DOI: https://doi.org/10.23939/csn2024.02.172
**УДК 621.3**

# ПРИНЦИПИ ПОБУДОВИ ТА РЕАЛІЗАЦІЇ СИСТЕМИ АВТОМАТИЗОВАНОГО ВИДАЛЕННЯ ТА КОНТРОЛЮ ФАЙЛІВ ДЛЯ OS WINDOWS

***С. В. Павлик, О. Л. Лашко, Д. О. Кушнір***

Національний університет “Львівська політехніка”,
кафедра електронних обчислювальних машин
*E-mail: serhii.pavlyk.mkisp.2024@lpnu.ua, oksana.l.lashko@lpnu.ua, dmytro.o.kushnir@lpnu.ua*



**У статті проводиться дослідження файлової системи на рівні ядра операційної системи. Розглянуто основні проблеми із втратою та захистом персональних даних серед користувачів, та загальні складності при фільтруванні контенту який зберігається на комп’ютері користувачів.**

**Здійснено аналіз, який доводить, що сьогодні все більше персональних даних втрачається, або ж виходить за межі персонального комп’ютера без відома власника. Також, визначено, що велика кількість файлів, які зберігаються на комп’ютері користувачів, є потенційно небезпечними та непотрібними. У статті приділено увагу розробці ефективного програмного рішення для вирішення проблеми із фільтруванням контенту, який зберігається на персональному комп’ютері користувача за допомогою фільтру файлової системи.**

**Метою статті є висвітлення основних аспектів проведеного дослідження та етапів створення програмної системи, яка автоматизовано видаляє небажаний контент та захищає від втрати важливих для користувача даних. Зокрема, така система надає можливість створити правила за якими буде відбуватися фільтрація даних користувача. Крім того, вона дозволяє системним адміністраторам переглядати оброблені статистичні дані про роботу системи для певного користувача, відображає інформацію як про видалені файли, так і про файли, які були створені як резервні копії на віртуальному шифрованому диску.**

**Ключові слова: шифрування, віртуальний диск, C, C++, фільтр файлової системи, DLP.**

## 1. Вступ

У сучасному цифровому світі безпека даних є ключовим аспектом, адже користувачі мають бути впевненими у захищеності своїх даних і контролювати, що відбувається на їх комп’ютері. Одним з важливих інструментів для цього є фільтрування контенту в файловій системі. Це допомагає уникати збереження небажаних тимчасових файлів та захищати конфіденційні дані від несанкціонованого доступу [1].

Фільтрування може відбуватися автоматично або вручну, через встановлення правил, що дозволяє системним адміністраторам контролювати процес створення та обробки файлів. Це також допомагає виявляти і видаляти файли, які створюються шкідливими програмами для збору даних про дії користувача. Наприклад, програма потай від користувача починає накопичувати всі дані про його дії, та в певний час відправляє ці дані на віддалений сервер зі зловмисними діями. Якщо системний адміністратор помітить це перший раз, йому достатньо додати у правила автоматичне видалення файлів формату в якому збираються дані. Такий підхід полегшує роботу та підвищує рівень безпеки.

У даній статті розглянуто процес розробки системи для автоматизованого фільтрування файлової системи користувача на основі встановлених правил. Вона надає можливість налаштовувати фільтрацію контенту через веб-інтерфейс, забезпечуючи автоматичне копіювання важливих файлів на віртуальний шифрований диск із можливістю вибору його розміру та фізичного розташування.

Для небажаного контенту передбачено автоматичне видалення файлів з можливістю налаштування розміру та формату файлів, які підлягатимуть видаленню, а також додавання винятків. Це програмне рішення підвищує безпеку роботи користувача, запобігаючи втраті важливих даних і дозволяючи користувачеві(системним адміністраторам) переглядати список заблокованих файлів для аналізу непотрібного контенту. Запропоновано алгоритм роботи модуля резервного копіювання.

