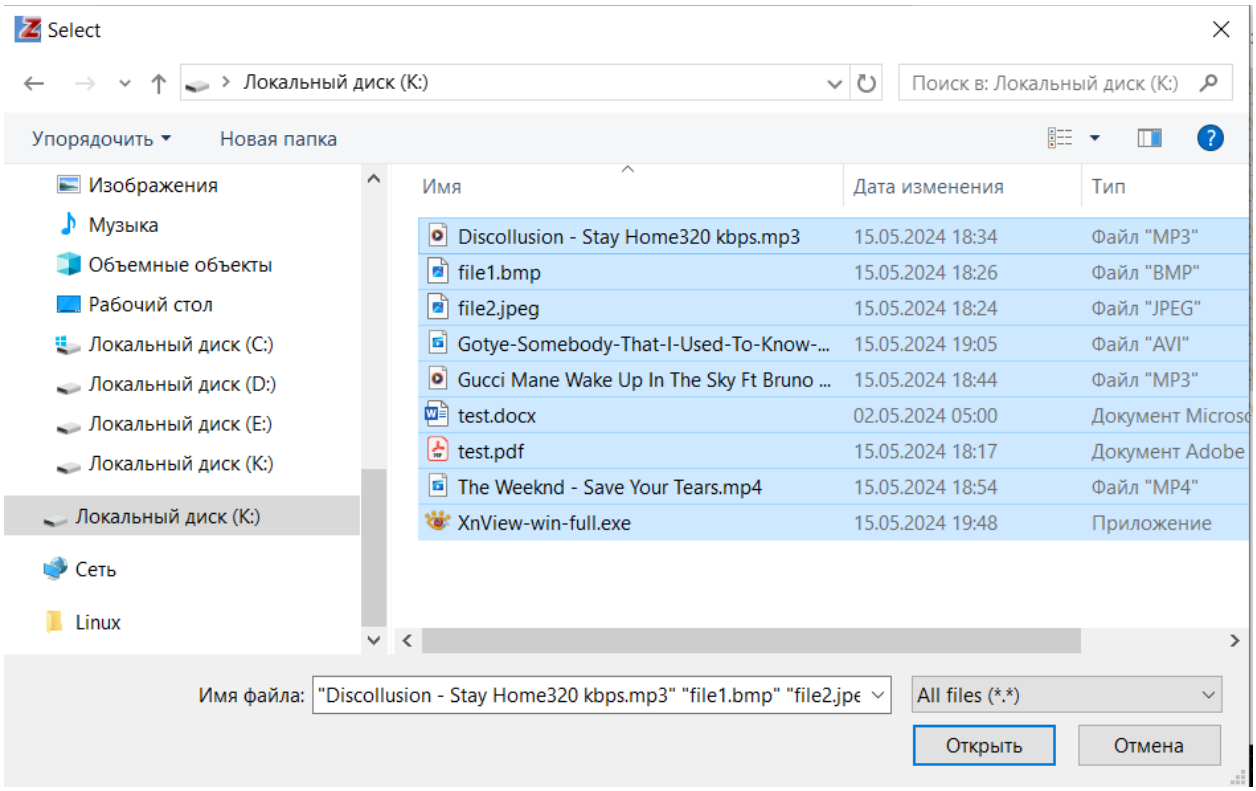

Рисунок Б.18 – Додавання файлів для знищення з SSD-диску за допомогою програми “PrivaZer”

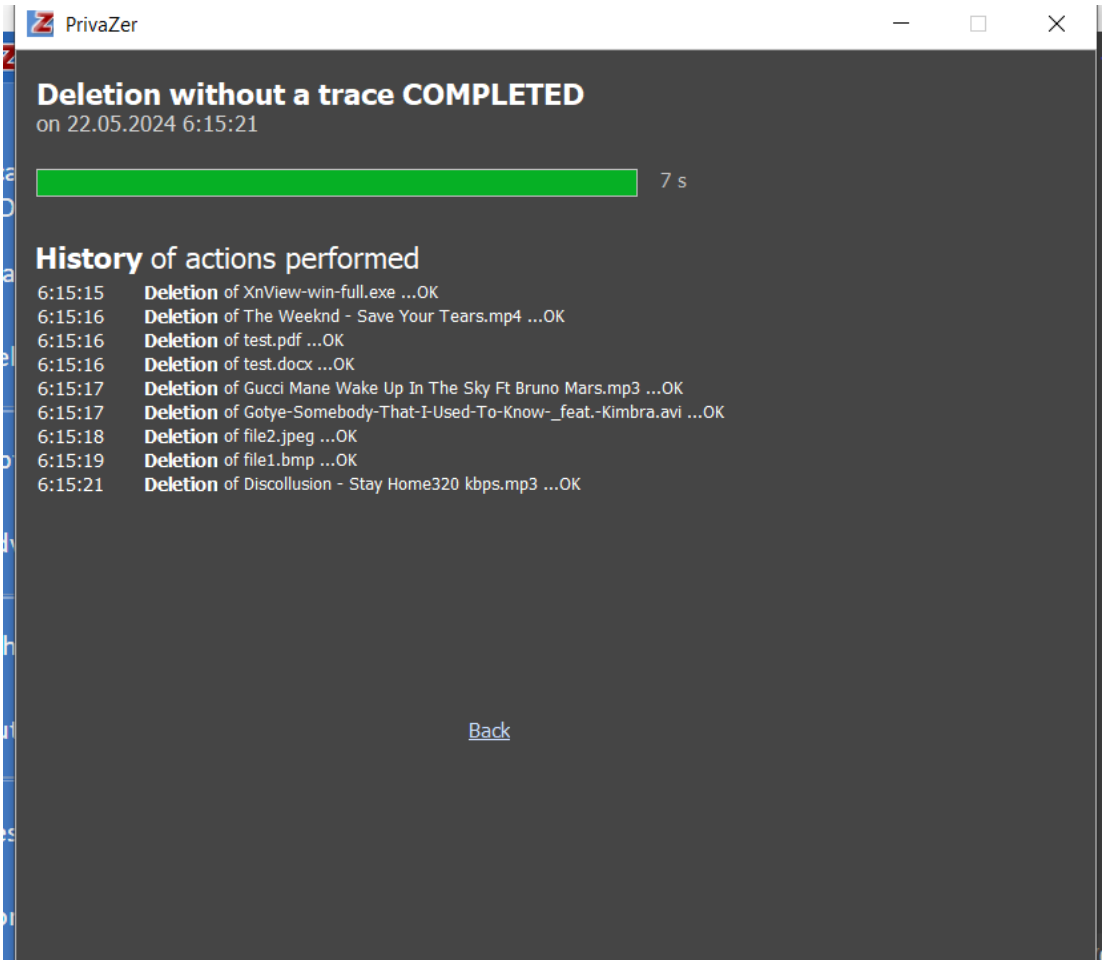

Рисунок Б.19 – Деталі знищення файлів з SSD-диску за допомогою програми “PrivaZer”

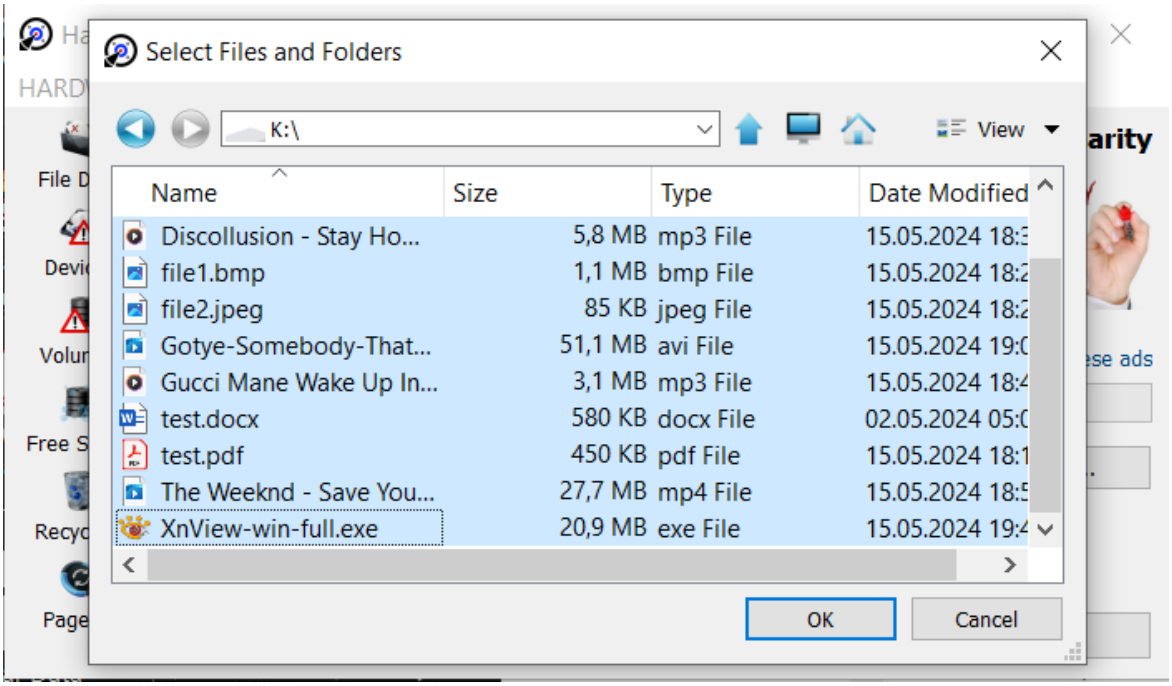

Рисунок Б.20 – Додавання файлів для знищення з SSD-диску за допомогою програми “Hardwipe”

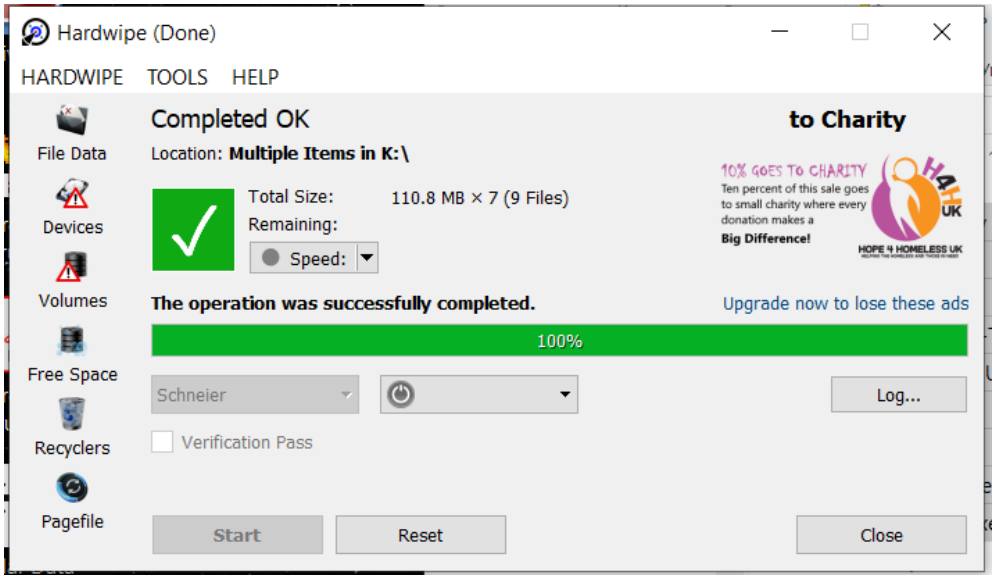

Рисунок Б.21 – Успішне знищення файлів з SSD за допомогою “Hardwipe”

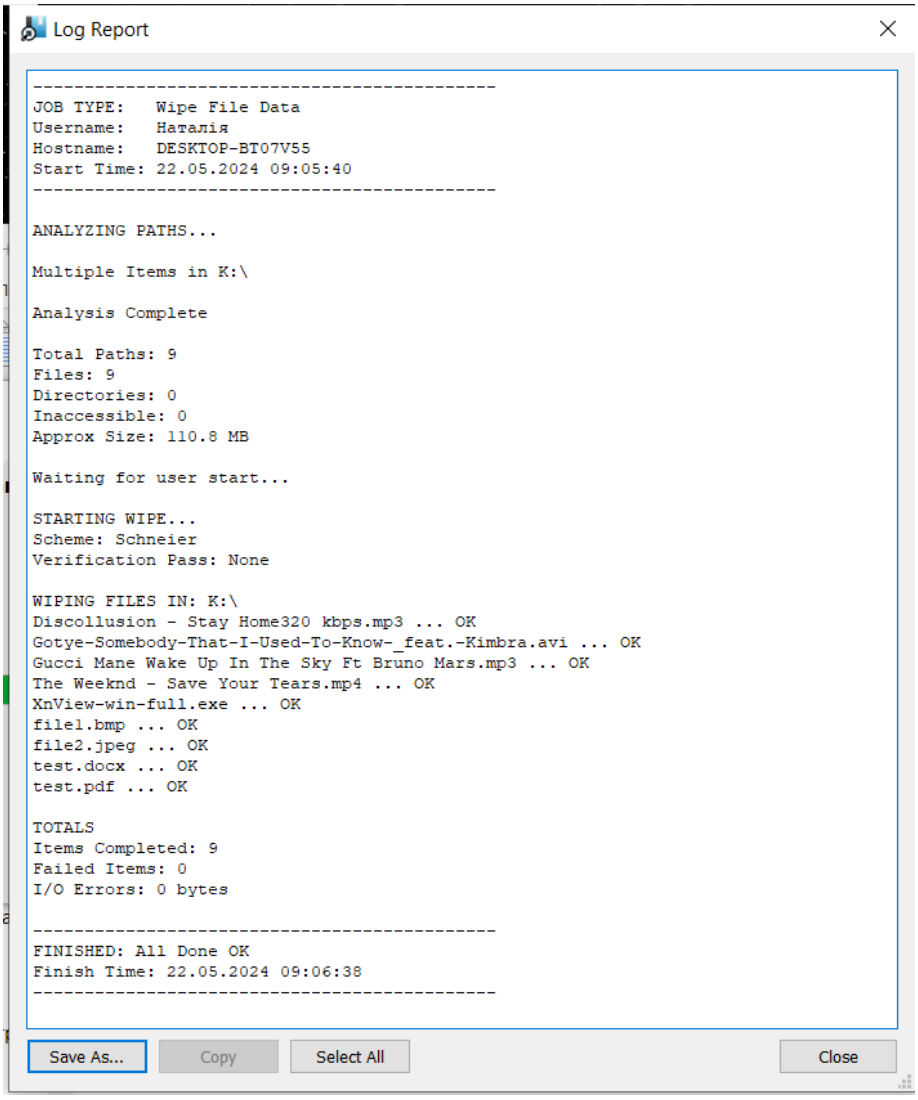

Рисунок Б.22 – Log знищення файлів з SSD за допомогою “Hardwipe”

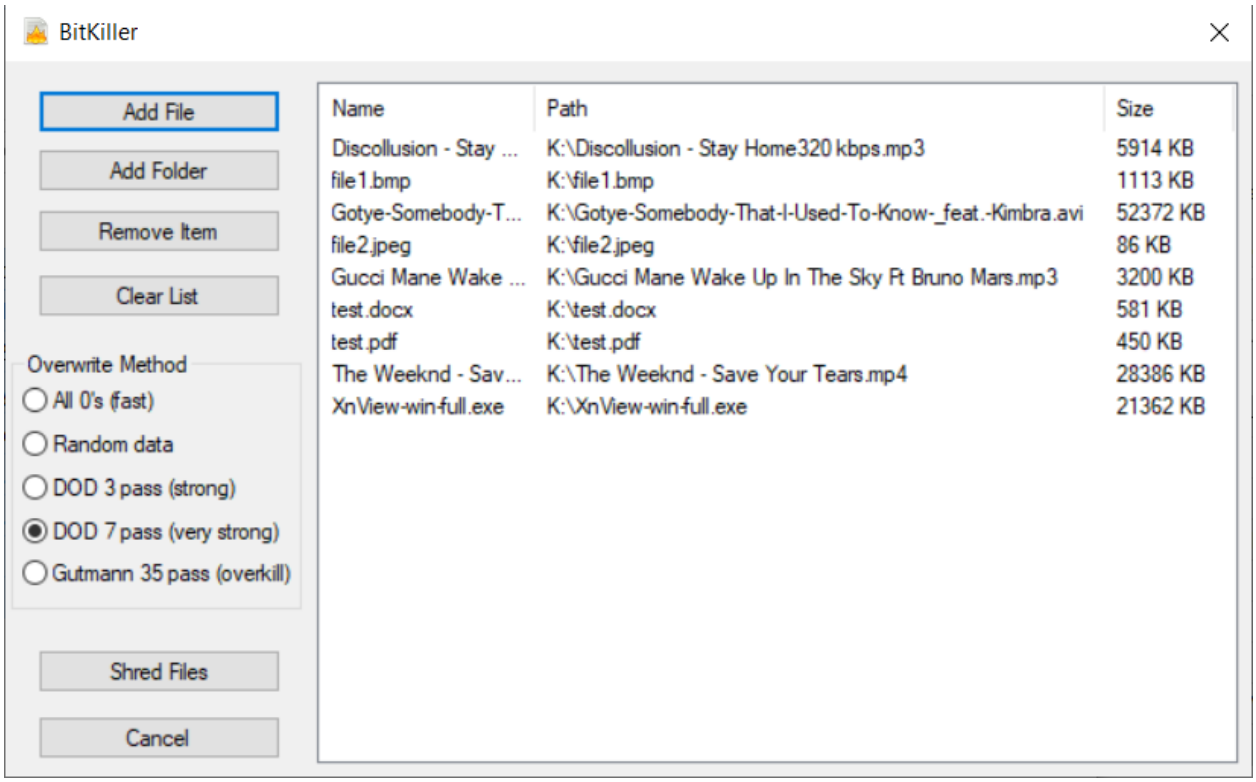

Рисунок Б.23 – Додавання файлів для знищення з SSD-диску за допомогою програми “BitKiller”

ДОДАТОК В

Процес тестування відновлення даних за допомогою програмного забезпечення “Recuva”

