УДК 004.056.53

О.М. Козак

ЗАСІБ ДЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ І ДОСЛІДЖЕННЯ

Вінницький національний технічний університет

Анотація. *У даній роботі проаналізовано різні види захисту програмного забезпечення від несанкціонованого копіювання та розповсюдження. Запропоновано та розроблено власний варіант засобу для захисту програмного забезпечення від несанкціонованого копіювання шляхом прив'язки до архітектури комп'ютера і шифрування, реалізований мовою програмування JAVA.*

Ключові слова: *захист програмного забезпечення, прив'язка до архітектури комп'ютера, несанкціоноване копіювання, JAVA.*

Abstract. *This paper analyzes different types of software protection against unauthorized copying and distribution. Proposed and developed its own version of the tool to protect software from unauthorized copying by binding to computer architecture and encryption, implemented in the JAVA programming language.*

Keywords: *software protection, binding to computer architecture, unauthorized copying, JAVA.*

Вступ

У сучасному світі вкрай важливою складовою розвинених інформаційних систем (ІС), які можуть кардинально відрізнятись за своєю будовою та масштабом дії, наприклад окремий персональний комп'ютер (ПК) у локальній мережі, або обчислювальна, телекомунікаційна система у глобальній мережі, є програмне забезпечення (ПЗ).

Сучасне ПЗ реалізує все більш складні та ефективні рішення для різноманітних складних задач, які стають перед людьми у всіх сферах людської діяльності. Саме через те, що задачі можуть бути досить складними, потрібне ПЗ для їх вирішення є вкрай вартісним, тому воно все частіше піддається впливу шкідливих факторів, які спотворюють його. Істотної шкоди програмним продуктам наносять шкідливі ПЗ, за допомогою яких здійснюється несанкціоноване копіювання та їх незаконне розповсюдження. Результатом таких дій є зниження якості ПЗ.

Наразі існує чимало засобів для захисту від несанкціонованого копіювання та незаконного розповсюдження [1]. Результатом такої великої кількості розроблених засобів є проблема вибору певного засобу для конкретної ІС для подальшої коректної роботи.

Метою даної роботи є розробка індивідуального, більш гнучкого, методу захисту програмного забезпечення від несанкціонованого копіювання і дослідження, який унеможливлює запуск програм на інших комп'ютерах і в той же час захищає від несанкціонованого дослідження.

Результати дослідження

Програмний засіб, що реалізує поставлені цілі, має дві складових: перша складова здійснює захист, друга – запуск захищеної програми на виконання. Кожна складова реалізована окремим програмним модулем. В основі захисту лежить не лише прив'язка до параметрів архітектури комп'ютера, що захищає від несанкціонованого копіювання, а й зберігання виконуваного файлу у вигляді, що не може бути виконаний без певних перетворень, і, як наслідок, не підлягає несанкціонованому статичному дослідженню.

Для програмної реалізації засобу захисту обрано мову Java, для реалізації графічного інтерфейсу користувача використано платформу JavaFX та середовище SceneBuilder [2].

Програмний застосунок для захисту має три блоки (рис. 1):

1) Блок отримання характеристик комп'ютера.
2) Блок формування індивідуального ключа.
3) Блок шифрування, який реалізовано за допомогою гешування за алгоритмом MD5 і побітової зміни захищуваного коду програми [3].

У блоці отримання характеристик комп'ютера спеціальні методи програмного застосунку звертаються до ключів реєстру [4]. Зчитування реалізовано за допомогою пакетів Advapi32Util та WinReg, які дозволяють отримати інформацію про BIOS, про жорсткий диск, про операційну систему та про процесор (рис. 2).