## 2. Огляд літературних джерел

Програми, що накладають обмеження на збереження файлів згідно з певними правилами, зазвичай відносять до категорії програм для запобігання втраті даних (DLP) або рішень для захисту файлів [2].

Аналіз потоку даних для виявлення конфіденційної інформації є складним завданням через численні фактори, що впливають на пошук. Для вирішення цієї проблеми розроблено різні технології, які можна умовно поділити на дві групи: проактивні та реактивні методи.

Проактивні методи базуються на аналізі змісту переданих текстів або документів, наприклад, морфологічний аналіз і регулярні вирази. Вони дозволяють виявляти потенційні витоки конфіденційних даних на основі ключових слів або шаблонів, аналогічно до антивірусного захисту [3].

Реактивні методи, такі як цифрові відбитки і мітки, виявляють витоки на основі властивостей документів або наявності спеціальних маркерів. Ці методи дозволяють реагувати на витоки вже після їхнього виявлення [4].

Фільтр драйвера файлової системи перехоплює спроби створення або відкриття файлів згідно певних правил і блокує їх, якщо їх потрібно видалити. Якщо файл відповідає критеріям резервного копіювання, він передається на драйвер віртуального шифрованого диска для шифрування та збереження.

Алгоритм шифрування критично важливий для безпеки, адже саме від нього залежить чи зможе сторонній користувач отримати доступ до приватних даних власника комп’ютера. У даній програмній системі для шифрування використовується симетричне шифрування XOR, яке базується на операції виключної диз'юнкції (XOR). Для шифрування тексту застосовується гама-послідовність випадкових чисел, яка накладається на вихідний текст. Ця гама використовується як для шифрування, так і для розшифрування даних. Один із способів отримати ключ для шифрування – це повторювати ключове слово до досягнення довжини повідомлення або ж можна згенерувати послідовність псевдовипадкових чисел рівну по довжині тексту повідомлення [5].

Для ефективної розробки драйверів ядра операційної системи Windows потрібно використовувати низькорівневу мову програмування, яка напряму надає доступ до пам’яті – це мова C. Окрім доведеної швидкодії та ефективності даної мови програмування вона є простою у використанні для розробки драйверів ядра. З використанням Windows Driver Kit (WDK) розробленим Майкрософт для створення драйверів ядра для операційної системи Windows розробка стає можливою, проте все ж не тривіальною задачею. Ці API надають функції для керування апаратними перериваннями, доступу до пам’яті та інших критичних операцій необхідних при розробці драйвера ядра [6].

Отже, використання технології фільтру файлової системи для контролю файлової системи користувача на рівні ядра є ефективним та прогресивним методом, який дозволяє відслідковувати кожну операцію відкриття файлів та відповідно забороняти доступ до читання/запису даних несанкціонованим користувачам. Використання проактивного методу для аналізу файлів дозволяє відповідальним особам (системним адміністраторам) налаштувати ефективні правила для видалення небажаного контенту або правила для резервного копіювання важливих персональних даних на машині користувача.

## 3. Постановка задачі

Виходячи з проведеного аналізу, актуальною задачею є розробка та втілення системи автоматизованого видалення та контролю файлів. Система повинна: підтримуватися операційними системами Windows 10 та Windows 11; автоматично видаляти та створювати резервну копію файлів з інтервалом від 1 до 60 хвилин, підтримувати хоча б 10 форматів файлів для сканування, підтримувати сканування файлів розміром від 1 Мб до 100 Мб, автоматично оновлювати правила фільтрування файлів кожні 15 хвилин; мати простий та зрозумілий інтерфейс користувача: створювати 25 віртуальних шифрованих дисків об'ємом від 20 Мб до 256 Мб.

## 4. Структура програмної системи автоматизованого видалення та контролю файлів

Першим кроком при побудові системи автоматизованого приховування та контролю файлів у Windows, є проєктування її структурної схеми. Вона дозволяє окреслити основні компоненти та їх взаємодію а також надає загальне уявлення про систему, допомагаючи розробникам краще зрозуміти її архітектуру та логіку функціонування.