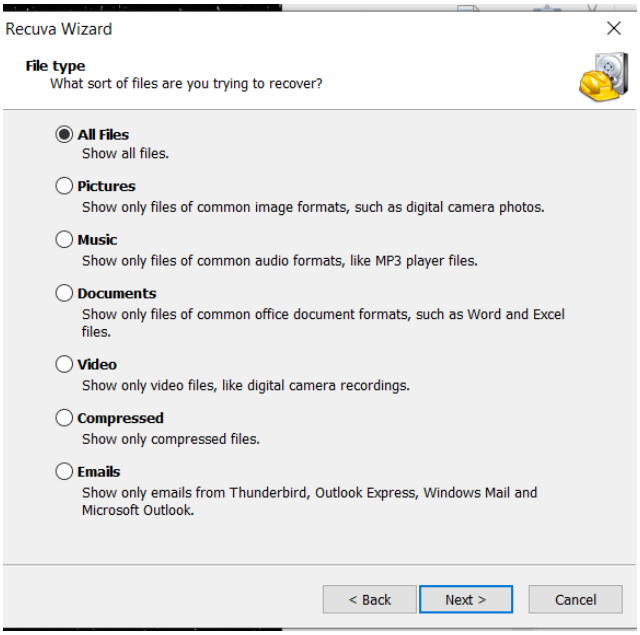

Рисунок В.1 – Вибір усіх типів файлів для відновлення

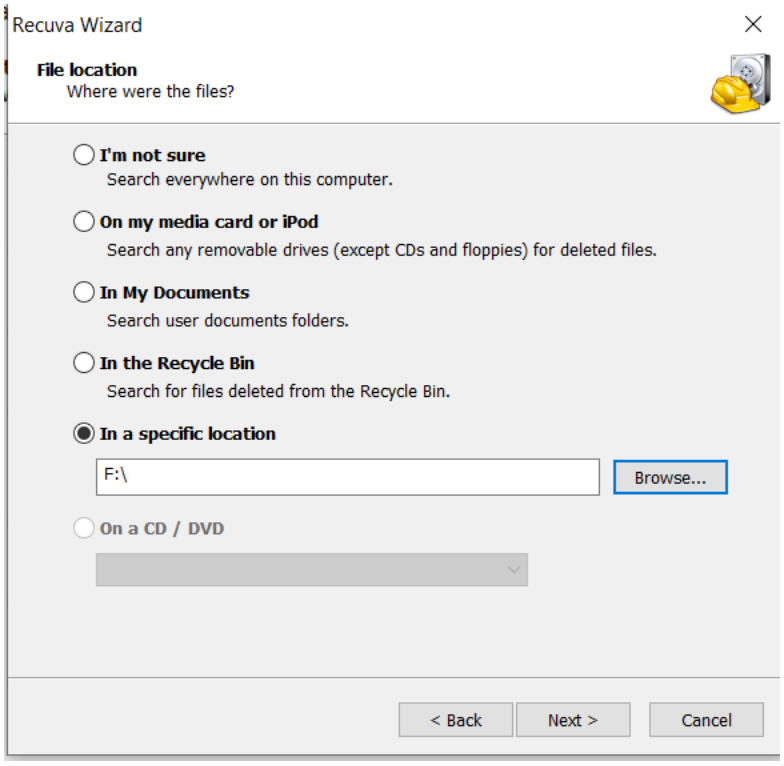

Рисунок В.2 – Вибір локації пошуку даних для відновлення

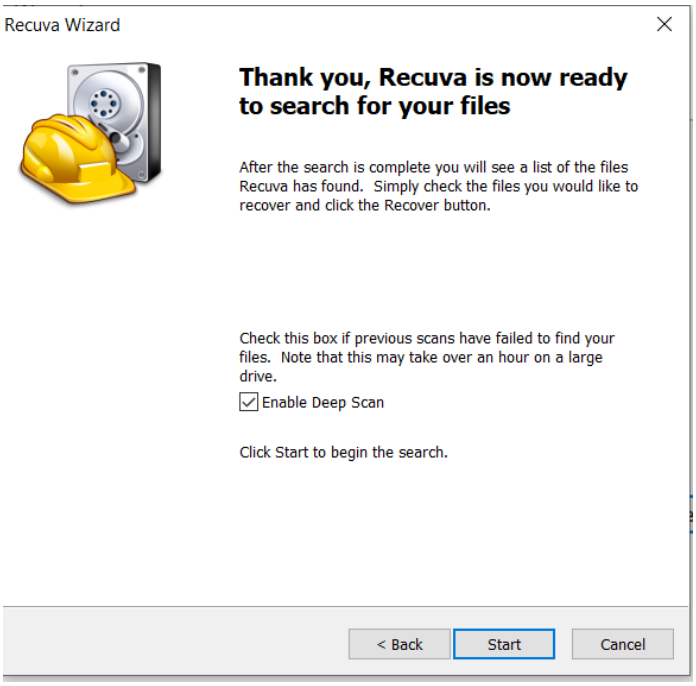

Рисунок В.3 – Вибір глибокого сканування диску

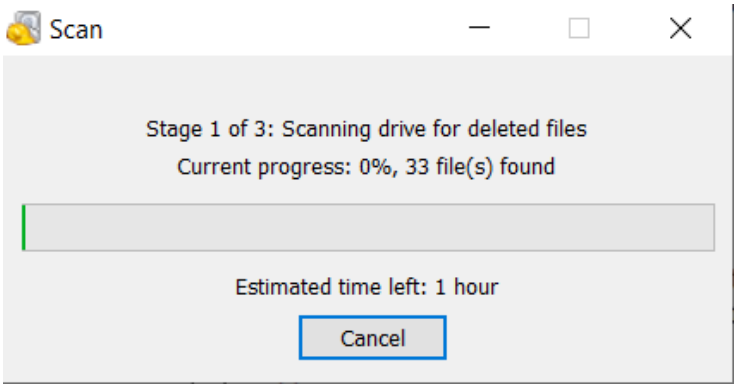

Рисунок В.4 – Глибоке сканування HDD-диску для знаходження видалених файлів після їх знищення програмою “Eraser”

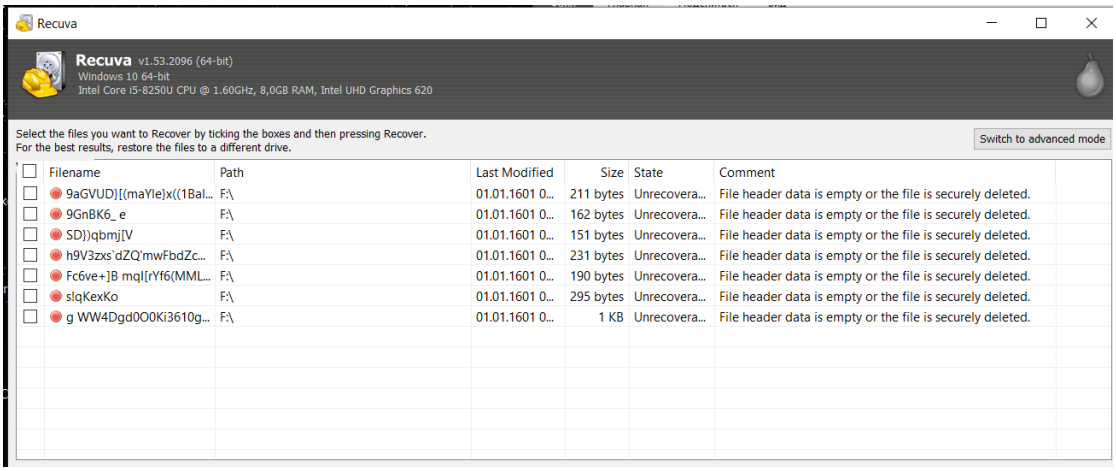

Рисунок В.5 – Результати сканування

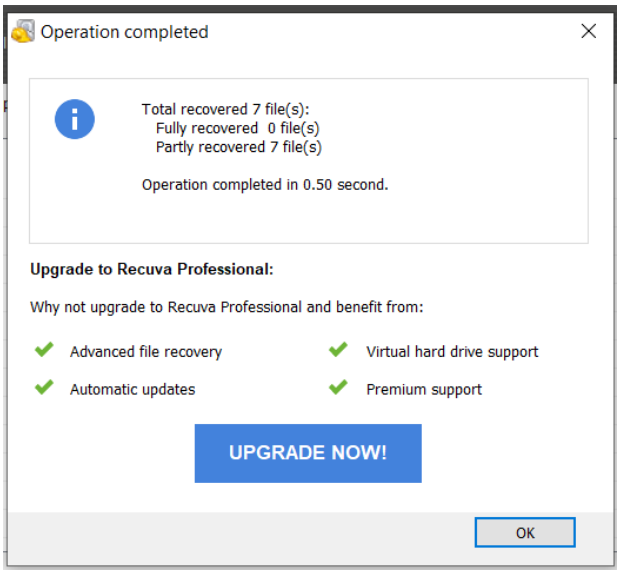

Рисунок В.6 – Log відновлення файлів, після їх знищення “Eraser”

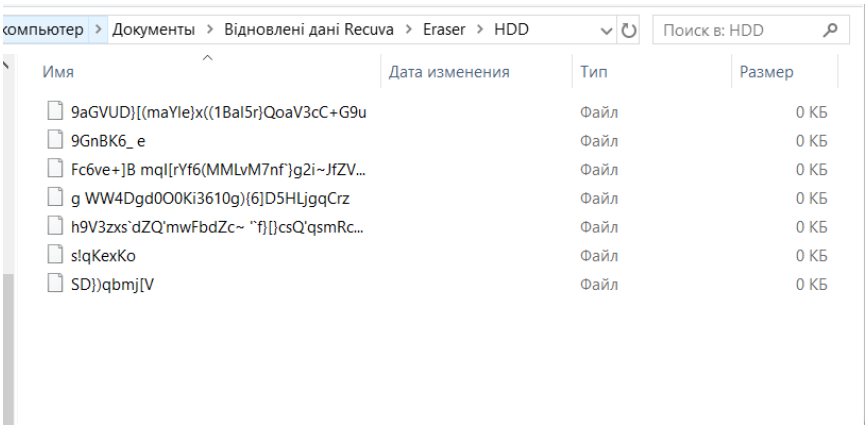

Рисунок В.7 – Відновленні файли з HDD-диску після їх знищення “Eraser”

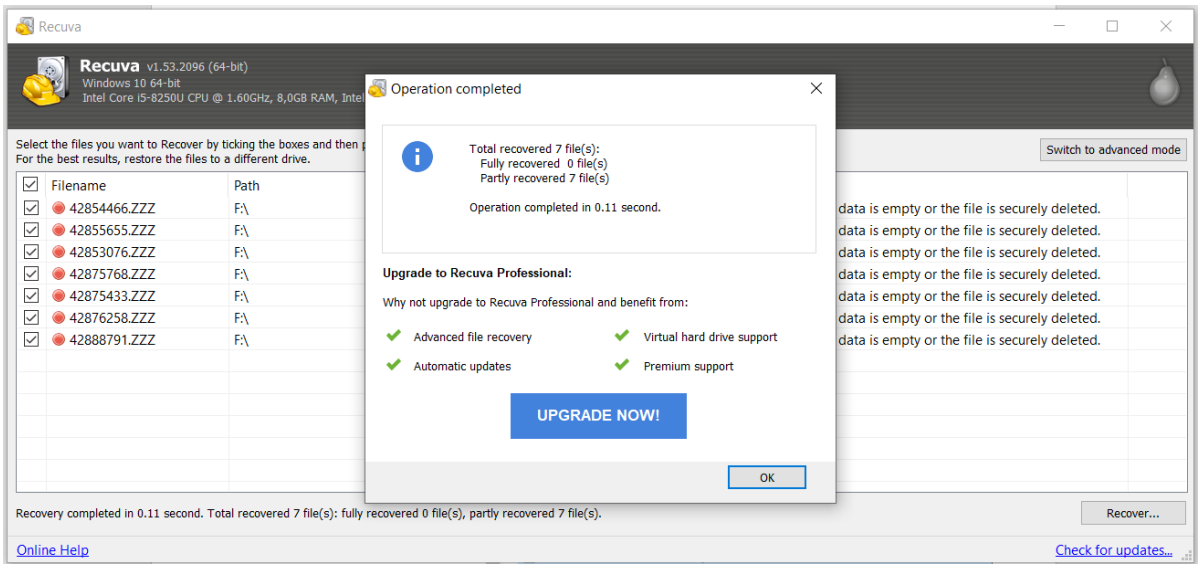

Рисунок В.8 – Деталі відновлення файлів, після їх знищення програмою “File Shredder” з HDD-диску

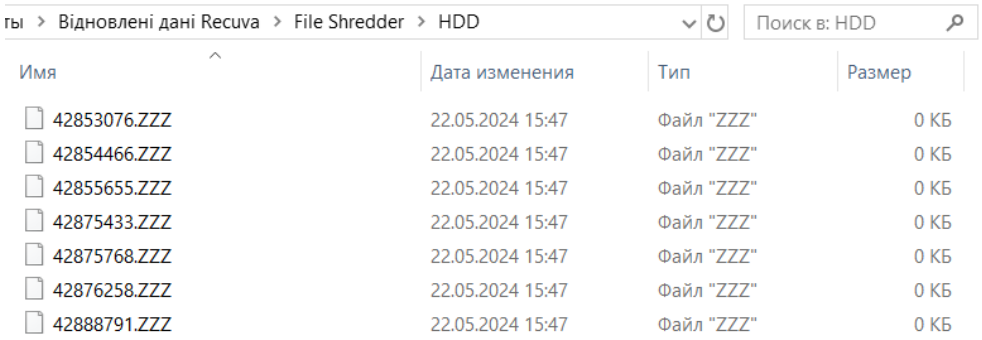

Рисунок В.9 – Відновленні файли з диску HDD після їх знищення програмним забезпеченням “File Shredder”

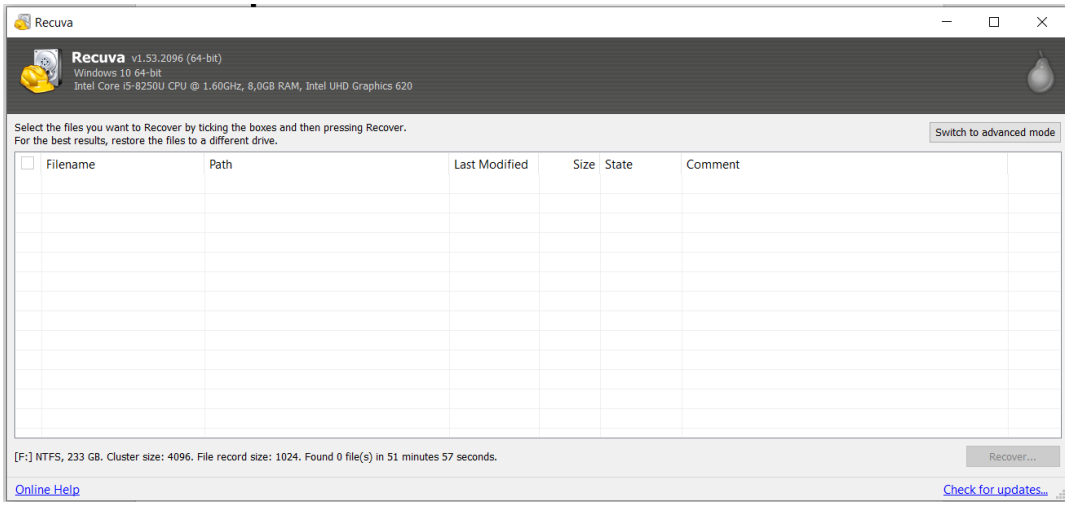

Рисунок В.10 – Результат сканування HDD-диску на наявність знищених файлів програмою “Secure Eraser”

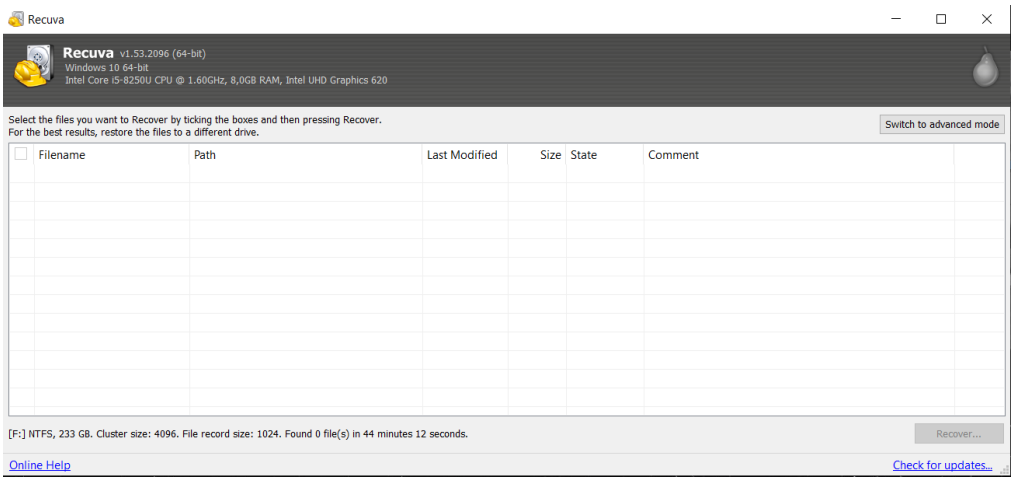

Рисунок В.11 – Результат сканування HDD-диску на наявність знищених файлів програмою “PrivaZer”