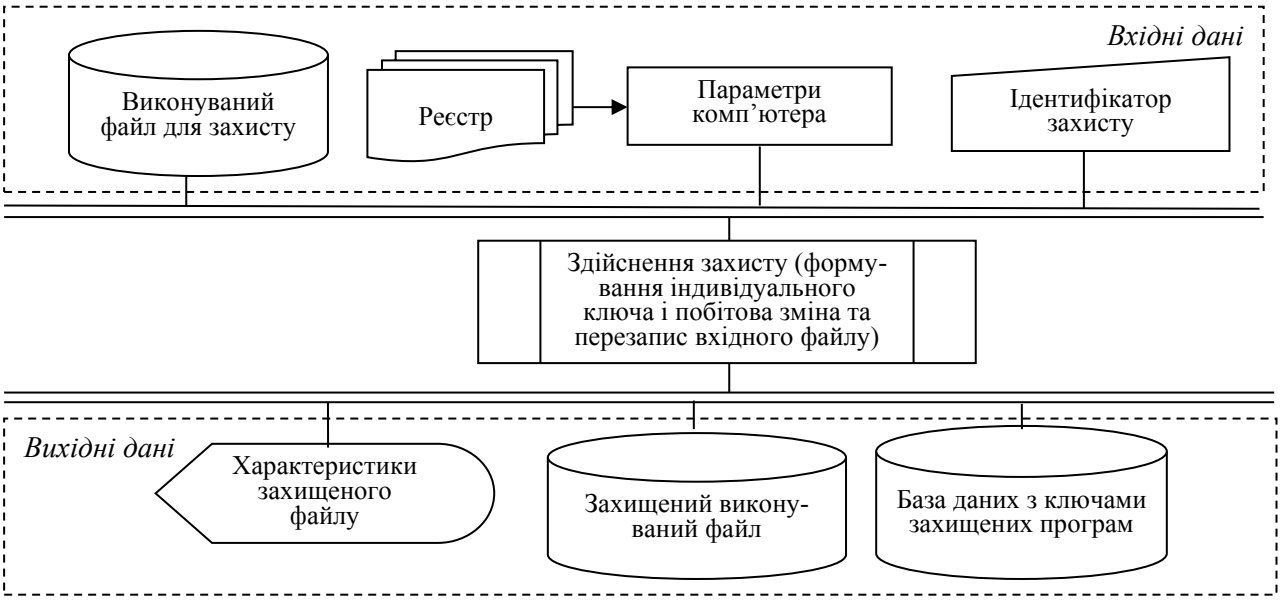
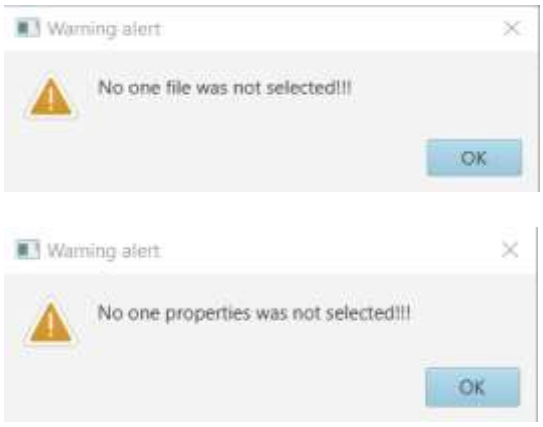


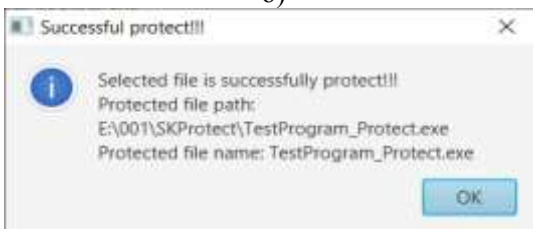
Рисунок 1 – Схема ресурсів програмного засобу

У другому блоці програмного засобу формується індивідуальний ключ захисту, вміст якого цілком залежить від бажань користувача і складається з певних значень параметрів архітектури комп'ютера. При цьому кількість і порядок цих значень у створеному ключі можуть бути довільними (у програмі передбачено виведення цієї інформації на екран) (рис. 2).

а)



б)



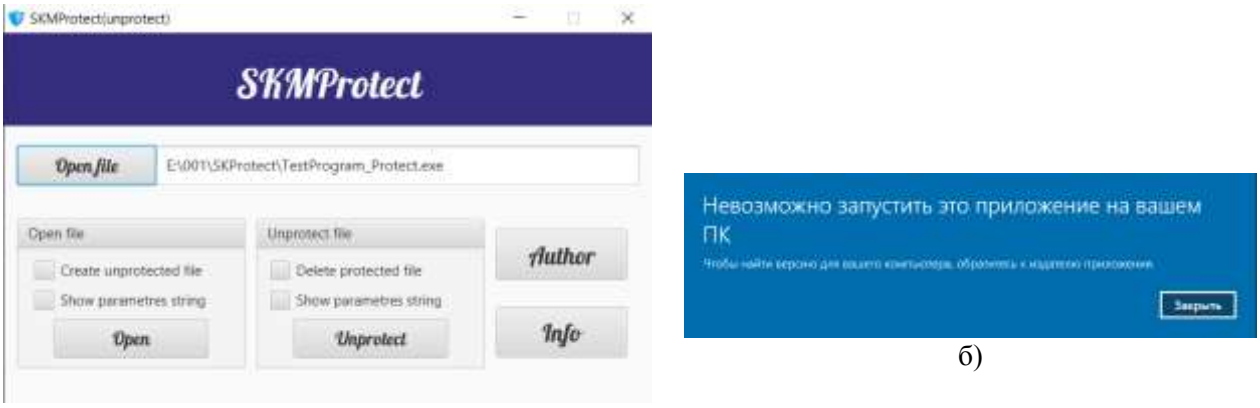
в)