Структурна схема, зображена на рисунку 1, складається з двох частин і включає шість взаємопов'язаних модулів.

- PostgreSQL база даних, що відповідає за зберігання даних користувача, включаючи авторизаційні дані (імейл та пароль), ім'я користувача, аватар, а також конфігурації системи.
- Вебсайт виступає як інтерфейс користувача (UI), дозволяючи налаштовувати правила резервного копіювання та видалення файлів, встановлювати максимальний обсяг для резервного копіювання та видалення, змінювати пароль облікового запису та переглядати статистичні дані.
- HTTP сервер забезпечує зв'язок між хмарною та локальною частинами системи, обробляючи, зберігаючи і передаючи дані між локальним Windows сервісом та хмарним інтерфейсом користувача.
- SHSService.exe — це Windows-сервіс, який отримує від сервера користувацькі конфігурації системи для фільтрування контенту. Він передає ці конфігурації драйверу файлової системи та драйверу віртуального шифрованого диска для реалізації на локальному рівні.
- Windows File Filter Driver обробляє команди відкриття або створення файлів і перевіряє, чи потрібно файл видалити або скопіювати для резервування. Він також отримує команди IOCTL для оновлення конфігурацій та передачі списку файлів, які необхідно видалити або резервно скопіювати.
- Windows Virtual Encrypted Disk Driver керує віртуальними шифрованими дисками. Він створює файли для цих дисків на основі конфігурацій, отриманих від сервісу, і забезпечує шифрування файлів, які копіюються на диски, а також керує всіма операціями з ними.