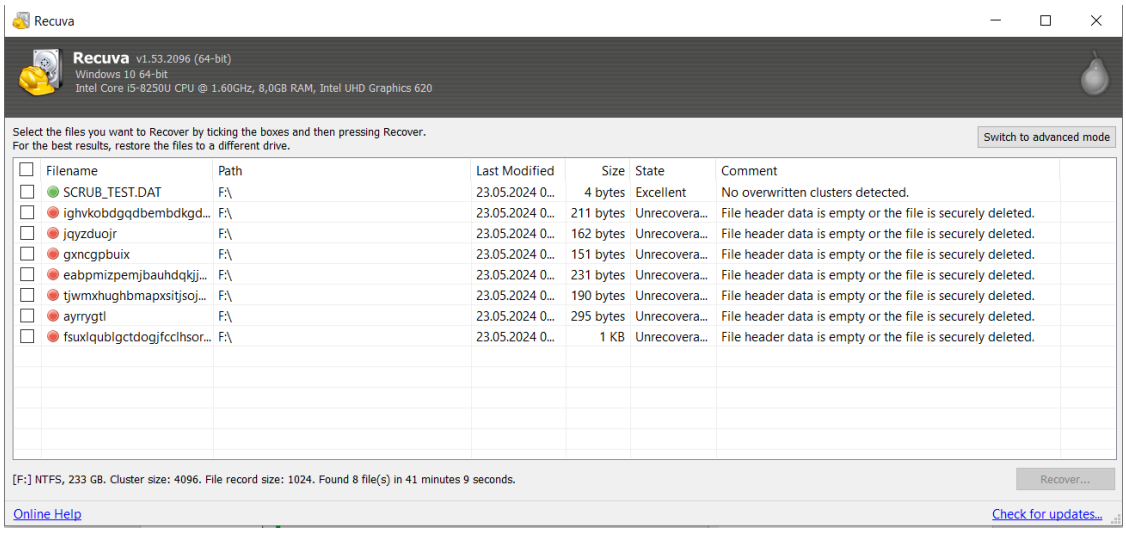

Рисунок В.12 – Результат сканування HDD-диску на наявність знищених файлів програмою “Hardwipe”

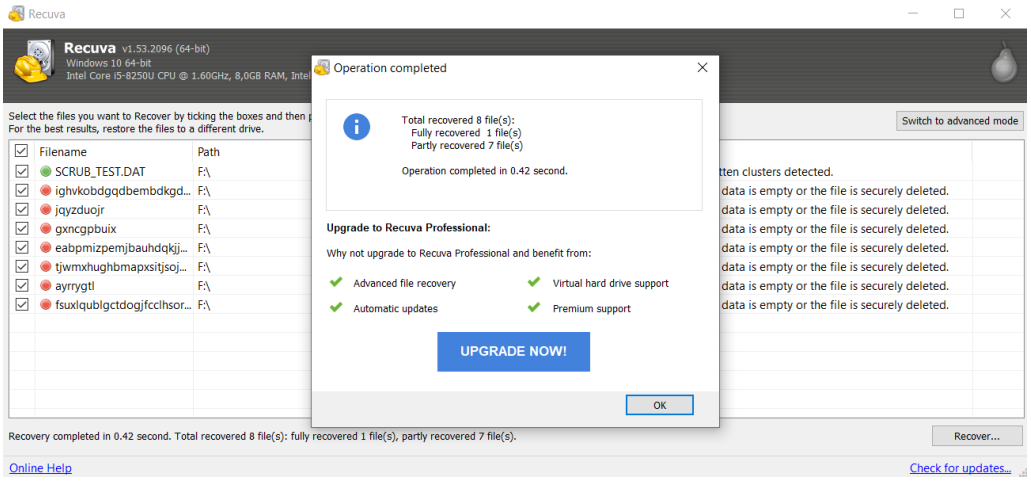

Рисунок В.13 – Відновлення файлів після їх знищення з HDD-диску програмою “Hardwipe”

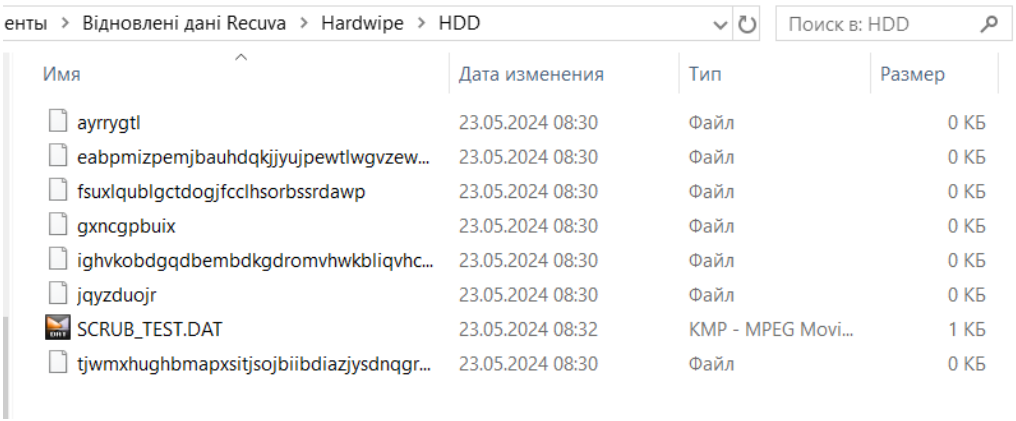

Рисунок В.14 – Відновлені файли після їх знищення з HDD-диску програмою “Hardwipe”

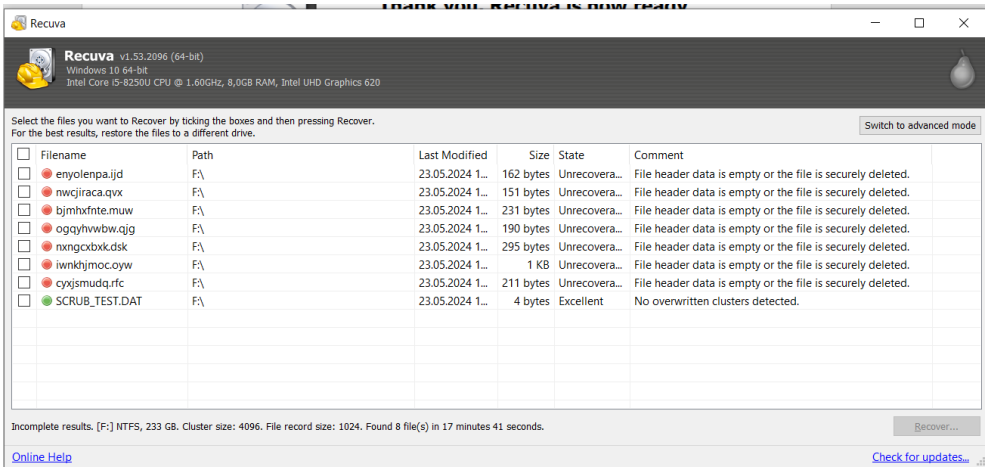

Рисунок В.15 – Результат сканування HDD-диску на наявність знищених файлів програмою “BitKiller”

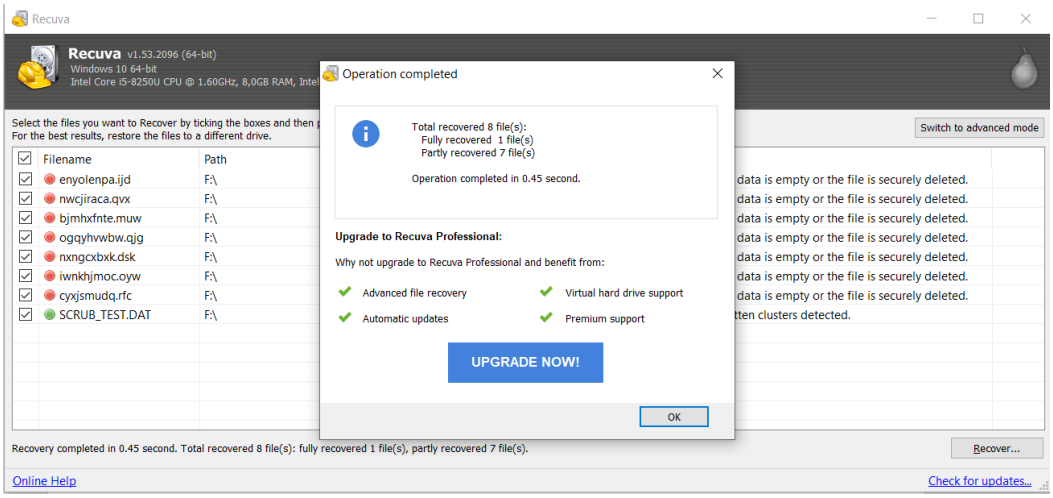

Рисунок В.16 – Відновлення файлів після їх знищення з HDD-диску програмою “BitKiller”

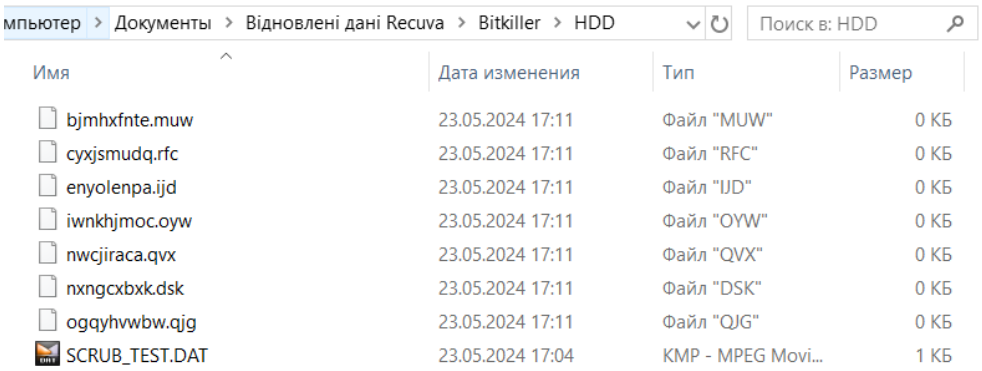

Рисунок В.17 – Відновлені файли після їх знищення з HDD-диску програмою “BitKiller”

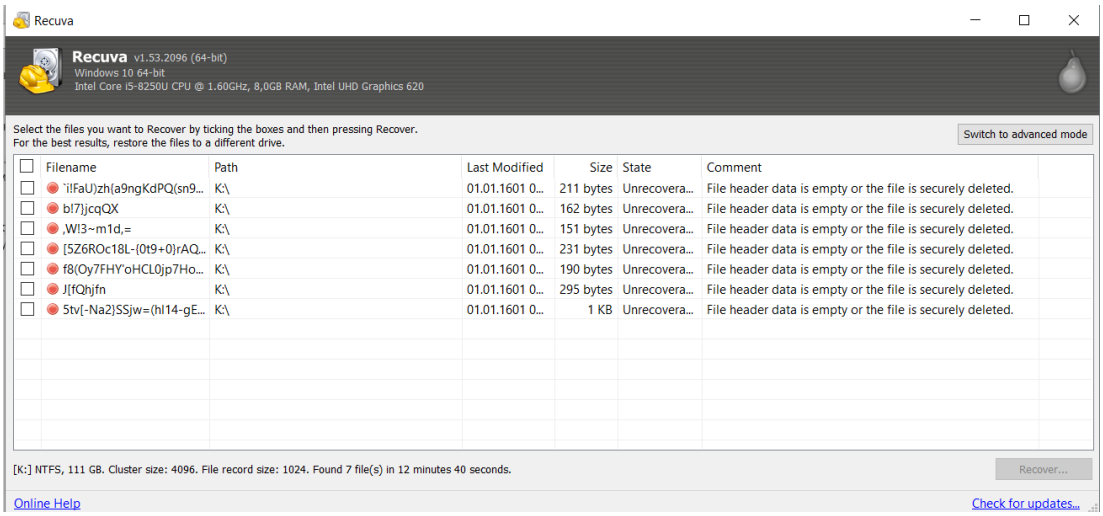

Рисунок В.18 – Результат сканування SSD-диску на наявність знищених файлів програмою “Eraser”

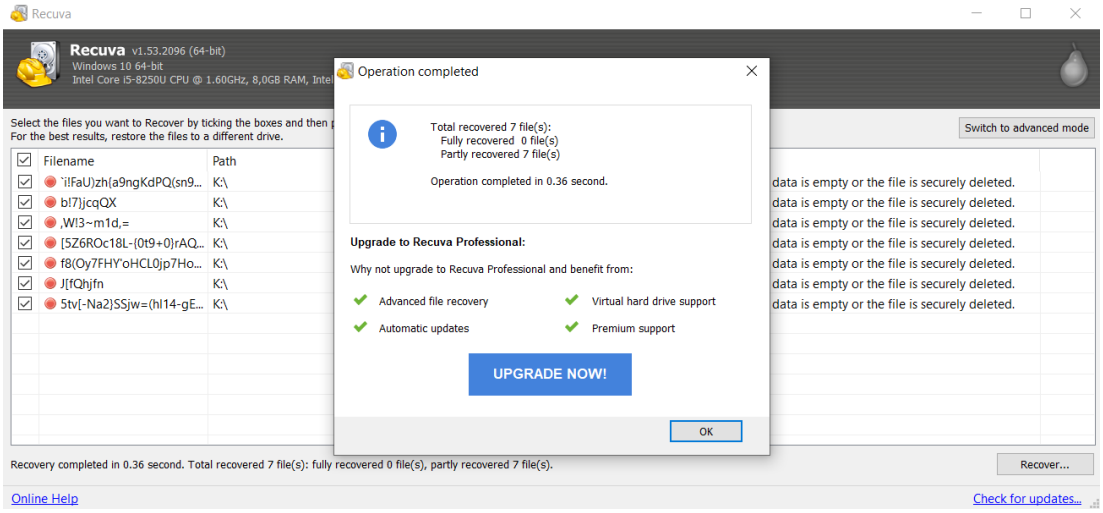

Рисунок В.19 – Відновлення файлів після їх знищення з SSD-диску програмою “Eraser”

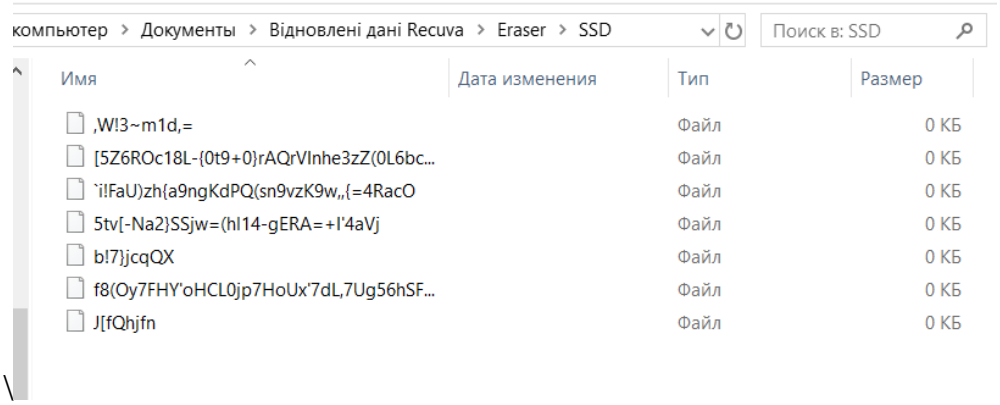

Рисунок В.20 – Відновлені файли після їх знищення з SSD-диску програмою “Eraser”

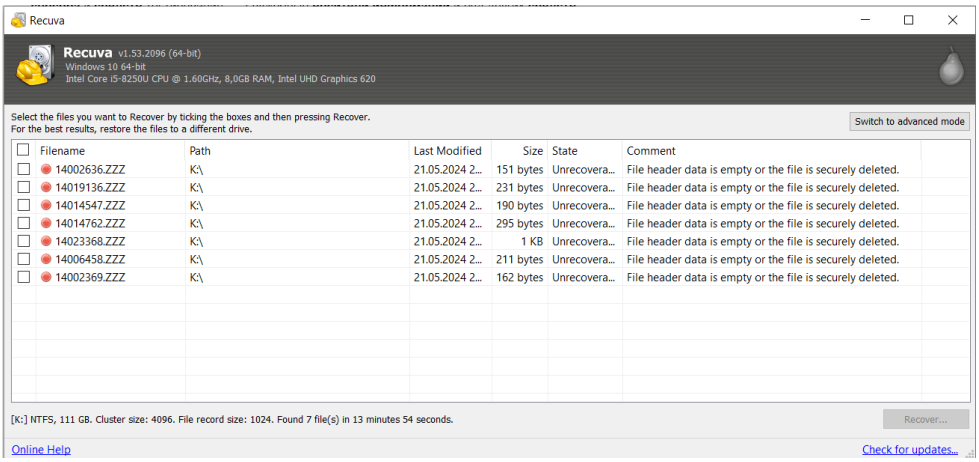

Рисунок В.21 – сканування SSD-диску на наявність знищених файлів програмою “File Shredder”

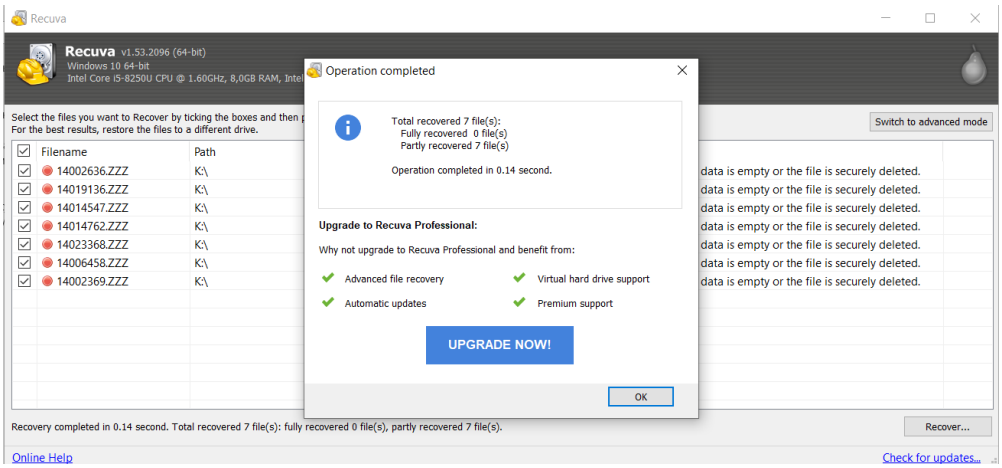

Рисунок В.22 – Відновлення файлів після їх знищення з SSD-диску програмою “File Shredder”

