РОЗРОБКА МОДЕЛІ ЗАХИСНОГО МЕХАНІЗМУ ОПЕРАЦІЙНИХ СИСТЕМ

Пономаренко В.В.[1], студентка гр. КІБ-20,
viktoriia.ponomarenko.kita@donntu.edu.ua;
Паращевін М.М.[1], студент гр. КІБ-20,
mark.parashchevin.kita@donntu.edu.ua;
Алтухова Т.В.[1], к.т.н., tetiana.altukhova@donntu.edu.ua
[1] Державний вищий навчальний заклад «Донецький національний технічний університет», Луцьк, Україна

З розвитком сучасного інформаційного захисту на рівні прикладного та системного програмного забезпечення (ПЗ) застосовуються різноманітні системи розмежування доступу до інформації, ідентифікації і аутентифікації, аудиту і моніторингу та антивірусного захисту, і вони на сьогоднішній час продовжують свій розвиток [1]. Наразі існує велика кількість різних систем і вони, загалом, адаптовані під ПЗ, що розроблено ще десять років назад, проте необхідно враховувати, що з безкінечним доступом до інформації в світі майже щодня з'являються більш розвинені програмні застосунки, інтелектуальні системи, де серед яких складно здійснити прогноз щодо їх внеску у розвиток світового ІТ-ринку. Кожне програмне забезпечення, особливо якщо воно розроблено на основі нового алгоритму, потребує більш ефективних систем захисту через поширення небезпеки ураження їх різноманітними вірусами [2], тому напрямок розробки антивірусних додатків є досить актуальним. З огляду на це мета даної роботи полягає в дослідженні захисних механізмів операційних систем на прикладі розробленого антивірусного додатку.

Антивірусний додаток представляє собою певний комплекс програм, що спрямований на ефективне виявлення і знешкодження шкідливого вірусного ПЗ та усунення небезпечних наслідків їх дій на комп'ютері. Даний додаток загалом виконує три основні функції, до яких відносять моніторинг та перевірка файлів на зараження задля локалізації і, відповідно, подальшого знешкодження вірусу, а також своєчасне оновлення антивірусних баз даних задля більш ефективного забезпечення своїх функціональних можливостей [3]. На даний час при розробці антивірусних програм також необхідно враховувати технології проведення аналізу на наявність вірусів, до яких належать сигнатурний та ймовірнісний аналіз [4].

Для розробки моделі захисного механізму операційної системи було застосовано технологію сигнатурного аналізу, який спрямований на перевірку наявності у файлах сигнатур вірусів. Даний аналіз вважається найбільш розповсюдженим методом виявлення вірусного ПЗ і застосовується практично у всіх сучасних антивірусних застосунках. В даному випадку при проведенні перевірки на наявність вірусів антивірусу необхідний набір вірусних

сигнатур, які зберігаються в антивірусній базі даних [5-7].

Рисунок 1. Головне меню розробленої моделі антивірусного застосунку на основі технології сигнатурного аналізу

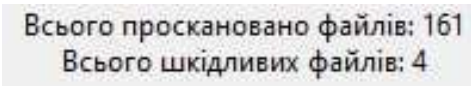

Рисунок 2. Результати сканування операційної системи

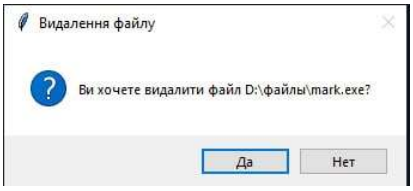

Рисунок 3. Спливаюче вікно для виконання операції видалення потенційно небезпечних загроз

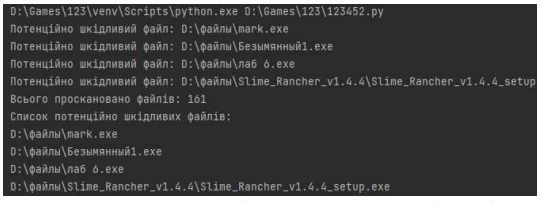

Рисунок 4. Перелік сканованих файлів

На рис. 1 представлено зовнішній вигляд розробленої моделі антивірусного застосунку на основі технології сигнатурного аналізу. Головне меню представлене спливаючим вікном та кнопками для виконання відповідних операцій, при натисканні яких виконується робота та надалі з'являється відповідний звіт екрані додатковим спливаючим вікном. Натискаючи кнопку «сканувати директорію» ми маємо змогу побачити результат сканування у такому форматі (рис.2).

