УДК 004.8:004.056.5:004.9

ГІБРИДНА АНТИВІРУСНА СИСТЕМА З МОДУЛЬНОЮ АРХІТЕКТУРОЮ ДЛЯ СУЧАСНИХ КОМП'ЮТЕРИЗОВАНИХ СЕРЕДОВИЩ

Даниїл КАШУБА[1] Ростислав ТКАЧУК[1,2], Орест ПОЛОТАЙ [1,2]
[1]Львівський державний університет безпеки життєдіяльності
[2]Національний університет «Львівська політехніка»

У роботі розглянуто сучасні підходи до забезпечення інформаційної безпеки комп'ютеризованих систем та обґрунтовано доцільність створення гібридної антивірусної системи з модульною архітектурою. Проаналізовано ефективність сигнатурного, евристичного та поведінкового аналізу, а також застосування математичних моделей для детекції шкідливого програмного забезпечення. Розроблено антивірусне ПЗ із високопродуктивним ядром на C++ та графічним інтерфейсом на C# / WPF, що забезпечує багаторівневий захист, модульність, масштабованість та можливість інтеграції з іншими застосунками. Описано технічну реалізацію, включно з використанням SQLite, OpenSSL та механізмів багатопоточності, а також експортовані функції ядра для інтеграції та розширення системи.

Ключові слова: *інформаційна безпека, антивірусна система, гібридний аналіз, сигнатурний аналіз, поведінковий аналіз, модульна архітектура, C++, C# / WPF, шкідливе ПЗ, Zero-Day загрози, SQLite, OpenSSL.*

The paper considers modern approaches to ensuring information security of computerized systems and justifies the feasibility of creating a hybrid antivirus system with a modular architecture. The effectiveness of signature, heuristic and behavioral analysis, as well as the use of mathematical models for detecting malicious software, is analyzed. Antivirus software with a high-performance C++ kernel and a C# / WPF graphical interface is developed, which provides multi-level protection, modularity, scalability and the ability to integrate with other applications. The technical implementation is described, including the use of SQLite, OpenSSL and multi-threading mechanisms, as well as exported kernel functions for system integration and expansion.

Keywords: *information security, antivirus system, hybrid analysis, signature analysis, behavioral analysis, modular architecture, C++, C# / WPF, malware, Zero-Day threats, SQLite, OpenSSL.*

Інформаційна безпека є критичним фактором стабільного функціонування сучасних комп'ютеризованих систем. Щодня фіксуються тисячі нових шкідливих програм, здатних викрадати дані, порушувати роботу операційних систем або атакувати інфраструктуру. Традиційні сигнатурні антивіруси часто виявляються неефективними проти нових та модифікованих загроз. Практичним прикладом є атака вірусу-вимагача у 2023 році, що уразила понад 50 000 робочих станцій у підприємствах Європи, незважаючи на наявність стандартних антивірусних програм [1].

Сучасні дослідження підкреслюють важливість гібридних рішень, що поєднують сигнатурний та поведінковий аналіз. Такий підхід дозволяє

не лише перевіряти хеші файлів, а й виявляти аномальні процеси в режимі реального часу, підвищуючи ефективність захисту. Розробка власного антивірусного ядра з прозорою архітектурою сприяє глибшому розумінню принципів роботи захисного ПЗ, що важливо як у наукових, так і в освітніх проєктах [2].

Аналіз сучасних антивірусних рішень показав, що комерційні системи забезпечують високу точність і багаторівневий захист, проте є закритими, ресурсомісткими та малопридатними для кастомізації. Відкриті рішення, такі як ClamAV, забезпечують гнучкість та інтегровуваність, але потребують доопрацювання для реалізації сучасних функцій, зокрема поведінкового аналізу. Порівняння методів детекції виявило, що сигнатурний підхід ефективний для відомих загроз, евристичні методи здатні виявляти нові загрози, проте характеризуються високим рівнем хибнопозитивів, а поведінковий аналіз є найбільш перспективним для виявлення Zero-Day загроз, хоча потребує значних обчислювальних ресурсів. Математичні моделі — автоматні, статистичні, логічні та ML-моделі — демонструють ефективність лише при комплексному застосуванні [3].

Створення антивірусного ПЗ вимагає поєднання високопродуктивного системного ядра та зручного користувацького інтерфейсу, при цьому компоненти мають бути модульними, безпечними, масштабованими та придатними до подальшого розвитку [2]. Основна проблема полягає у виборі таких засобів розробки й архітектури, які одночасно забезпечать:

– доступ до низькорівневих функцій ОС для поведінкового та сигнатурного аналізу;

– високу швидкодію та оптимізацію;

– безпечний та сучасний графічний інтерфейс;

– легкість оновлення, розширення та інтеграції;

– відповідність вимогам реальних середовищ Windows.