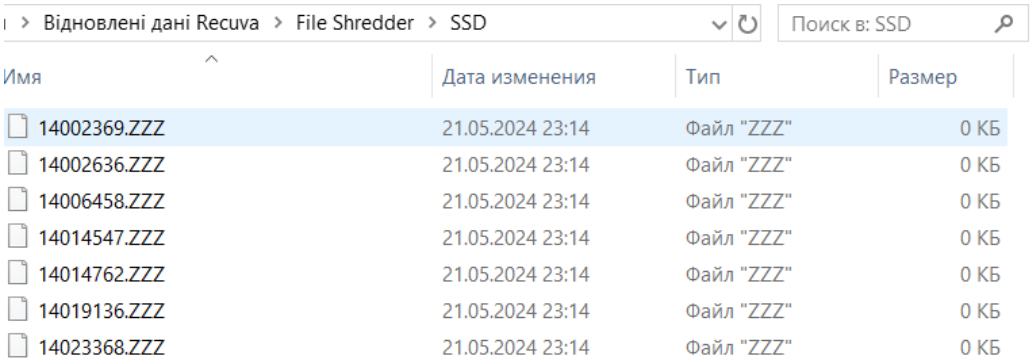

Рисунок В.23 – Відновлені файли після їх знищення з SSD-диску програмою “File Shredder”

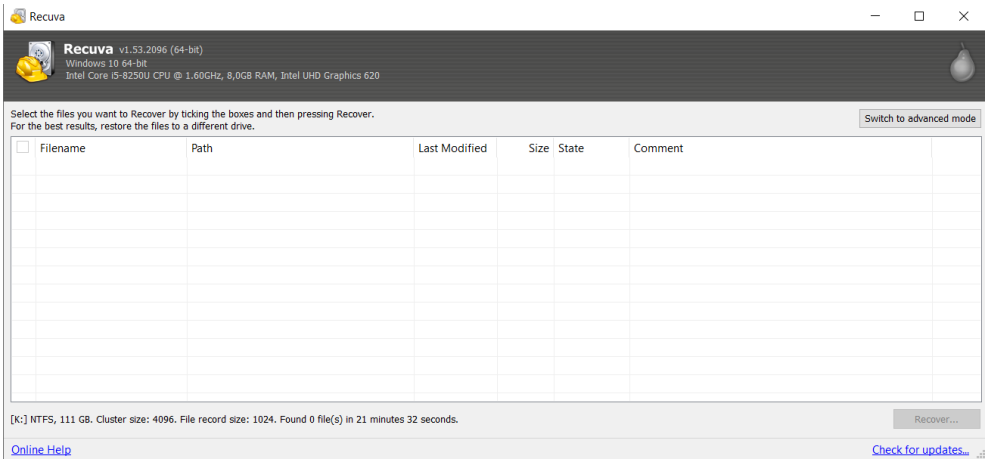

Рисунок В.24 – Результат сканування SSD-диску на наявність знищених файлів програмою “Secure Eraser”

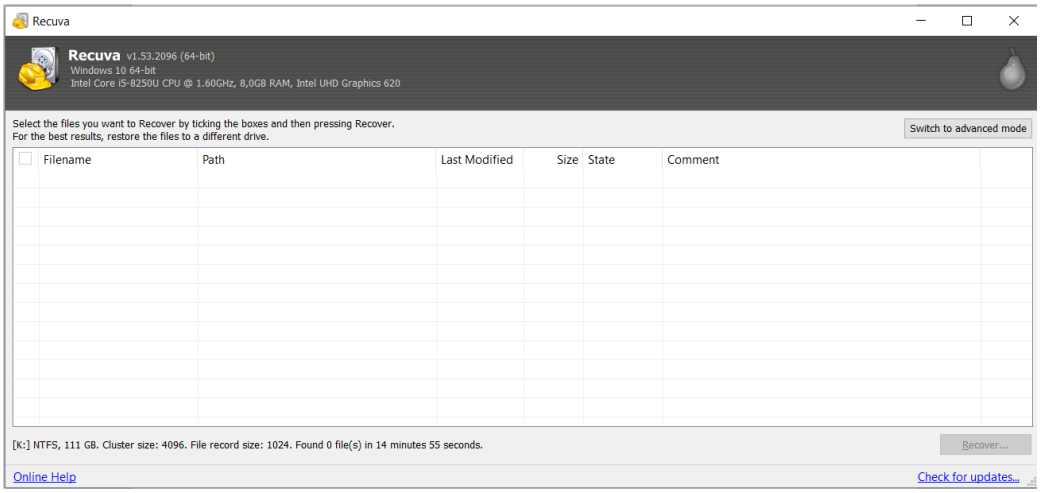

Рисунок В.25 – Результат сканування SSD-диску на наявність знищених файлів програмою “PrivaZer”

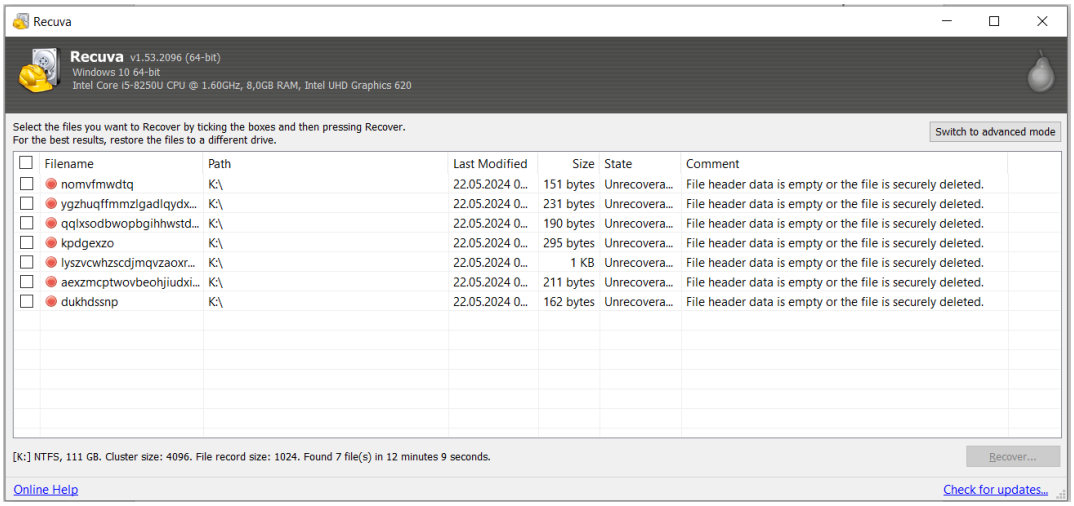

Рисунок В.26 – Результат сканування SSD-диску на наявність знищених файлів програмою “Hardwipe”

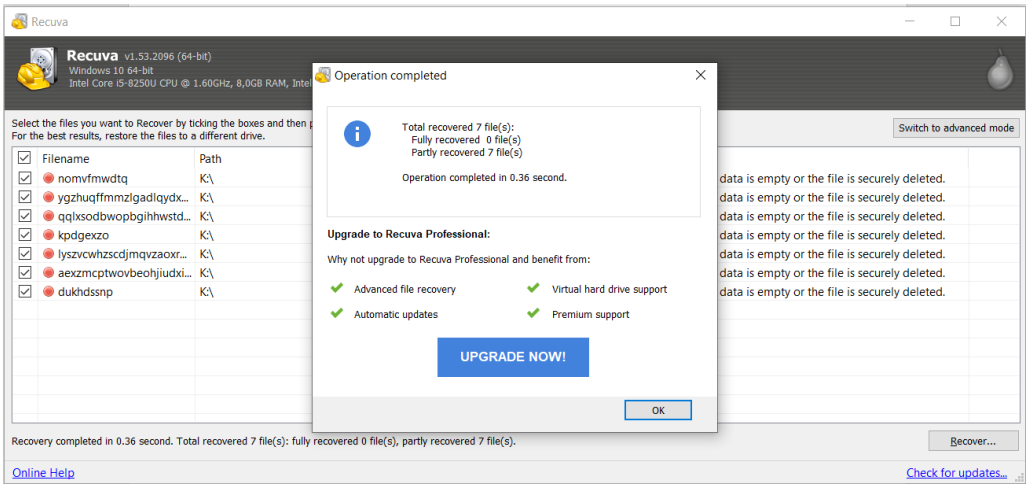

Рисунок В.27 – Відновлення файлів після їх знищення з SSD-диску програмою “Hardwipe”

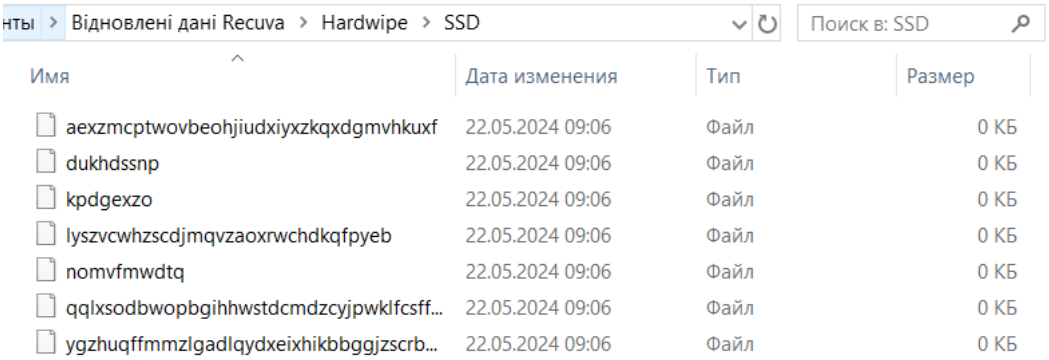

Рисунок В.28 – Відновлені файли після їх знищення з SSD-диску програмою “Hardwipe”

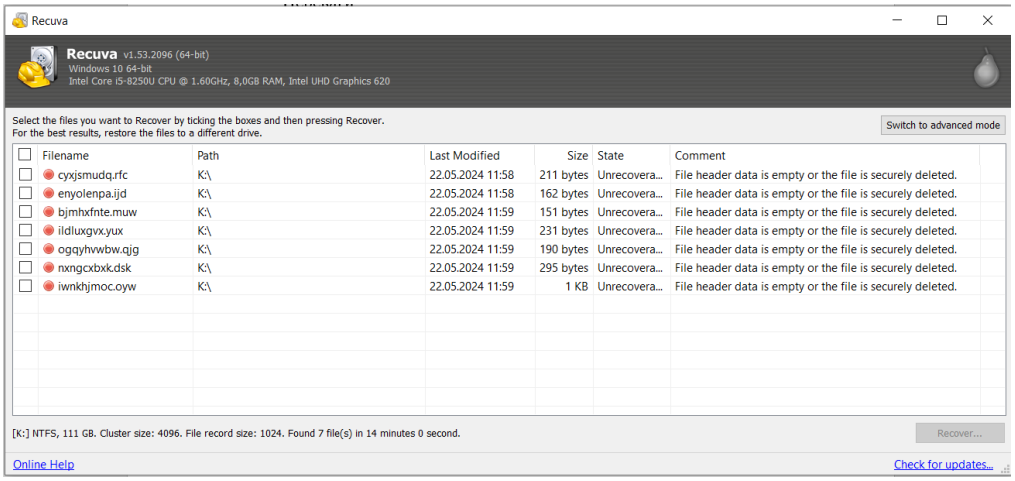

Рисунок В.29 – Результат сканування SSD-диску на наявність знищених файлів програмою “BitKiller”

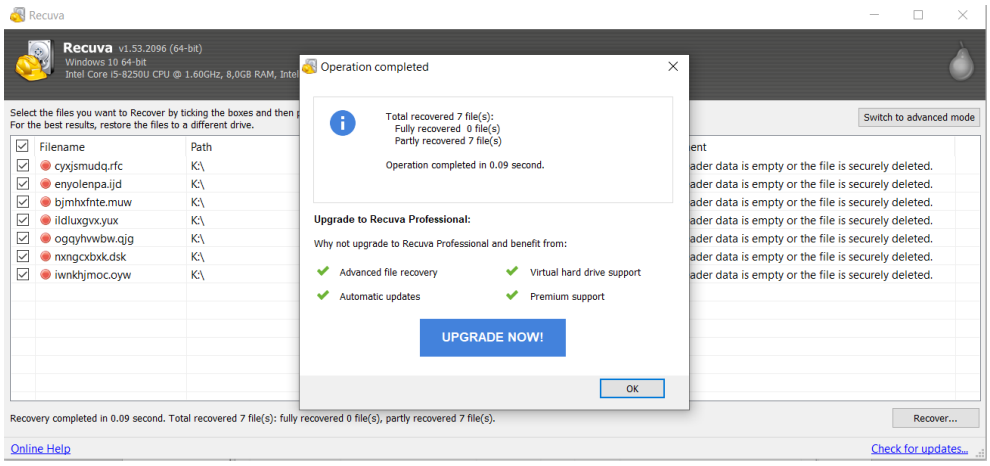

Рисунок В.30 – Відновлення файлів після їх знищення з SSD-диску програмою “BitKiller”

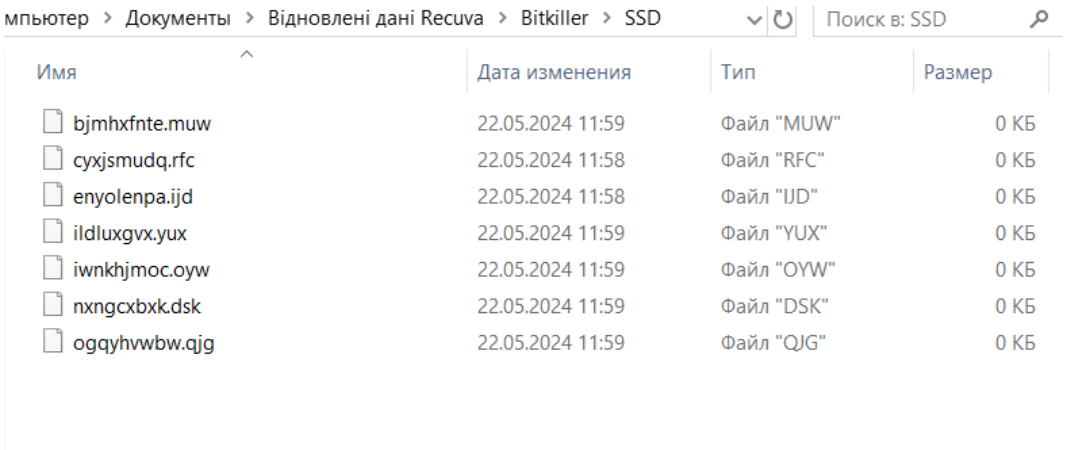

Рисунок В.31 – Відновлені файли після їх знищення з SSD-диску програмою “BitKiller”

ДОДАТОК Г

Процес тестування відновлення даних за допомогою програмного забезпечення “Disk Drill”

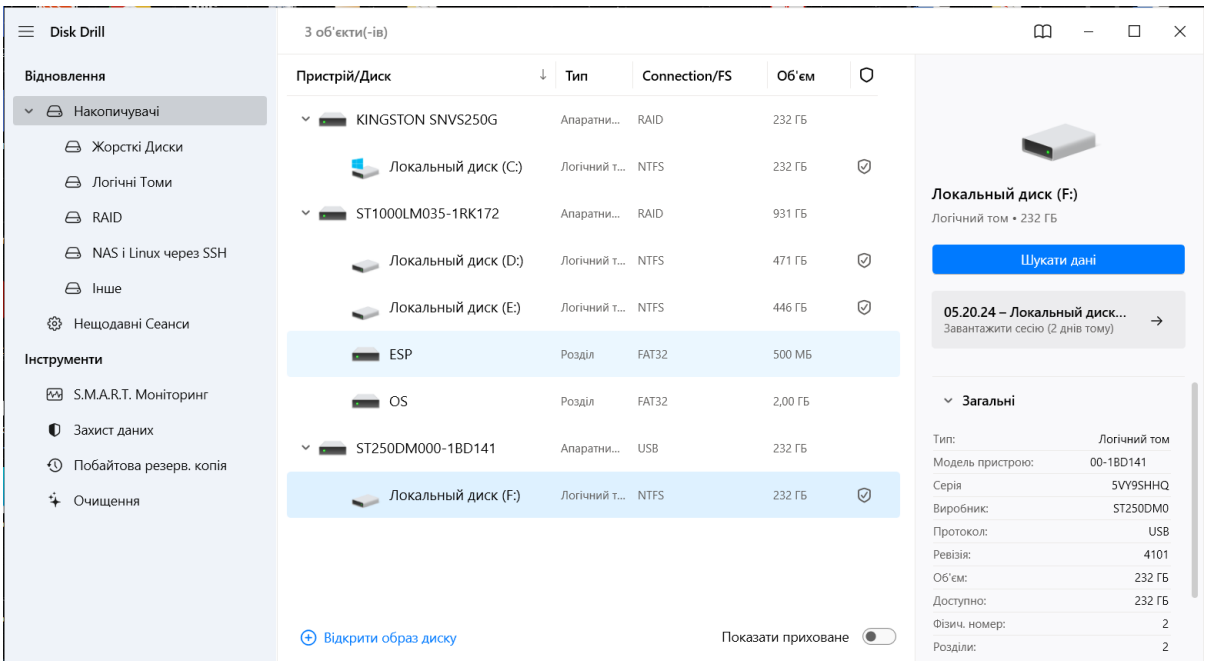

Рисунок Г.1 – Вибір диску для сканування на наявність втрачених або видалених файлів