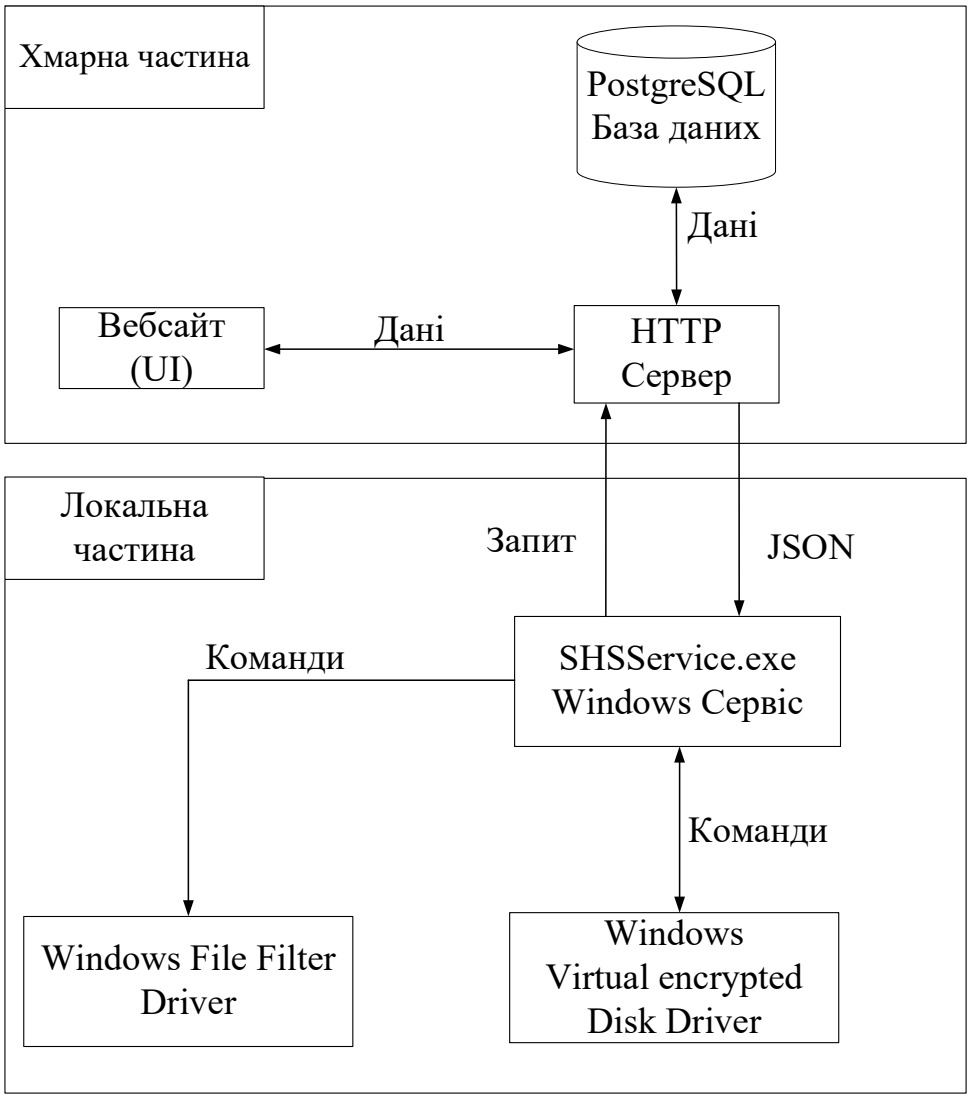


*Рис. 1. Структурна схема системи автоматизованого приховування та контролю файлів.*

### 5. Алгоритм роботи модуля резервного копіювання

На старті, сервіс надсилає запит до HTTP сервера для отримання користувацьких конфігурацій, зокрема налаштувань для резервного копіювання. Далі се'рвіс створює віртуальні диски, звертаючись до віртуального пристрою \Device\Vdisk{number}, який був створений драйвером віртуального диску при його запуску. Сервіс призначає диску відповідну літеру та відправляє команду драйверу для створення або відкриття файлу, який використовуватиметься як віртуальний диск. Після цього диск монтується як логічний диск.

Отримавши підтвердження від драйвера віртуального диску про успішне створення та монтування, сервіс, за необхідності, виконує форматування диску.

Наступний етап – налаштування фільтра файлової системи. Сервіс надсилає драйверу фільтра список розширень файлів, для яких необхідно виконувати резервне копіювання.

Коли всі драйвери налаштовані, сервіс переходить у режим очікування і працює в два потоки: один потік відстежує оновлення конфігурацій, а інший чекає запланованого часу для запуску резервного копіювання.

Процес резервного копіювання, де драйвер віртуального диску відіграє ключову роль, детально описаний в алгоритмі роботи цього модуля, зображеному на рис. 2.