Рисунок 2 – Фрагменти роботи програмного засобу захисту (а - вигляд вікна вибору параметрів прив'язки; б – результати помилкових спрацювань; в – повідомлення про здійснення захисту)

Третій блок методів програмного захисту реалізує шифрування і побайтову заміну вхідного файлу. Гешування було обрано як додатковий метод захисту від викрадення бази даних та відкриття рядків прив'язки. Для вдалого захисту виконуваного файлу відбувається побітова зміна вхідного файлу та перезапис його у вихідний файл. Даний механізм впроваджує рядок прив'язки у структуру виконуваного файлу побітово. Вихідний файл, який отримує користувач, неможливо буде відкрити без додаткового програмного забезпечення, яке знімає даний захист шляхом перевірки конфігурації персонального комп'ютера.

В результаті виконання вказаних дій вхідний виконуваний файл буде збережено у захищуваному вигляді, і будь-яка спроба виконати його на іншому комп'ютері або навіть на цьому самому пристрої без спеціальної програми стане не можливим.

Другий модуль програмного засобу призначений для зняття захисту. При знятті захисту всі дії майже аналогічні діям, які виконуються при встановленні захисту, з тією різницею, що додатково здійснюється перевірка сформованого рядка прив'язки при виконанні зняття захисту та зчитаного рядка прив'язки із бази даних, який був використаний при встановленні захисту на виконуваний файл. У цьому моменті алгоритм зняття захисту може продовжитись або видати помилку та завершитись. При продовженні відбувається відновлення виконуваного файлу шляхом побітового зчитування та запису у новий файл із ігноруванням бітів, які відповідають рядку прив'язки. Дані біти будуть просто відкинуті та не записані у вихідний файл, таким чином буде відновлено виконуваний файл (рис. 3).



а) б)

Рисунок 3 – Фрагменти роботи програми для зняття захисту (а – запуск виконуваного файлу, б – відмова при несанкціонованому запуску)

У разі виникнення помилки користувач отримує повідомлення про те, що конфігурація його персонального комп'ютера відрізняється від тієї, на якій було встановлено захищений виконуваний файл, тому у знятті захисту буде відмовлено.

Висновки

В результаті виконання роботи розроблено та реалізовано індивідуальний метод захисту програмного забезпечення від несанкціонованого копіювання шляхом прив'язки до архітектури ПК. Для коректного застосування реалізованого методу захисту вимагається використання локальної бази даних для збереження інформації про захищений файл та індивідуальний ключ, за допомогою якого було захищений обраний файл.

Основним недоліком даного методу захисту є те, що при зміні певної апаратної частини, до якої здійснена прив'язка певного ПЗ, користувач, який придбав ліцензію, більше не матиме доступу до програми. Для вирішення цієї проблеми, можна створити сервіс для зберігання особливого ідентифікатора користувача, ключів прив'язки та програм, які були придбані даним користувачем і в разі заміни частини архітектури, виконувати переприв'язку виконуваних файлів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Средства защиты от копирования программных продуктов [Електронний ресурс]. URL: https://arsenal-info.ru/b/book/572319677/64.
2. Java: The inside story [Електронний ресурс]. URL: http://sunsite.uakom.sk /sunworldonline/swol-07-1995/swol-07-java.html.
3. Хеш-функція MD5 [Електронний ресурс]. : URL: https://habr.com/ru/sandbox/26876/.
4. РеестрWindows [Електронний ресурс]. URL :https://regedit.readthedocs. io/introduce .html.

Козак Олександр Михайлович – студент групи 1БС-19б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sashakozak073@gmail.com.

Kozak Oleksandr M. – Department of Information Techologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, email : sashakozak073@gmail.com.