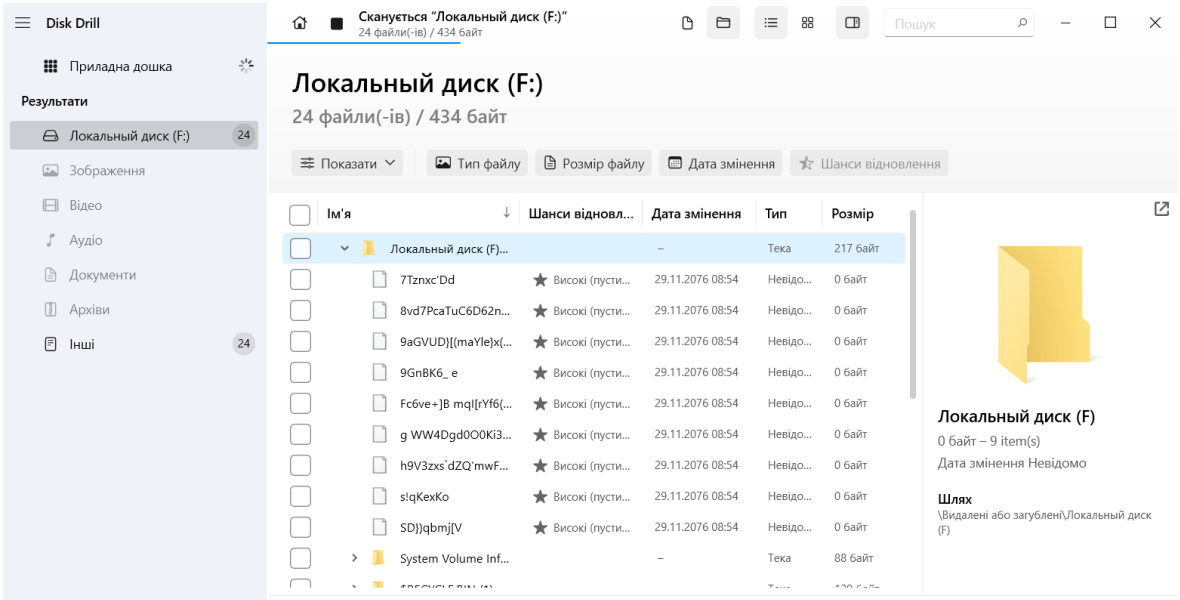

Рисунок Г.2 – Процес сканування HDD-диску на наявність знищених файлів програмою “Eraser”

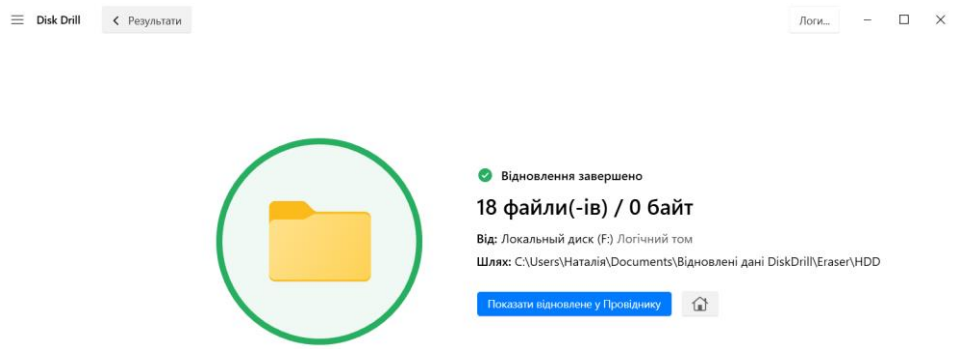

Рисунок Г.3 – Завершення відновлення файлів з HDD-диску після їх знищення програмою “Eraser”

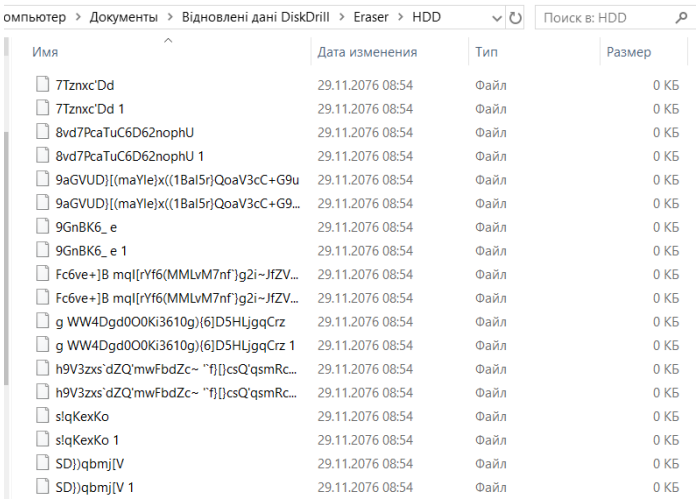

Рисунок Г.4 – Відновлені файли з HDD після їх знищення “Eraser”

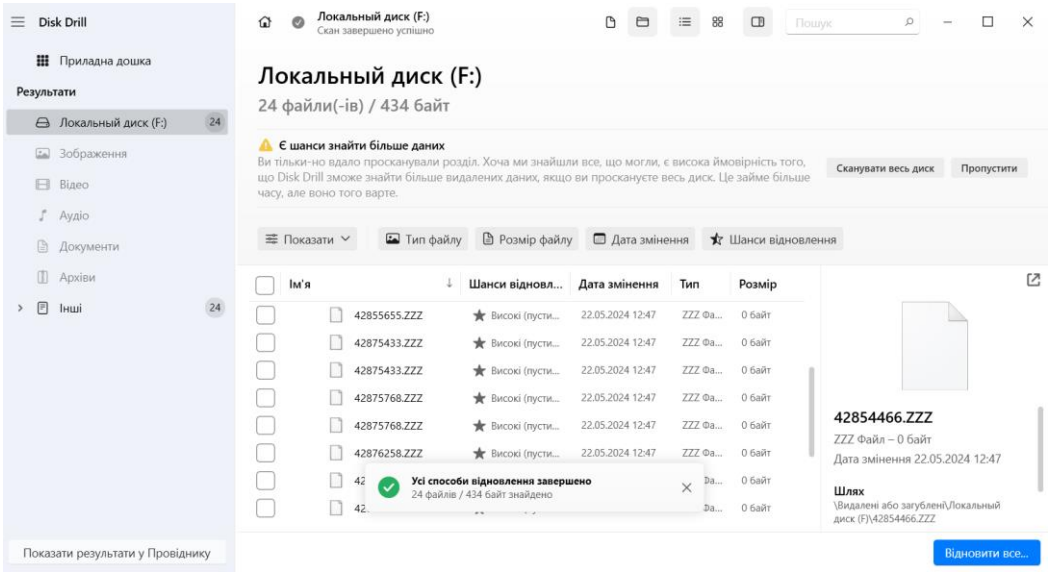

Рисунок Г.5 – Результат сканування файлів з HDD-диску після їх знищення програмою “File Shredder”

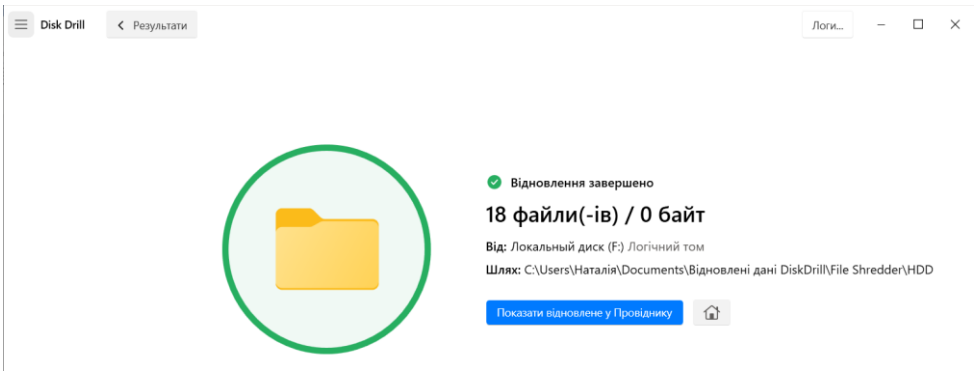

Рисунок Г.6 – Завершення відновлення файлів з HDD після їх знищення програмою “File Shredder”

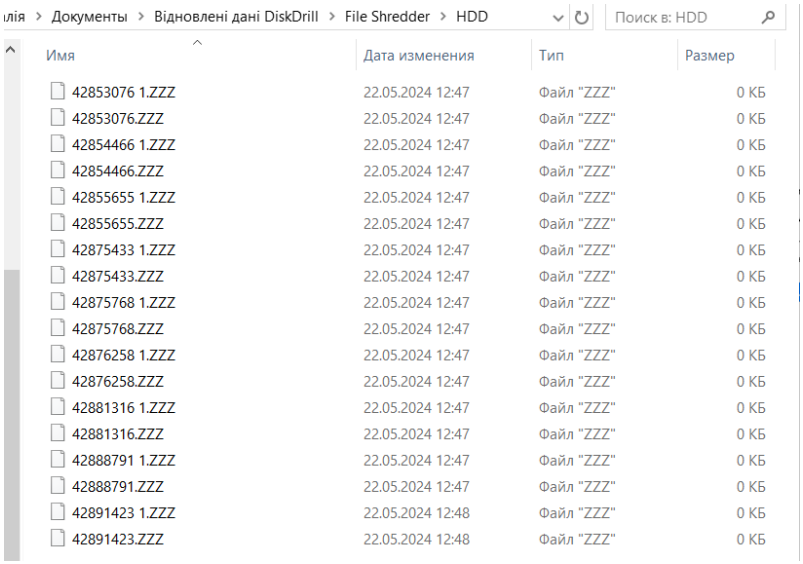

Рисунок Г.7 – Відновлені файли з HDD після їх знищення “File Shredder”

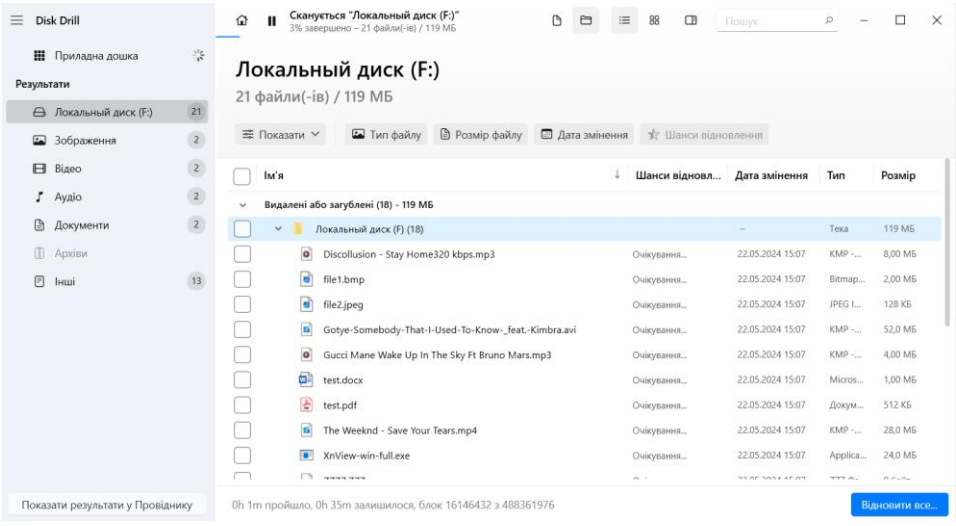

Рисунок Г.8 – Процес сканування HDD на наявність знищених файлів програмою “Secure Eraser”

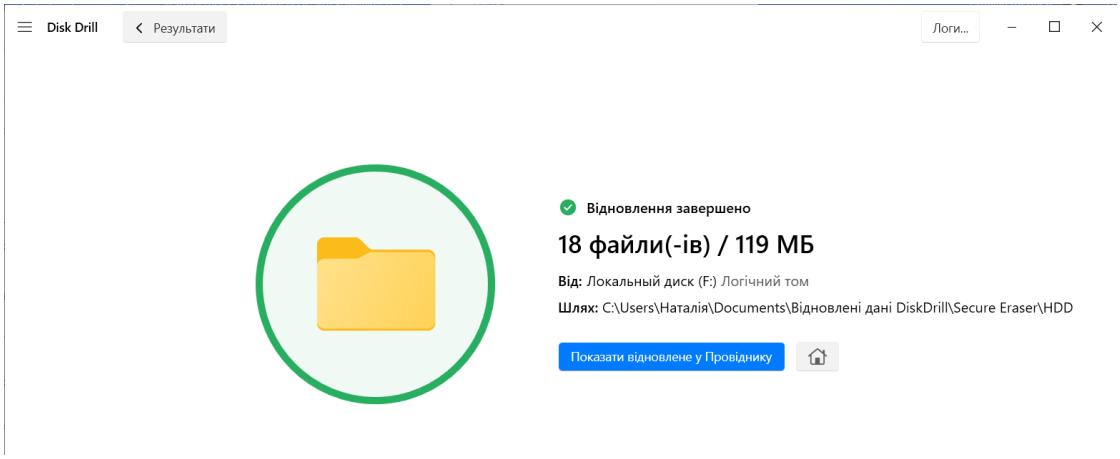

Рисунок Г.9 – Завершення відновлення файлів з HDD-диску після їх знищення програмою “Secure Eraser”

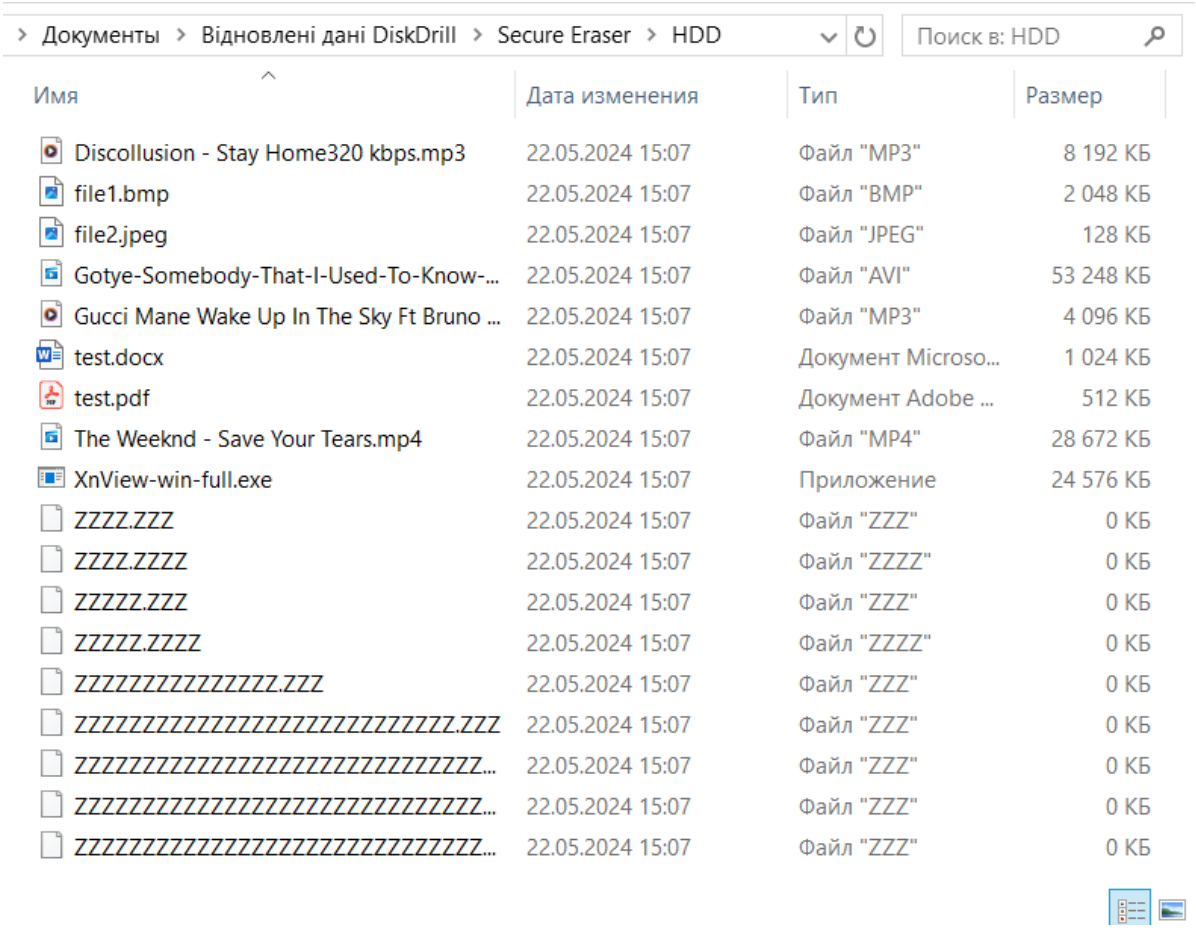

Рисунок Г.10 – Відновлені файли з HDD-диску після їх знищення програмою “Secure Eraser”

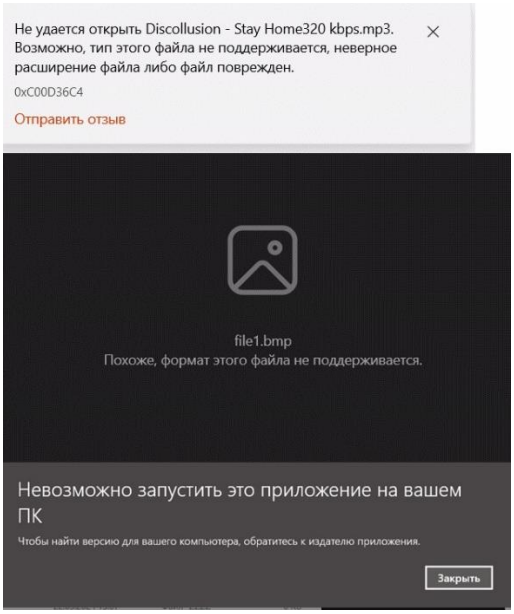

Рисунок Г.11 – Помилки при спробах відкрити відновлені файли

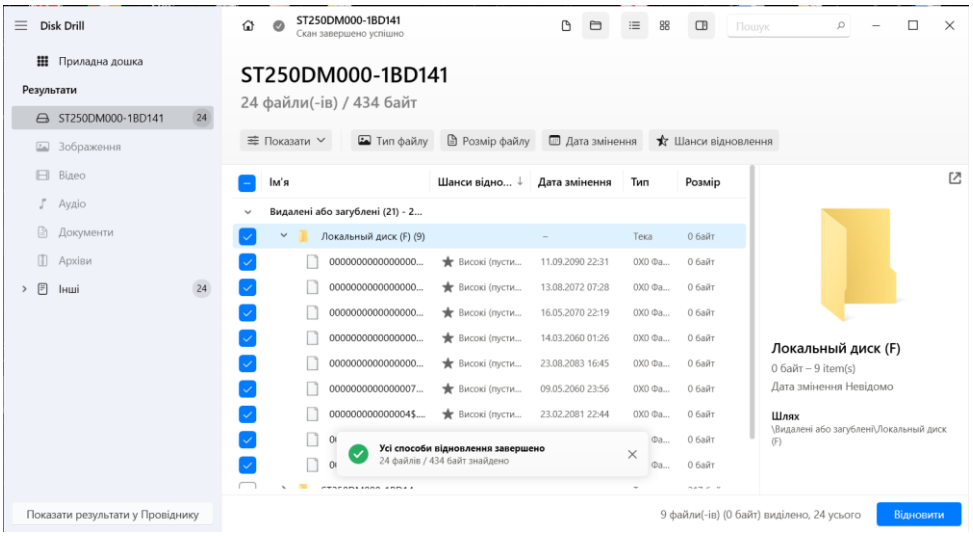

Рисунок Г.12 – Завершення сканування HDD на наявність знищених файлів програмою “PrivaZer”