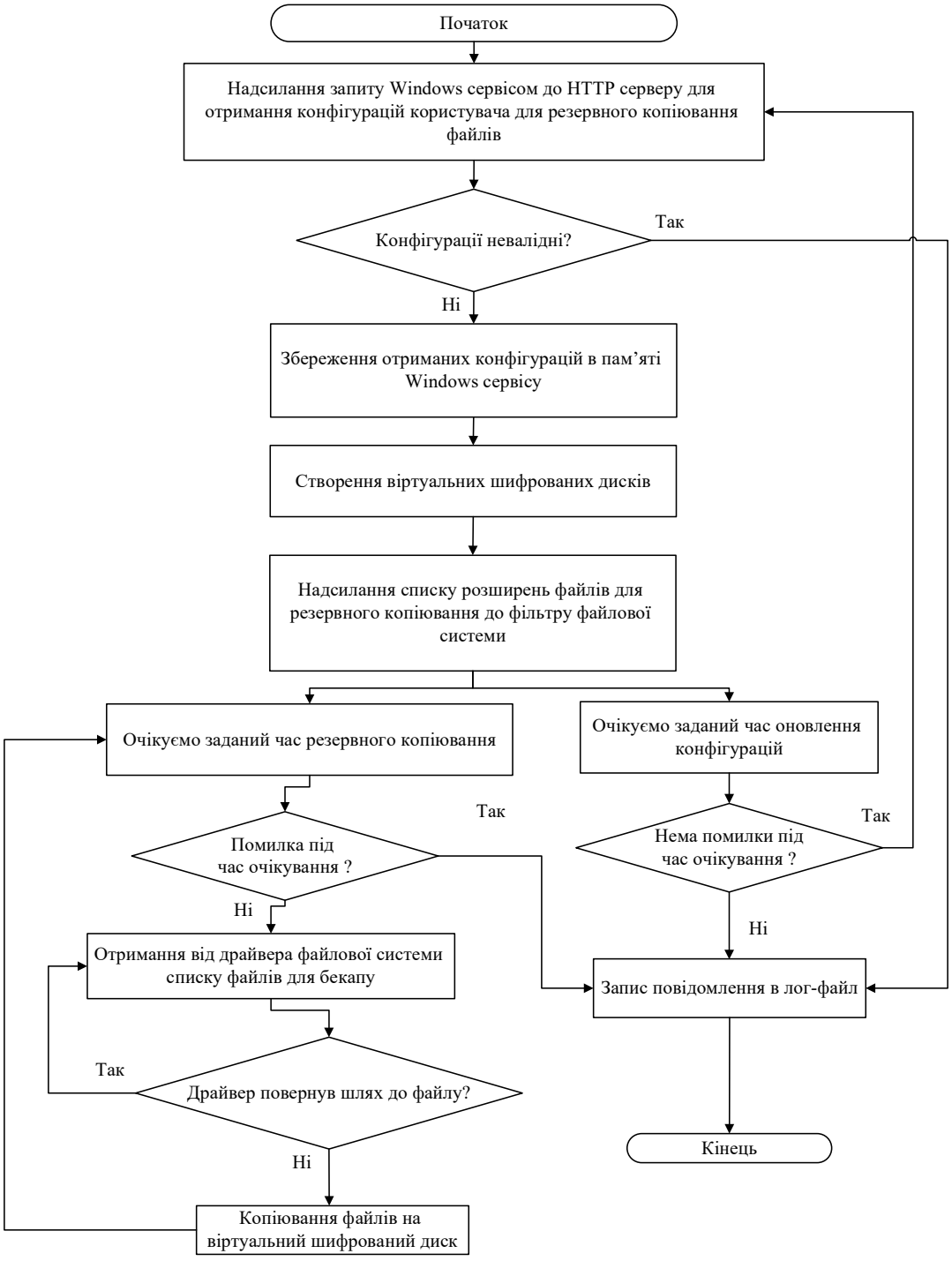


*Рис. 2. Схема алгоритму роботи модуля резервного копіювання.*

## 6. Результати дослідження

Для перевірки працездатності створеної системи, за допомогою графічного інтерфейсу було встановлено правила для максимальної кількості дисків із найбільшими можливими розмірами, як показано на рисунку 3, і ці налаштування успішно збережено. На рисунку 4 видно, що, окрім системних дисків C, D та H, дійсно були створені, змонтовані та відформатовані логічні шифровані диски з об'ємами, які відповідають налаштуванням, заданим на сайті під час створення правил резервного копіювання.

Однак диски D та H не могли бути створені на цій віртуальній машині, оскільки вони існують як фізичні диски. Відповідні повідомлення про помилку створення віртуальних шифрованих дисків було записано в лог-файли.

```
Debug. Failed to mount disk d .Current disk already exist.
Debug. Failed to mount disk h .Current disk already exist.
```