Враховуючи ці обмеження, доцільним є створення гібридної антивірусної системи з модульною архітектурою, що поєднує сигнатурний та поведінковий аналіз з можливістю подальшого розширення евристичними та ML-методами. Такий підхід забезпечує оптимальний баланс між точністю, швидкодією, масштабованістю та адаптивністю до нових загроз [4, 5].

Для реалізації високопродуктивного ядра обрано мову C++ з доступом до низькорівневих механізмів Windows та підтримкою багатопоточності. Графічний інтерфейс створено на C# / WPF, що забезпечує інтеграцію з .NET, сучасну UI-архітектуру та легкість підтримки. Система побудована за трирівневою архітектурою (ядро — інтеграційний рівень — інтерфейс), що гарантує модульність, масштабованість і незалежність компонентів. Використані інструменти (Visual Studio 2022, MSVC, NuGet) та бібліотеки (SQLite, OpenSSL, WinAPI, WPF) забезпечують безпечну, продуктивну та керовану розробку, а апаратні вимоги відповідають типовому обладнанню Windows [6, 7].

Антивірусне ПЗ реалізовано на основі багаторівневої модульної архітектури, що розмежовує функції аналізу загроз, керування даними та

взаємодії з користувачем. Основу системи становить високопродуктивне ядро як динамічна бібліотека C++, що виконує сигнатурний та поведінковий аналіз, працює з локальною базою сигнатур і формує результати перевірки. Інтеграція з .NET-клієнтом здійснюється через C++/CLI або P/Invoke, поєднуючи native-продуктивність з керованою логікою та WPF-інтерфейсом.

Інтерфейс користувача реалізовано за шаблоном MVVM, що забезпечує ізоляцію бізнес-логіки та уніфіковане оновлення даних. Кожен функціональний компонент оформлений як окремий модуль із власною ViewModel, а стилі та ресурси структуруються у словниках для єдності дизайну. Сигнатурна база на SQLite завантажується в оперативну пам'ять для забезпечення O(1) перевірки хешів, а сигнатурний аналіз здійснюється за алгоритмами SHA-256 та MD5 (OpenSSL). Поведінковий модуль моніторить процеси та порівнює їх зі списком ризикових шаблонів, а фонове виконання й атомарні структури гарантують коректність багатопотокових операцій.

Ядро надає експортовані функції (ScanDirectory, IsFileMalicious) для інтеграції в інші застосунки та автоматичної інсталяції через NuGet-пакет, що забезпечує масштабованість, розширюваність і можливість подальшої інтеграції з хмарними сервісами аналізу шкідливих файлів.

Література

1. CISA. Cyberattack Against MGM Resorts [Електронний ресурс] // U.S. Cybersecurity and Infrastructure Security Agency (CISA), 2023. — Режим доступу: https://www.cisa.gov/news-events/alerts/aa23-239a

2. Філіпчук Б., Ткачук Р. Л. Захист персонального комп'ютера від шкідливого програмного забезпечення. Актуальні проблеми пожежної безпеки та запобігання надзвичайним ситуаціям в умовах сьогодення : зб. тез доповідей Всеукраїнської науково-практичної конференції з міжнародною участю (Львів, 25 жовтня 2022 р.). Львів : ЛДУБЖД, 2022. С. 478–481.

3. Боднар О., Ткачук Р. Л. Тактика моделей cyber kill chain і unified kill chain: розкриття анатомії кібератак. Інформаційна безпека та інформаційні технології : зб. тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. Львів : ЛДУБЖД, 2023. С. 22–27.

4. GitHub. SharpCompress – Modern compression library for .NET. URL: https://github.com/adamhathcock/sharpcompress

5. Ткачук Р. Л., Полотай О. І., Балацька В. С., Брич Т. Б., Кухарська Н. П. Моделювання захисту операційних систем від реалізації кібератак з використанням критерію Пірсона. Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. пр. Львів : ЛДУ БЖД, 2025. № 31. С. 117–125. DOI: https://doi.org/10.32447/20784643.31.2025.12

6. AV-Test Institute. Test Results – Antivirus Software for Windows (April 2024). URL: https://www.av-test.org/en/antivirus/home-windows/

7. SQLite. SQLite. URL: https://www.sqlite.org/docs.html – Дата звернення: 10.06.2025.