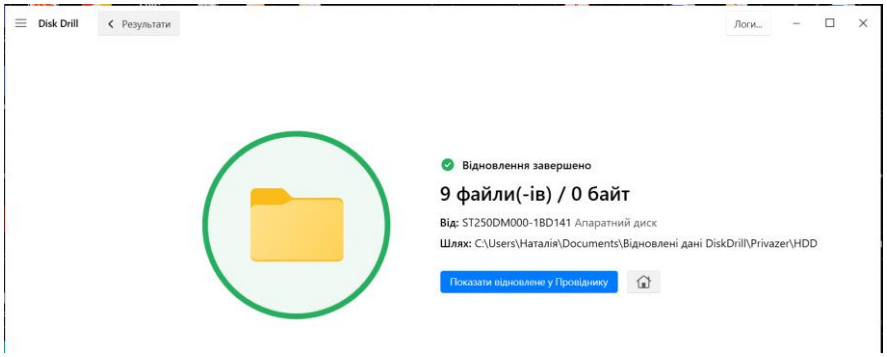

Рисунок Г.13 – Завершення відновлення файлів з HDD після їх знищення програмою “PrivaZer”

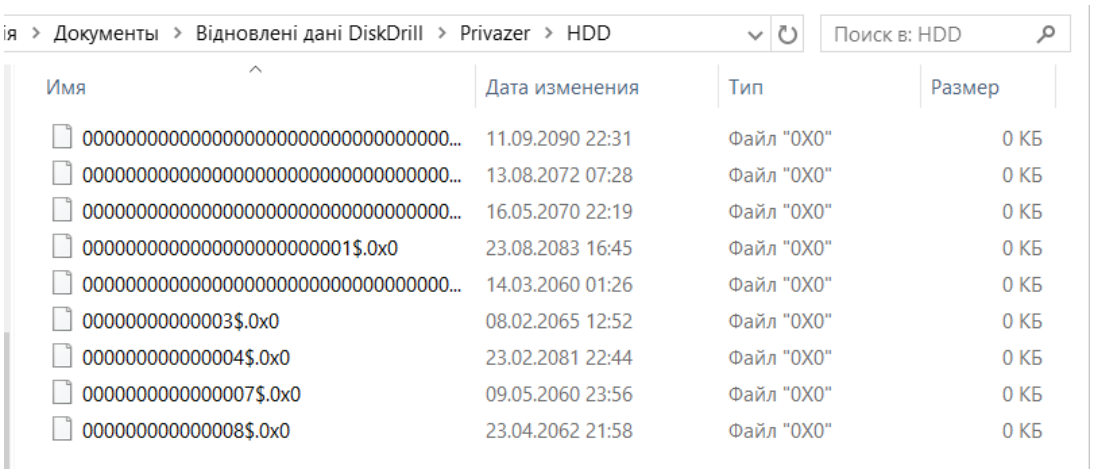

Рисунок Г.14 – Відновлені файли з HDD-диску після їх знищення “PrivaZer”

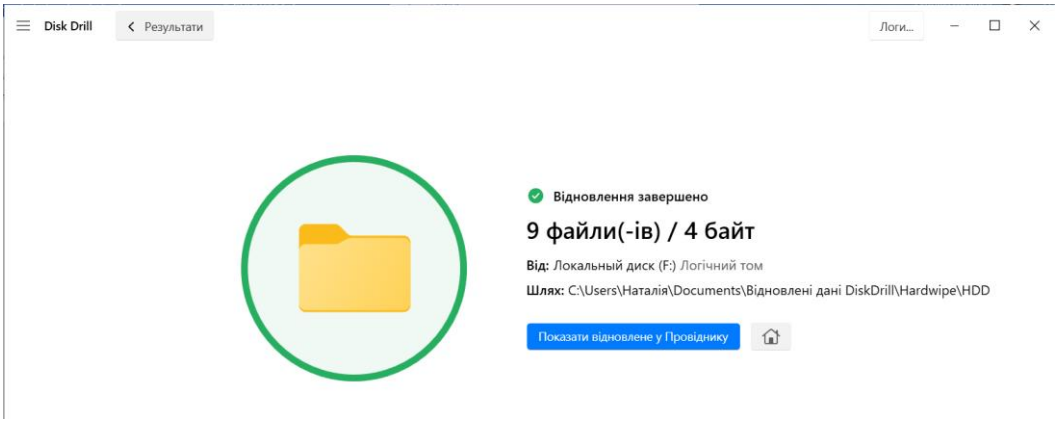

Рисунок Г.15 – Завершення відновлення файлів з HDD-диску після їх знищення програмою “Hardwipe”

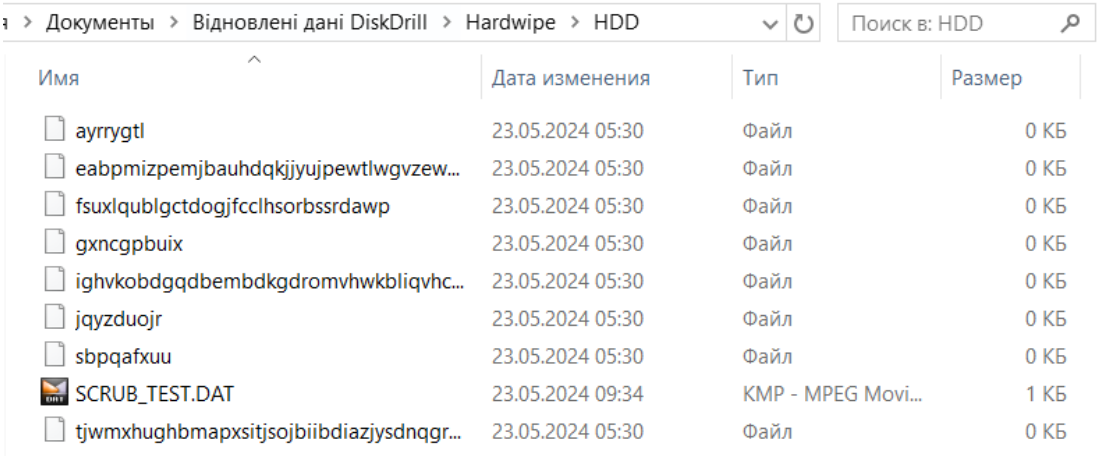

Рисунок Г.16 – Відновлені файлів з HDD-диску після їх знищення програмою “Hardwipe”

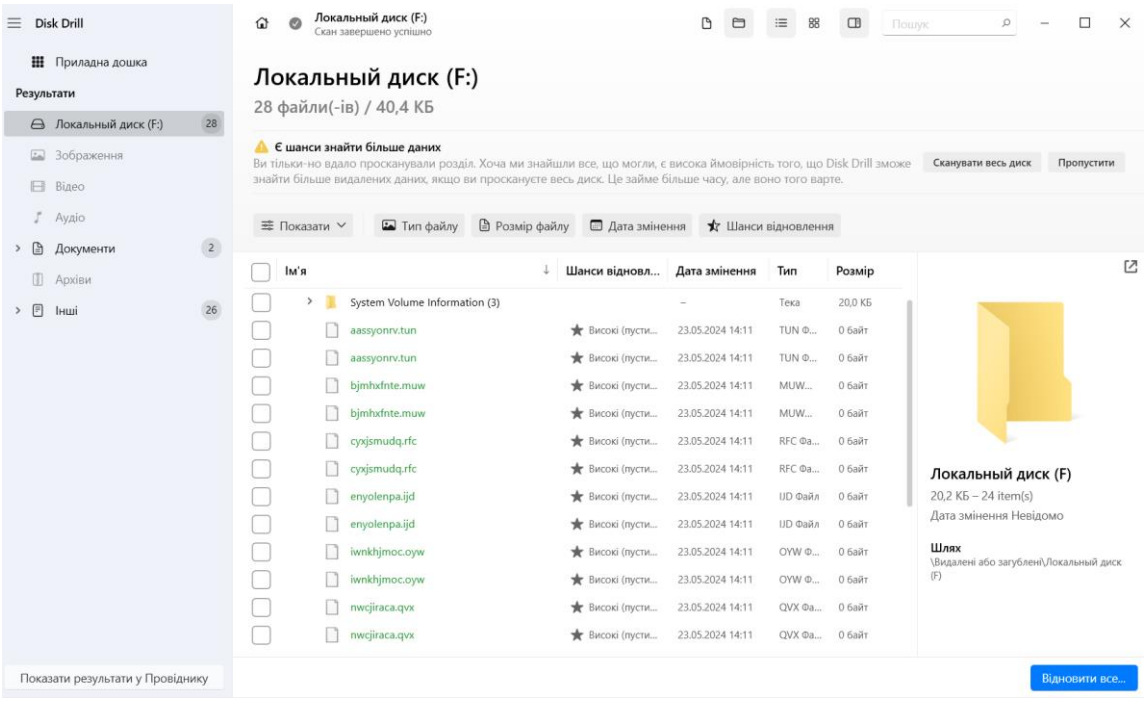

Рисунок Г.17 – Завершення сканування HDD-диску на наявність знищених файлів програмою “BitKiller”

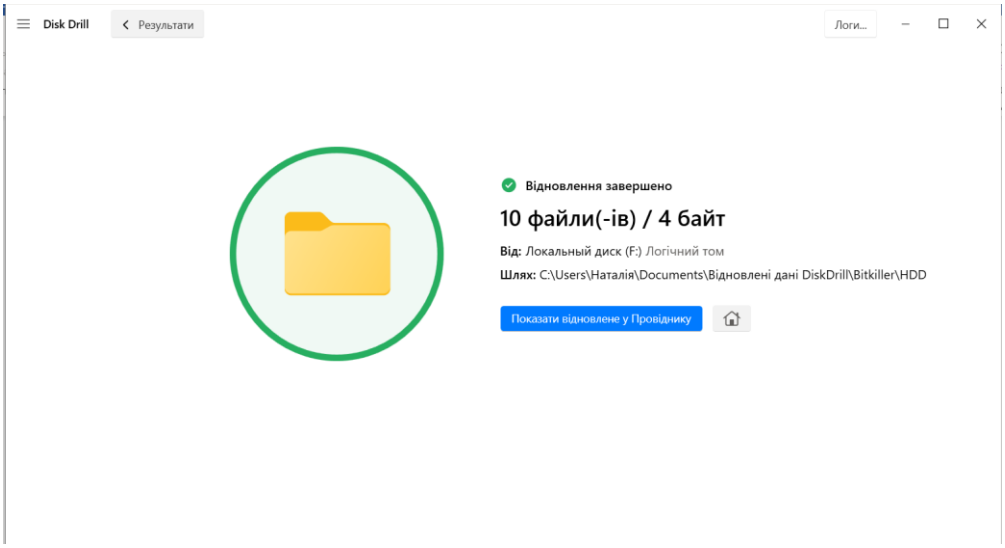

Рисунок Г.18 – Завершення відновлення файлів з HDD-диску після їх знищення програмою “BitKiller”

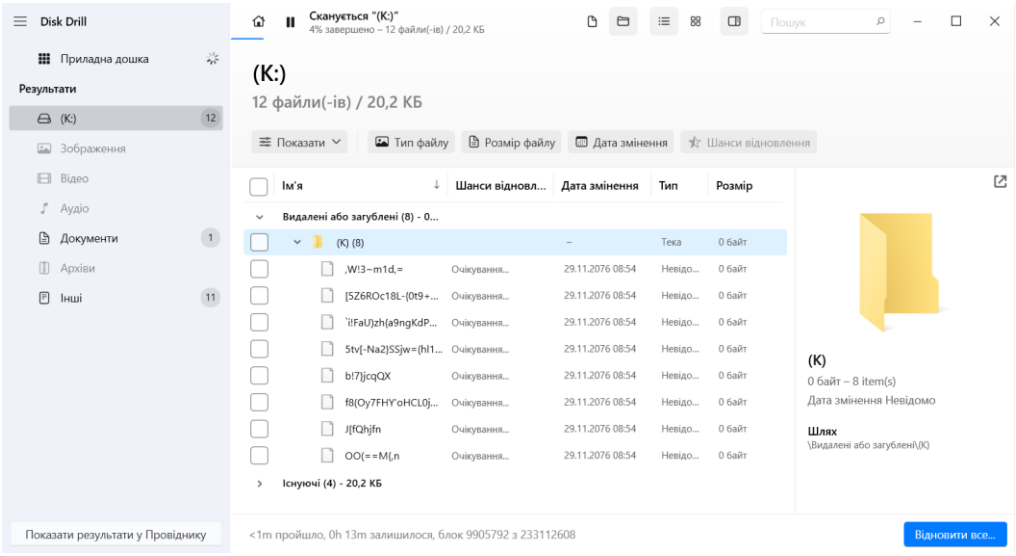

Рисунок Г.19 – Процес сканування SSD-диску на наявність знищених файлів програмою “Eraser”

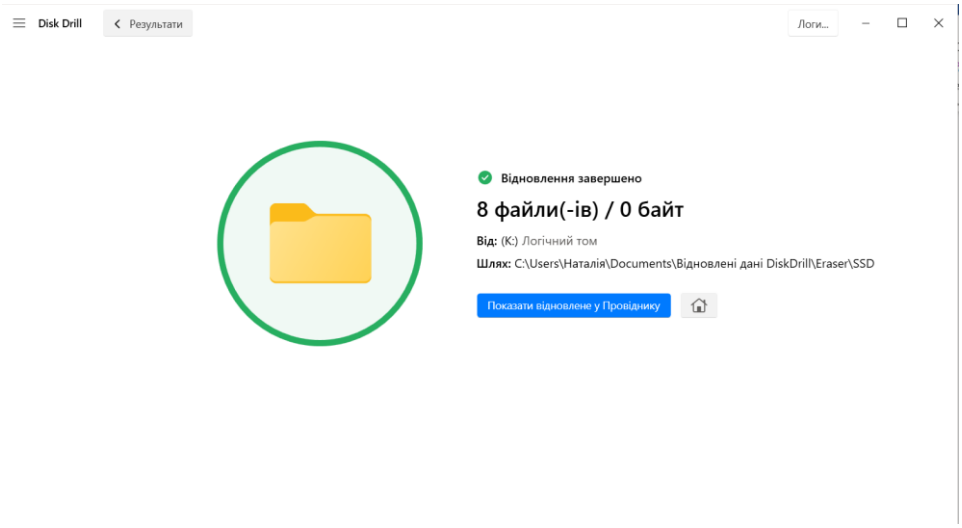

Рисунок Г.20 – Завершення відновлення файлів з SSD-диску після їх знищення програмою “Eraser”

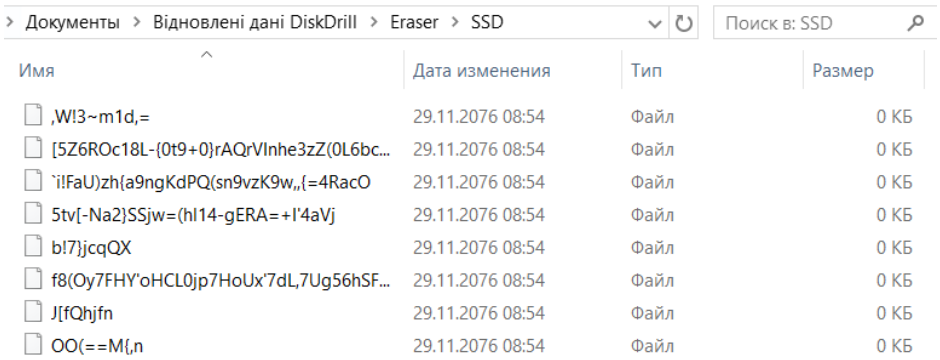

Рисунок Г.21 – Відновлені файли з SSD-диску після їх знищення програмою “Eraser”