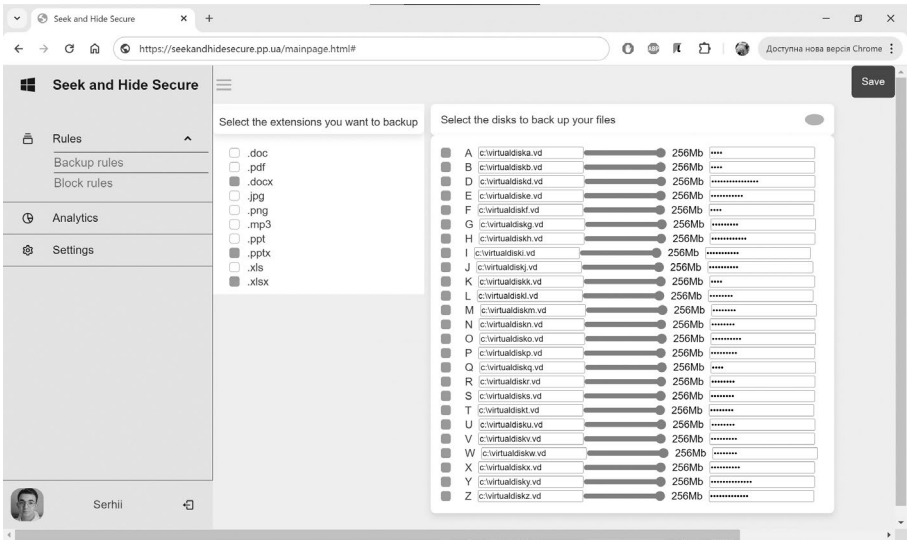


*Рис. 3. Задані конфігурації правил резервного копіювання на максимальні значення.*

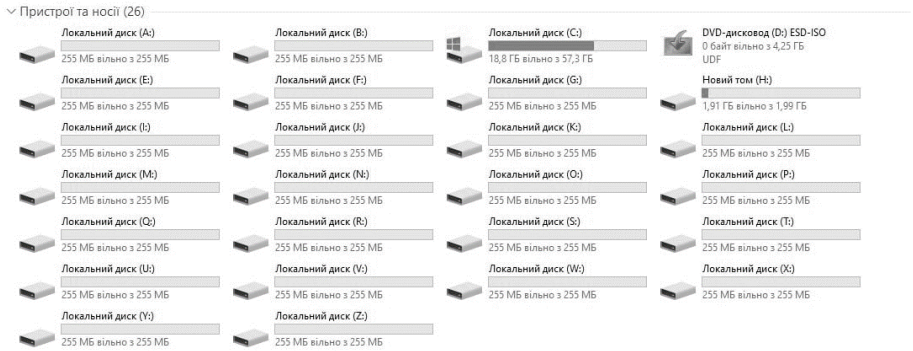


*Рис. 4. Успішно створенні віртуальні шифровані диски та встановленні як логічні диски з заданими максимальними параметрами.*

Для перевірки коректності роботи модуля блокування файлів, виставляю правила блокування на сайті зображені на рисунку 5.

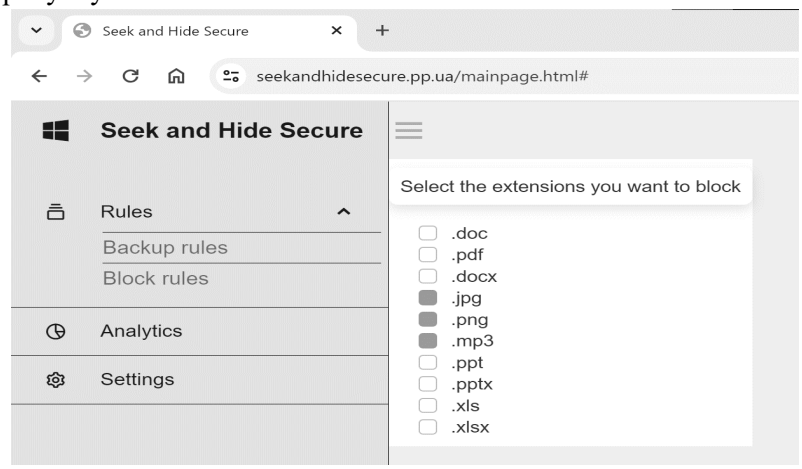


*Рис. 5. Задані конфігурації правил видалення файлів.*

Також створюю три тестові файли: testaudio.mp3, testphoto1.jpg, testimage1.png. Властивості яких зображено на рисунку 6.

