Павлик С.В., гр. КІСП-21
Науковий керівник – д.ф., доцент Кушнір Д.О.

Принципи побудови та реалізації системи автоматизованого видалення та контролю файлів для OS Windows

Стан проблеми. 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.

Програми, що накладають обмеження на збереження файлів згідно з певними правилами, зазвичай відносять до категорії програм для запобігання втраті даних (DLP) [1].

Аналіз потоку даних для виявлення конфіденційної інформації є складним завданням через численні фактори, що впливають на пошук. Для вирішення цієї проблеми розроблено проактивні методи [2].

Використання технології фільтру файлової системи [3] для контролю користувацької файлової системи на рівні ядра є ефективним підходом, що забезпечує відстеження всіх операцій відкриття файлів і запобігає несанкціонованому доступу до даних.

Постановка задачі. Актуальною задачею є розробка та втілення системи автоматизованого видалення та контролю файлів. Розробити структурну схему системи схему алгоритму роботи модуля резервного копіювання.

Розв'язання задачі.

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, складається з двох частин і включає шість взаємопов'язаних модулів:

- PostgreSQL база даних, що відповідає за зберігання даних користувача та конфігурації системи.
- Вебсайт виступає як інтерфейс користувача (UI), дозволяючи налаштовувати конфігурації системи.
- HTTP сервер з'єднує хмарну та локальну частини системи.
- Windows-сервіс отримує від сервера користувацькі конфігурації системи фільтрації контенту та передає їх драйверу файлової системи й драйверу віртуального шифрованого диска для реалізації на локальному рівні.
- Windows File Filter Driver обробляє операції створення та відкриття файлів, визначаючи необхідність їх видалення або копіювання для резервного збереження.

• Windows Virtual Encrypted Disk Driver керує віртуальними шифрованими дисками: створює відповідні файлові образи згідно з отриманими конфігураціями, забезпечує шифрування даних, що копіюються, та виконує всі операції з цими дисками.

Після отримання користувацьких конфігурацій, сервіс створює віртуальні диски, звертаючись до віртуального пристрою, який був створений драйвером віртуального диску при його запуску. Далі, 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. Після чого сервіс, за необхідності, виконує форматування диску.

Коли всі драйвери налаштовані, сервіс переходить у режим очікування і працює в два потоки: один потік відстежує оновлення конфігурацій, а інший виконує резервне копіювання.

У результаті тестування підтверджено високу швидкодію розробленої системи. Наукова новизна полягає у ефективності роботи системи, що забезпечується використанням фільтра файлової системи на рівні ядра, що дозволяє виявляти та передавати файли на обробку зі швидкістю до 1 секунди.

Під час експерименту фільтр зафіксував операцію створення файлу із затримкою 0.004 секунд та передав його на проактивний аналіз щодо відповідності критеріям видалення або резервного копіювання. За результатами аналізу файл був класифікований як такий, що підлягає видаленню, і видалений системою через 0.582 секунд.

Таким чином, загальний час обробки одного тестового файлу становив 0.586 с., що менше за максимальний заявлений показник у 1 с.

Висновки. У роботі розроблено програмну систему для автоматизованого контролю файлової системи, що забезпечує високу швидкодію завдяки фільтру, який обробляє всі операції створення та відкриття файлів. Розроблена система може бути використана як складова загальної системи захисту даних працівників або слугувати основою для її подальшої розробки та розширення.

Література.

[1] 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.

[2] 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

[3] D. A. Solomon, "The Windows NT kernel architecture," in Computer, vol. 31, no. 10, pp. 40-47, Oct. 1998, doi:

10.1109/2.722284.