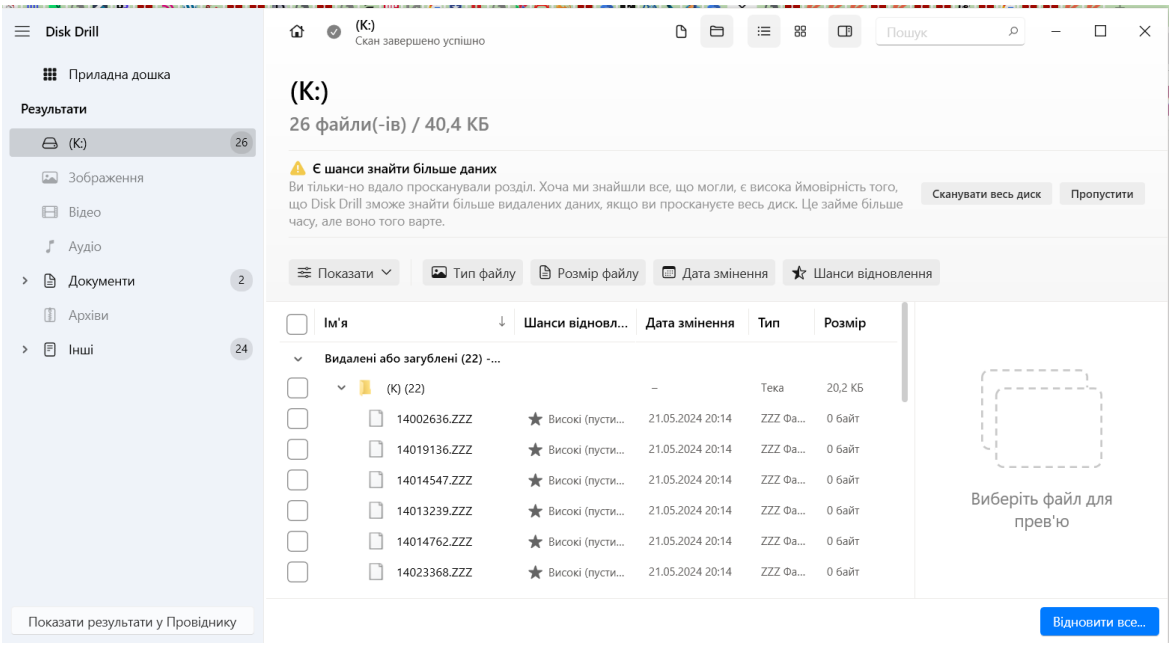

Рисунок Г.22 – Завершення сканування SSD-диску на наявність знищених файлів програмою “File Shredder”

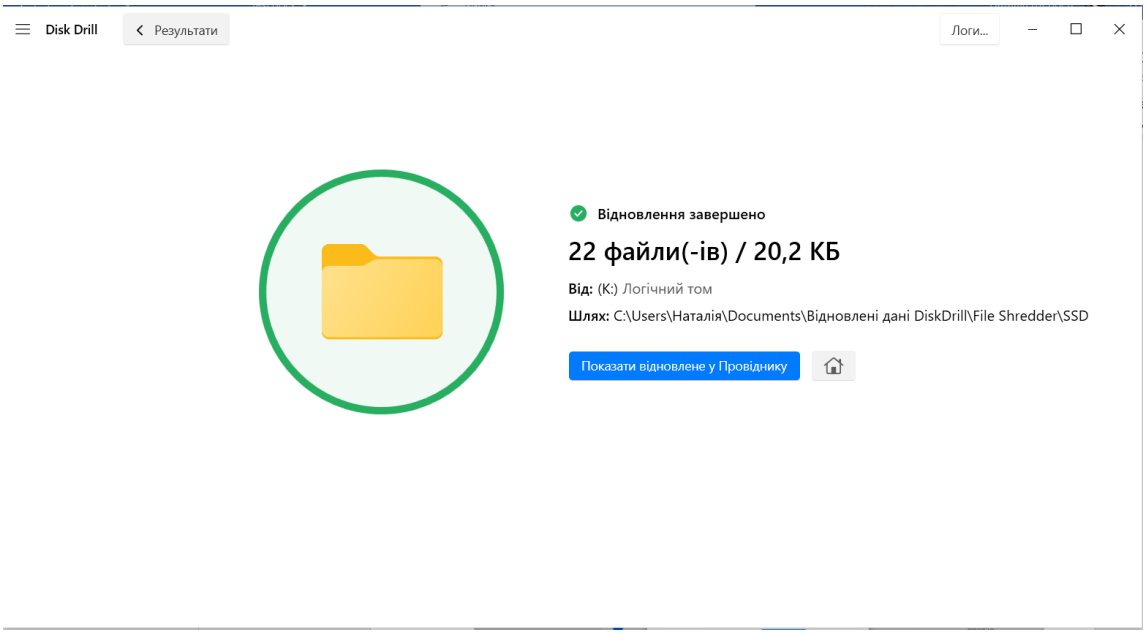

Рисунок Г.23 – Завершення відновлення файлів з SSD-диску після їх знищення програмою “File Shredder”

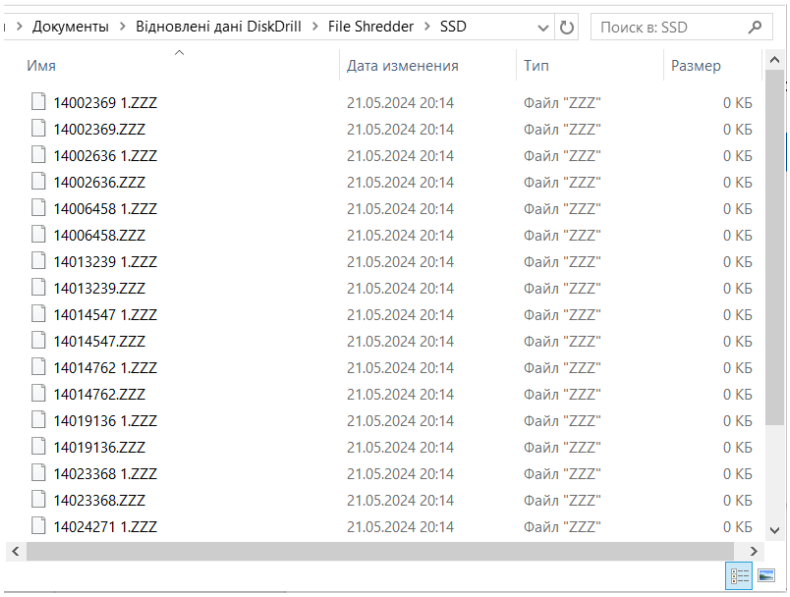

Рисунок Г.24 – Відновлені файли з SSD-диску після їх знищення програмою “File Shredder”

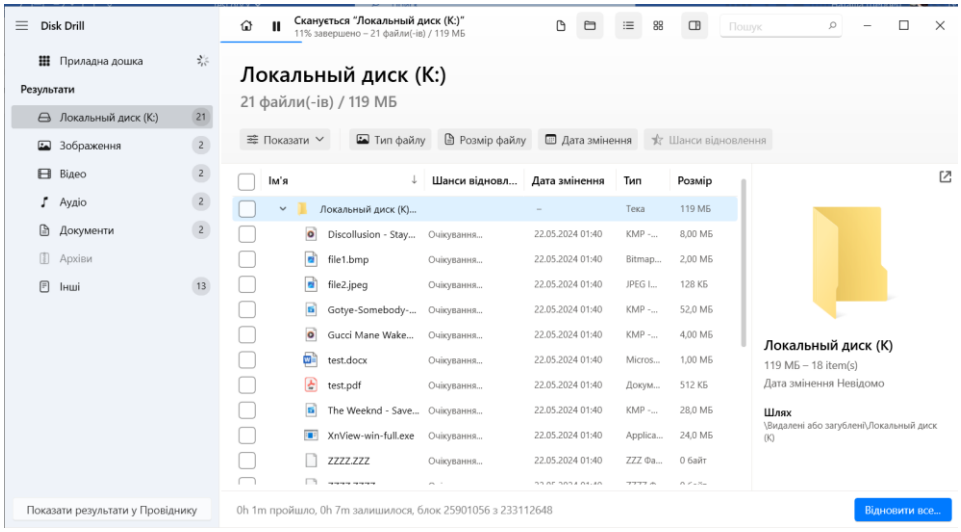

Рисунок Г.25 – Процес сканування SSD-диску на наявність знищених файлів програмою “Secure Eraser”

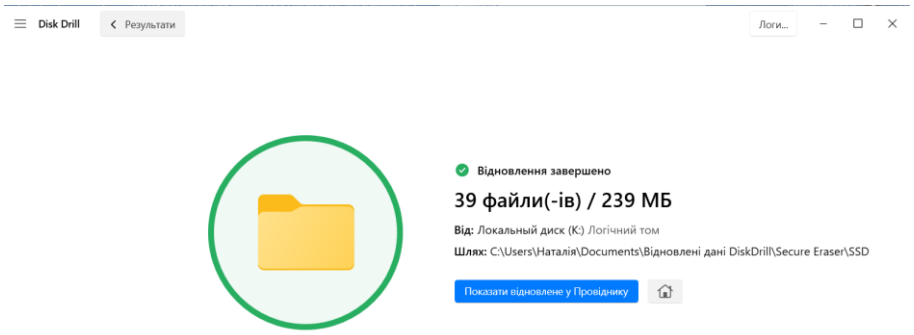

Рисунок Г.26 – Завершення відновлення файлів з SSD-диску після їх знищення програмою “Secure Eraser”

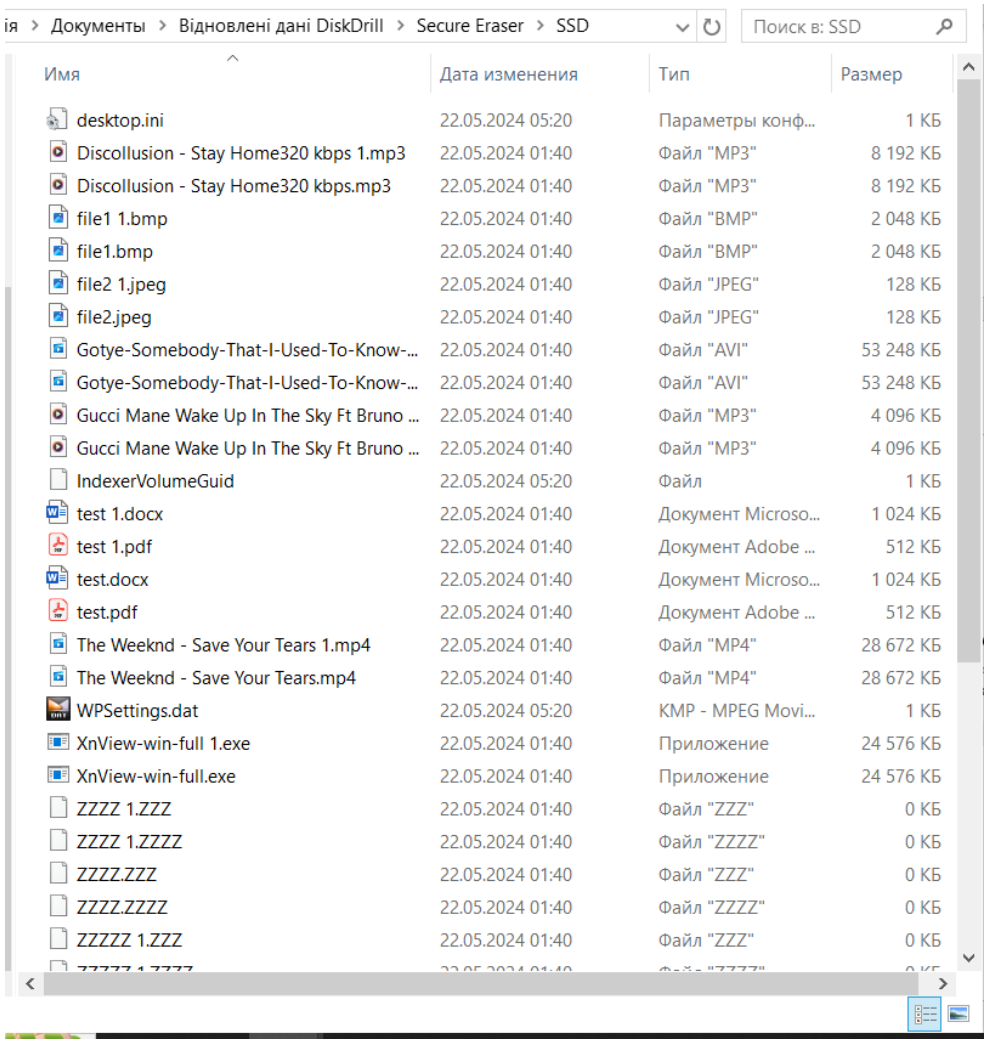

Рисунок Г.27 – Відновлені файли з SSD-диску після їх знищення програмою “Secure Eraser”

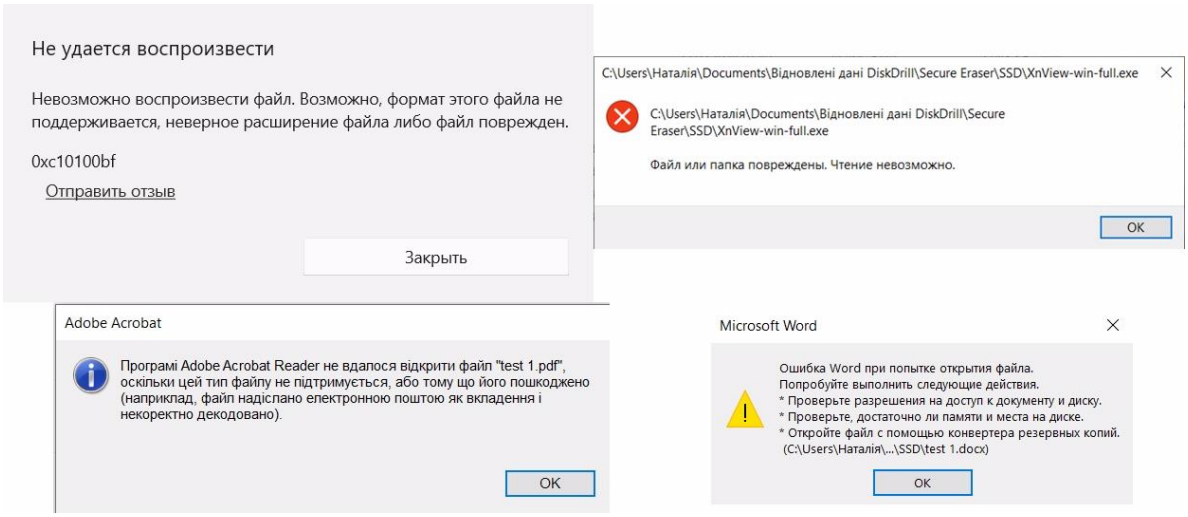

Рисунок Г.28 – Помилки при спробах відкрити відновлені файли

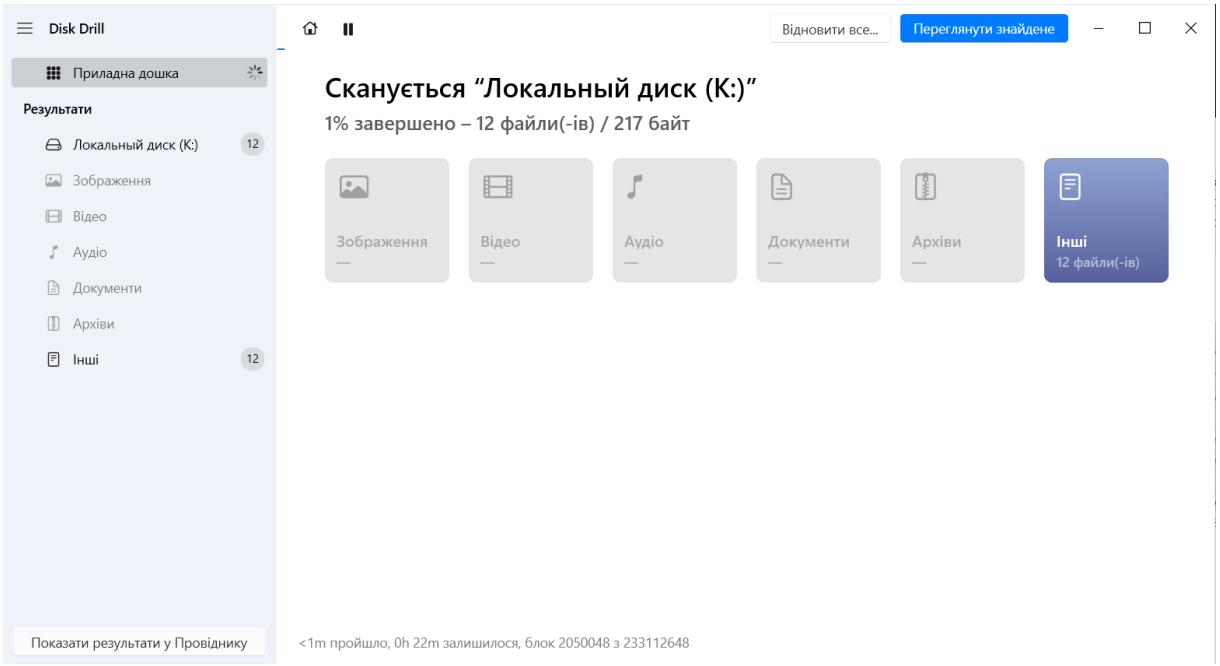

Рисунок Г.29 – Процес сканування SSD-диску на наявність знищених файлів програмою “PrivaZer”

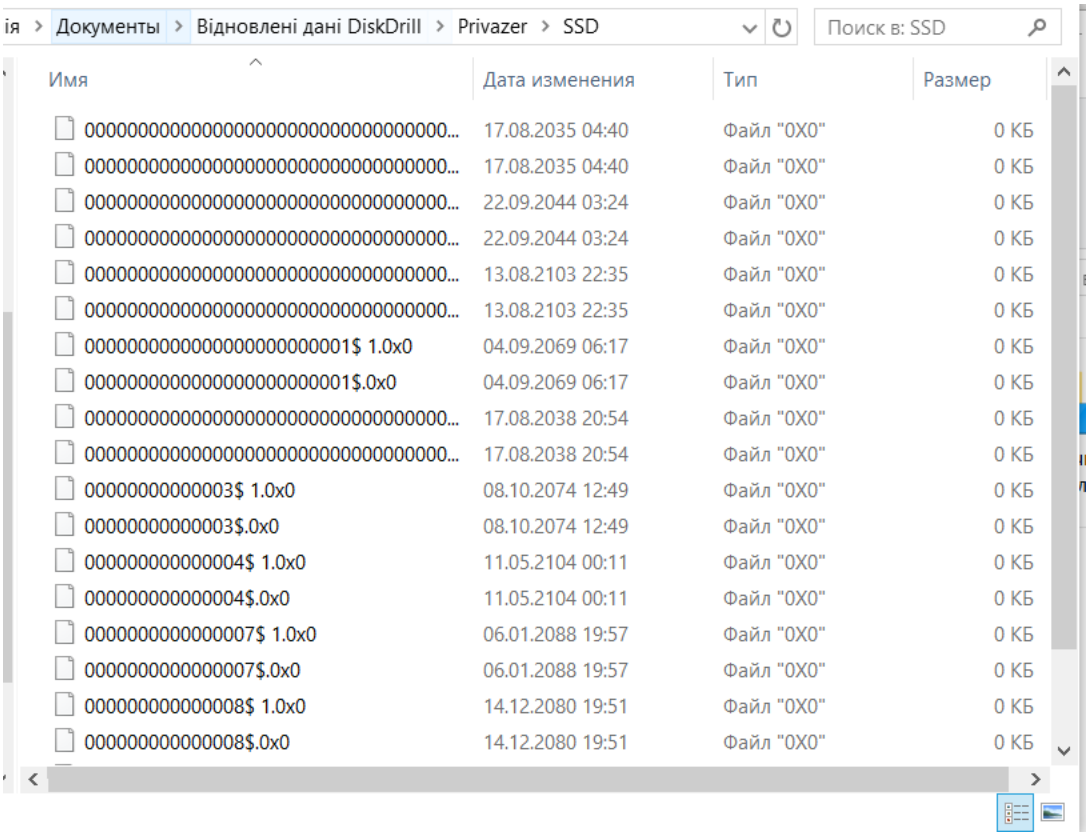

Рисунок Г.30 – Відновлені файли з SSD-диску після їх знищення програмою “PrivaZer”