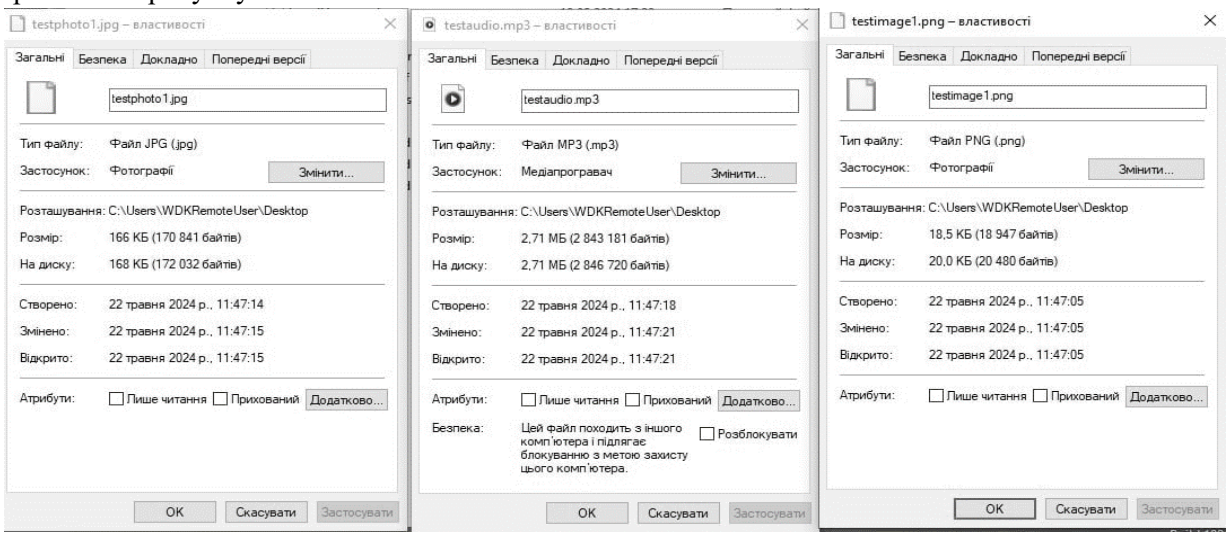


*Рис. 6. Створені тестові файли для перевірки роботи модуля автоматичного видалення файлів.*

Згідно із рисунком 7 через 5 хвилин (стандартний час автоматичного видалення) після створення, файли повинні бути видаленні. Відповідні записи можна знайти в програмі ProcMon, яка показує дії файлової системи в режимі реального часу.

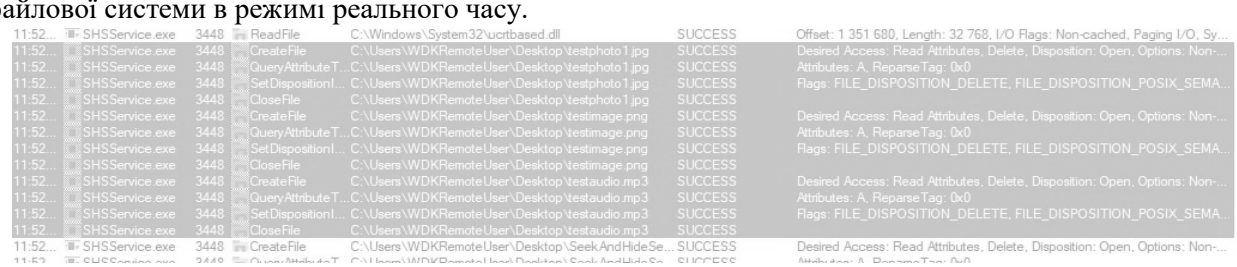


*Рис. 7. Процес видалення сервісом тестових файлів у програмі ProcMon.*

Це доводить коректність роботи модуля автоматичного видалення файлів.