У разі виявлення антивірусним застосунком шкідливих файлів з розширенням '.exe', '.bat', '.vbs', то вона автоматично генерує спливаюче вікно, яке пропонує видалити потенційно небезпечні загрози (рис. 3). Після підтвердження програмному додатку результати сканування файлів виглядають ось таким чином (рис. 4).

Після завершення відповідних операцій із додатком користувач має змогу подивися коли він в останнє виконував маніпуляції з ним, а саме для цього обирається функція «Останнє сканування», і надалі застосунок генерує спливаюче вікно, де вказується дата і час останнього сканування (рис. 5).

Таким чином, на основі розробленої моделі захисного механізму операційної системи, який відповідає критеріям антивірусного застосунку, виконано дослідження основних функціональних можливостей виявлення небезпечних вірусних загроз та визначено, що дана програма дозволяє відстежувати, ідентифікувати та видаляти небезпечні файли.

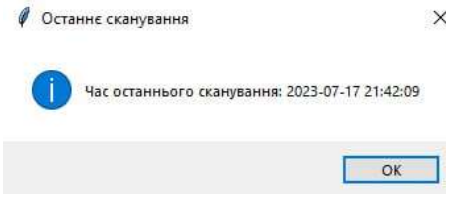

Рисунок 5. Спливаюче вікно щодо інформації про останнє сканування

Така модель має можливості адаптації під особисті потреби кожного початківця в ІТ з урахуванням майбутнього його вдосконалення та різноманітної модернізації на основі розширення функціональних можливостей і розширення антивірусної бази даних.

Література

1. Internetworking Technology Handbook: User manual / Jackson C. –Massachusets : Cisco Systems, 2011. –P. 56 -67.

2. Cecil A. A Summary of Network Traffic Monitoring and Analysis Techniques/ A. Cecil // Computer Systems Analysis. –2006. – P.4 – 7.

3. Основні види вірусних програм [електронний ресурс]. Режим доступу: https://zillya.ua/index.php?q=osnovni-vidi-virusnikh-program – Дата доступу: листопад 2023. – Назва з титул. екрана.

4. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

5. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ “ОЮА”, 2017. – 128 с.

6. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. – [Чинний від 1999.04.28]. – К.:ДСТСЗІ СБУ, 1999. – № 22.

7. ДСТУ ISO/IEC 15408-5:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки (ISO/IEC 15408-5:2022, IDT) [електронний ресурс]. Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104390 – Дата доступу: листопад 2023. – Назва з титул. екрана.

Анотація

В роботі розглянуто питання розробки моделі захисного механізму операційних систем та її програмної реалізації у вигляді антивірусного програмного застосунку на основі технології сигнатурного аналізу, який спрямований на перевірку наявності у файлах сигнатур вірусів. Виконано дослідження основних функціональних можливостей розробленого додатку виявлення небезпечних вірусних загроз та визначено, що дана програма дозволяє відстежувати, ідентифікувати та видаляти небезпечні файли.

Ключові слова: захисні механізми, операційна система, антивірус, програмний додаток, сигнатурний аналіз.

Abstract

The paper considers the development of a model of the protective mechanism of operating systems and its software implementation in the form of an anti-virus software application based on the technology of signature analysis, which is aimed at checking the presence of virus signatures in files. The main functionalities of the developed application for detecting dangerous virus threats are studied and it is determined that this application allows tracking, identifying and deleting dangerous files.

Keywords: protective mechanisms, operating system, antivirus, software application, signature analysis.