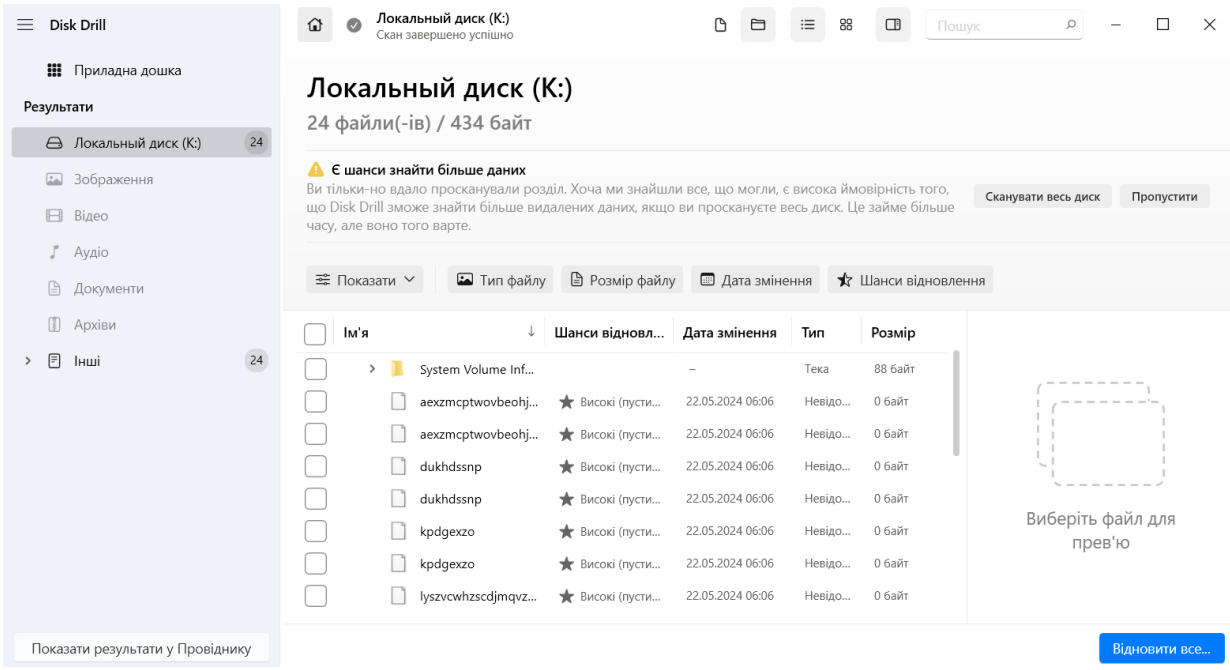

Рисунок Г.31 – Завершення процесу сканування SSD-диску на наявність знищених файлів програмою “Hardwipe”

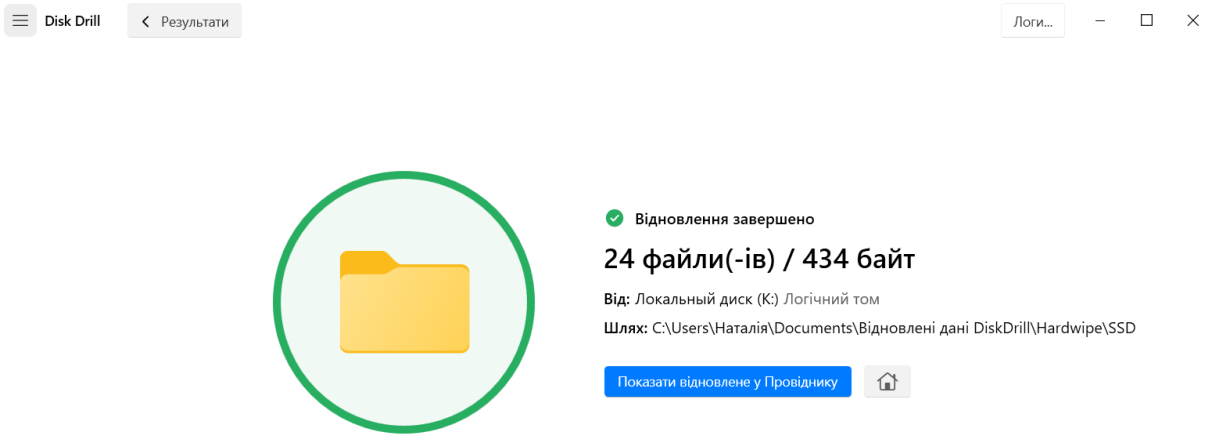

Рисунок Г.32 – Завершення відновлення файлів з SSD-диску після їх знищення програмою “Hardwipe”

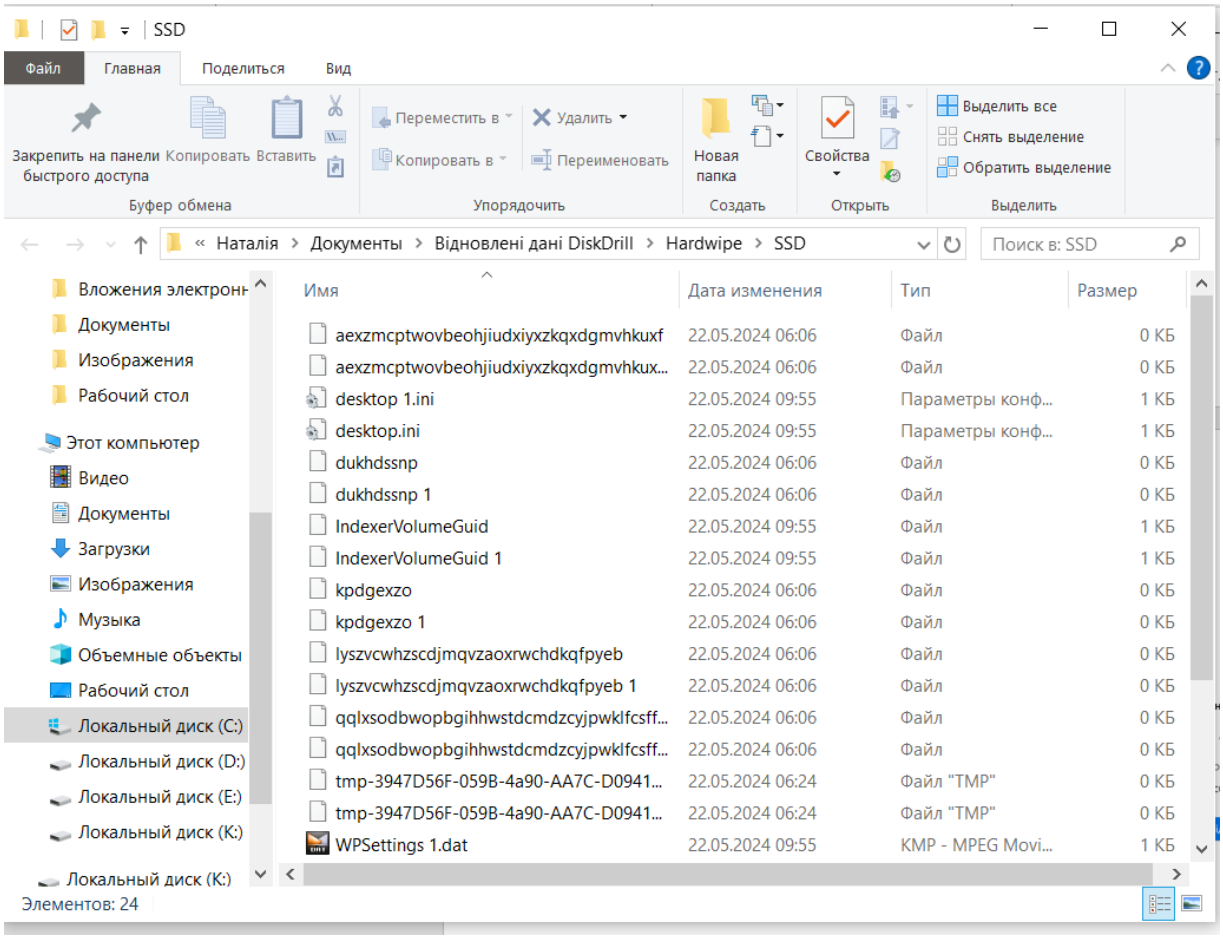

Рисунок Г.33 – Відновлені файли з SSD-диску після їх знищення програмою “Hardwipe”

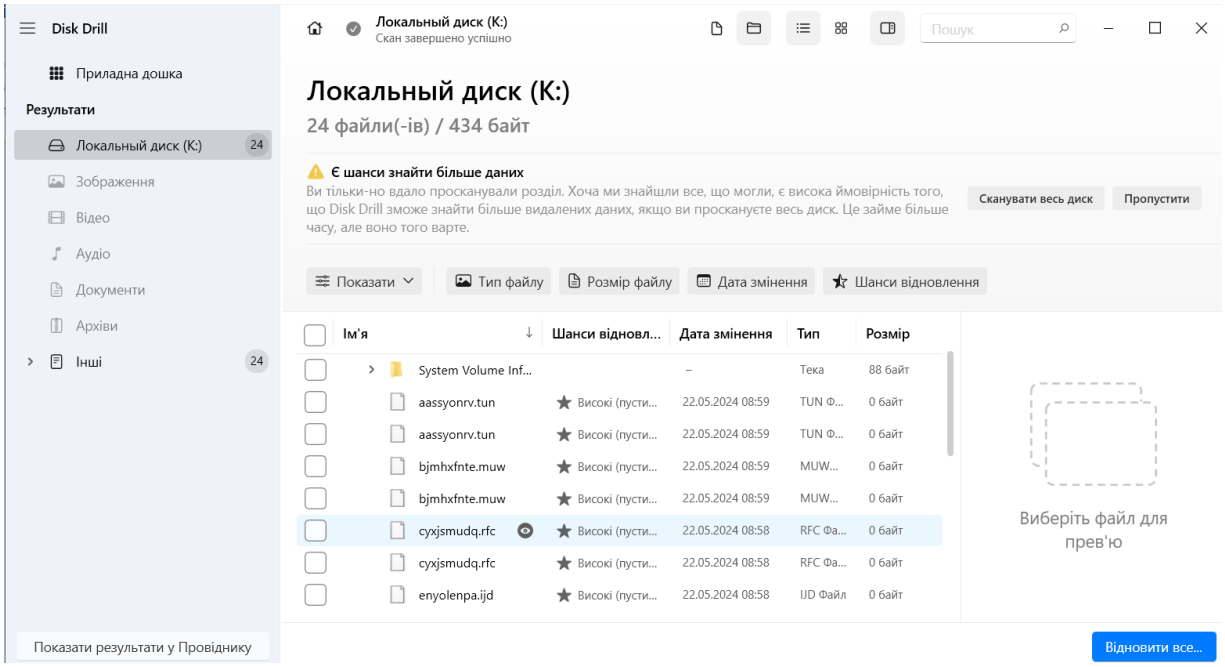

Рисунок Г.34 – Процес сканування SSD-диску на наявність знищених файлів програмою “BitKiller”

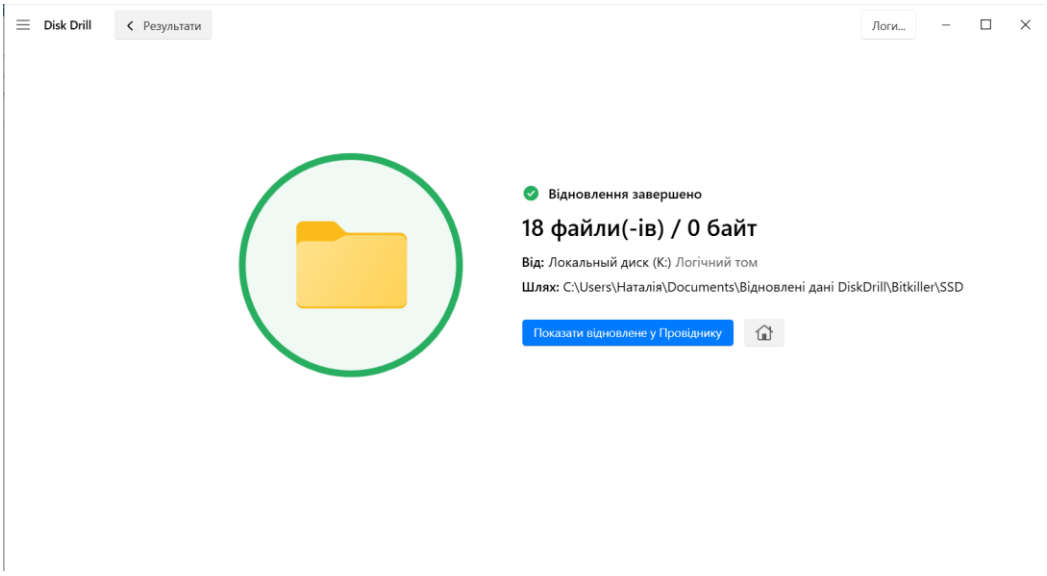

Рисунок Г.35 – Завершення відновлення файлів з SSD-диску після їх знищення програмою “BitKiller”

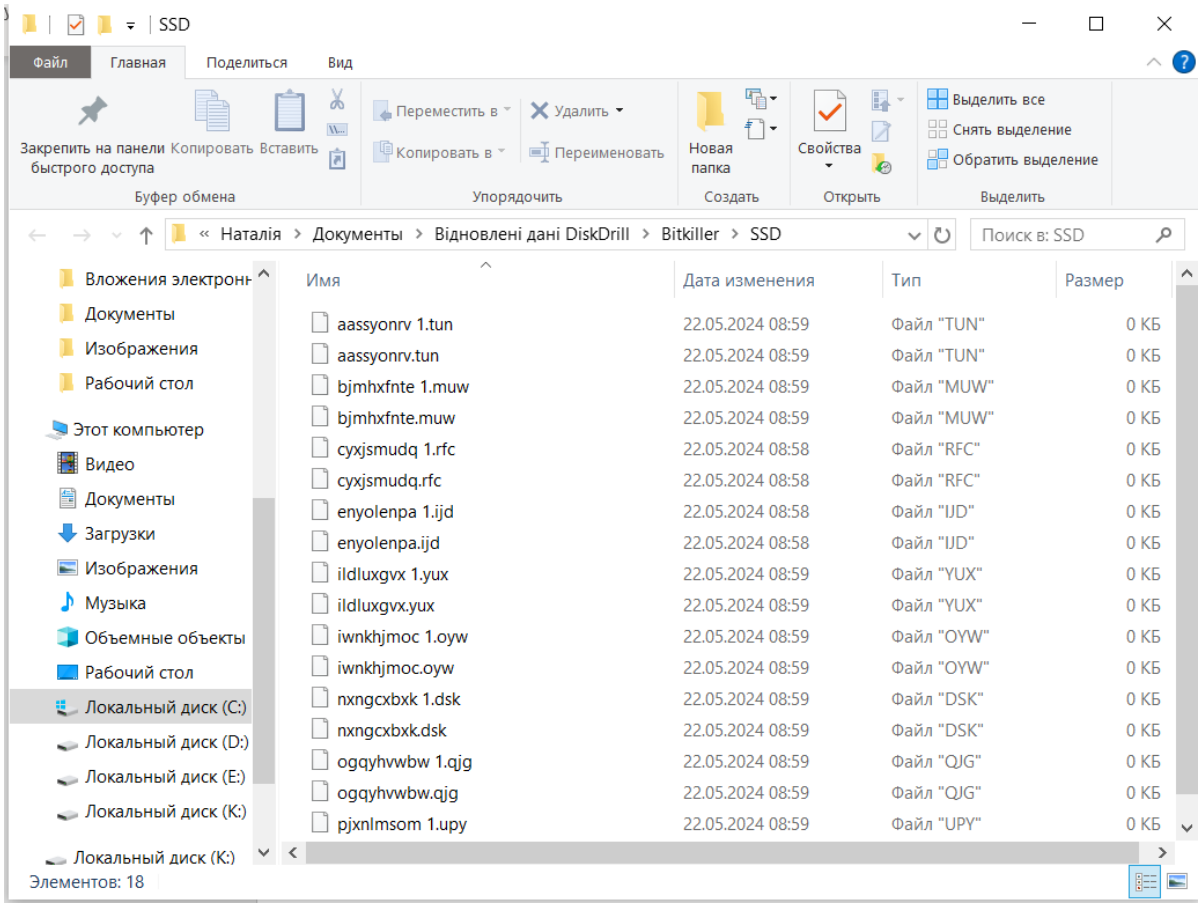

Рисунок Г.36 – Відновлені файли з SSD-диску після їх знищення програмою “BitKiller”