## 7. Висновки

Проведене дослідження в предметній області забезпечення резервного копіювання даних та виявлення даних за допомогою фільтрів файлових систем, показало актуальність розробки системи автоматизованого видалення та контролю файлів для OS WINDOWS. Тому, було створено структурну схему, яка визначила основні компоненти системи та їх взаємодію. Далі, запропоновано та втілено алгоритми резервного копіювання корисних файлів та видалення небажаних.

Результати тестування підтверджують успішну реалізацію системи автоматизованого видалення та контролю файлів для OS Windows.

Розроблена програмна система є рішенням для ефективного автоматизованого контролю файлової системи завдяки швидкодії роботи фільтру файлової системи, який опрацьовує всі операції відкриття або створення файлів та перевіряє файли на відповідність правил встановлених користувачем, що забезпечує високу швидкодію, надійність та ефективність роботи.

Впровадження для користування даного програмного рішення допоможе збільшити безпеку роботи користувача та, водночас, надасть змогу не втратити важливі дані. Також, користувач зможе переглянути список заблокованих файлів, що допоможе в аналізі та обсязі непотрібних файлів зберігалося б на машині користувача, що може бути корисно не лише для самого користувача, а і для системного адміністратора, який зможе провести більш глибокий аналіз отриманої інформації, та, можливо встановити джерело та резонність програми, яка використовує або зберігає небажанні для користувача файли.

**Список літератури**

1. *Tripathi, Manas, and Arunabha Mukhopadhyay. 2020. "Financial Loss Due to a Data Privacy Breach: An Empirical Analysis ." Journal of Organizational Computing and Electronic Commerce 30 (4): 381–400. doi:10.1080/10919392.2020.1818521.*
2. *A. Buda and A. Coleşa, "File System Minifilter Based Data Leakage Prevention System," 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet), Cluj-Napoca, Romania, 2018, pp. 1-6, doi: 10.1109/ROEDUNET.2018.8514147.*
3. *R. Colbaugh and K. Glass, "Proactive defense for evolving cyber threats," Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, Beijing, China, 2011, pp. 125-130, doi: 10.1109/ISI.2011.5984062.*
4. *S. R. Subramanya and B. K. Yi, "Digital signatures," in IEEE Potentials, vol. 25, no. 2, pp. 5-8, March-April 2006, doi: 10.1109/MP.2006.1649003.*
5. *F. Huo and G. Gong, "XOR Encryption Versus Phase Encryption, an In-Depth Analysis," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 4, pp. 903-911, Aug. 2015, doi: 10.1109/TEMC.2015.2390229.*
6. *D. A. Solomon, "The Windows NT kernel architecture," in Computer, vol. 31, no. 10, pp. 40-47, Oct. 1998, doi: 10.1109/2.722284.*

# PRINCIPLES OF DESIGNING AND IMPLEMENTING SYSTEM OF AUTOMATED FILE DELETION AND CONTROL FOR WINDOWS OS

***C. V. Pavlyk, O. L. Lashko, D. O. Kushnir***

Lviv Polytechnic National University,
Department of Electronic Computers
E-mail: serhii.pavlyk.mkisp.2024@lpnu.ua, oksana.l.lashko@lpnu.ua, dmytro.o.kushnir@lpnu.ua



**The article examines the file system at the kernel level of the operating system. It addresses the primary issues related to personal data loss and protection and the general challenges of filtering content stored on users' computers.**

**The analysis reveals that increasing personal data is being lost or leaked from personal computers without users' knowledge. It also shows that many files stored on users' computers are potentially dangerous or unnecessary. The article emphasizes the development of an effective software solution to tackle the issue of filtering content on users' personal computers using a file system filter.**

**The article's objective is to outline the key aspects of the study and the steps involved in creating a software system that automatically removes unwanted content and protects important user data from being lost. Specifically, the system allows creating rules for filtering user data. Additionally, it enables system administrators to review processed system performance statistics for individual users. It displays information about both deleted files and files that have been backed up to a virtual encrypted disk.**

**Keywords: C, C++, DLP, Encryption, File system filter, Virtual disk.**