МЕТОДИКА ВИБОРУ ЗАСОБІВ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Руденко О.С.

Харківський національний університет радіоелектроніки,
Україна.

E-mail: oleksii.rudenko@nure.ua

Abstract

The current work is devoted to reviewing modern tools of commercial software protection and development recommendations and methodology of protection tool selection. The review of the problem state and available solutions in the market allowed the author to systematize existing protection tools and propose a set of criteria that can be used for their ranging depending on software developer requirements. In a such way, the task was brought to a standard multicriteria problem and proposed an effective method for this problem solution. Also, an example of a developed method practical application was given. Finally, the conclusions were made, and announced possible direction of future investigations.

Основною метою розробки будь-якого комерційного програмного забезпечення є генерація прибутку. В свою чергу, реалізація цієї мети напряму залежить від ступеня захисту програмного забезпечення від несанкціонованого доступу та обраних моделей ліцензування та монетизації. Розробка та підтримка власних систем захисту та ліцензування потребує значних ресурсів від компаній-розробників та не гарантує отримання безпечного та ефективного рішення. З іншого боку, на ринку існує широка пропозиція готових рішень в сфері захисту програмного забезпечення але вибір оптимального рішення з урахуванням всіх особливостей продукту, безпеку якого треба забезпечити, не є тривіальним завданням. Складність вибору полягає в браку інформації по існуючим системам захисту, відсутності порівняння цих систем та рекомендацій щодо вибору в залежності від потреб розробника програмного забезпечення, необхідності врахування економічної складової. Виходячи з вищезазначеного, можна зробити висновок щодо актуальності ретельного аналізу готових рішень захисту програмного забезпечення та розробки прикладної методики вибору в залежності від потреб розробника.

На першому етапі роботи був проведений широкомасштабний огляд та аналіз сучасних систем захисту програмного забезпечення. Умовно розглянуті засоби можна розподілити на три групи: засоби захисту програмного коду від аналізу, модифікації та несанкціонованого доступу; засоби ліцензування та монетизації програмного забезпечення; засоби моніторингу несанкціонованого доступу до комерційного програмного забезпечення. Під час огляду особлива увага приділялася комплексним системам захисту з міркувань скорочення часу на розгортку системи та повної сумісності між складовими елементами. В результаті аналізу були визначені критерії оцінювання комплексних систем захисту програмного забезпечення. Далі була виконана систематизація розглянутого матеріалу, в результаті якої була складена зведена порівняльна таблиця-матриця строками якої є розглянуті комплексні системи захисту, а стовбцями – запропоновані критерії. В разі відсутності певної властивості у системі захисту, відповідна клітинка матриці містить нуль. Якщо ця властивість притаманна системі – маємо число від нуля до ста в залежності від рівня реалізації даної властивості (значення «100» відповідає найвищому рівню). Отже значення в таблиці є безрозмірними (нормовані) та можуть бути порівняні між собою. Таким чином задача вибору комплексної системи захисту програмного забезпечення була зведена до звичайної багатокритеріальної задачі. Для вирішення багатокритеріальної задачі вибору комплексного рішення захисту програмного забезпечення запропоновано використовувати метод адитивної згортки. Згідно з цим методом, визначається підсумковий узагальнений критерій для кожної з альтернатив за формулою:

$$K(x) = \sum_{j=1}^{n} a_j \cdot K_j(x), \quad (1)$$

де $K_j(x)$ – набір приватних критеріїв;

n – кількість приватних критеріїв;

a_j – відносна вага.

Найкраще рішення в изначається виразом:

$$x^* = \arg\max_{x \in X} K(x). \quad (2)$$

Метод адитивної згортки для вирішення багатокритеріальної задачі було обрано через простоту його математичного апарату, можливість виділення більш вагомих критеріїв та доведену адекватність результатів. Відносні ваги для кожного критерію якості змінні для кожної окремої задачі. Саме завдяки «зважуванню» критеріїв якості, запропонована методика дозволяє врахувати особливості програмного забезпечення та потреби розробника. В роботі надано рекомендації щодо вибору значень відносних ваг критеріям якості.

Також запропонований метод вирішення багатокритеріальної задачі вибору системи захисту дозволяє застосовувати систему обмежень неприйнятних рішень. Ряд обмежуючих умов або перевірок на граничні значення критеріїв може бути накладено на системи захисту, в результаті чого неприйнятні альтернативи будуть виключені із подальшого розгляду. Прикладом такого обмеження може бути гранична вартість системи захисту (наприклад, вартість не повинна перевищувати вартість власної розробки або виділений бюджет), або відсутність якості, критичної для розробника (наприклад, відсутність засобів обфускації вихідного коду програмного забезпечення).

В якості перевірки запропонованого підходу була вирішена задача вибору комплексної системи захисту для спеціального інженерного програмного забезпечення AxSTREAM®, розробник SoftInWay Inc. [1]. Розробником були висунуті наступні вимоги до комплексної системи захисту:

– максимальний рівень захисту продукту від копіювання та методів зворотнього аналізу коду;
– надійна та стійка до зламу система ліцензування;
– різноманіття моделей ліцензування та монетизації;
– наявність надійних хмарних сервісів ліцензування користувачів;
– наявність системи моніторингу використання програмного забезпечення є бажаною, але не обов’язковою;
– обмеження по бюджету на придбання та обслуговування системи ліцензування та захисту.

Урахування вимог розробника дозволило визначити вагові коефіцієнти критеріїв якості та визначити необхідні обмеження. Після застосування системи обмежень неприйнятних рішень було визначено 3 альтернативи: CodeMeter® від Wibu Systems [2], Revenera® від Flexera [3] та Sentinel LDK® від Thales [4]. Далі для кожної з альтернатив було визначено підсумковий критерій за формулою (1). За умовою (2) найкращим рішенням для захисту програми AxSTREAM® виявся комплекс Revenera®. На основі розглянутого прикладу можна зробити висновок, що розроблений підхід дозволяє обґрунтовано обрати систему захисту програмного забезпечення з урахуванням вимог та обмежень компанії-розробника. Нажаль, запропонована методика не є сталою і вимагає оновлення даних щодо актуальних систем комплексного захисту та їх ефективності.

В якості подальших робіт планується розглянути застосування комбінацій окремих рішень для захисту коду, ліцензування та моніторингу використання та порівняти їх ефективність з комплексними рішеннями. В подальшому за результатами досліджень можливо створення спеціального агрегатору готових рішень під вимоги користувача, який буде оновлюватися та доповнюватися користувачами або розробниками систем захисту програмного забезпечення.

Література

1. AxSTREAM® software platform. URL: https://www.softinway.com/software/ (дата звернення: 10.09.2023).

2. .Codemeter: The all-in-one technology. URL: https://www.wibu.com/us/products/codemeter.html (дата звернення: 30.08.2023).

3. Revenera software licensing solutions. URL: https://www.revenera.com/software-monetization/products/software-licensing (дата звернення: 30.08.2023).

4. Sentinel LDK: Out-of-the box software protection, licensing and entitlement management solution. URL: https://cpl.thalesgroup.com/sites/default/files/content/product_briefs/field_document/2023-04/Sentinel-LDK-pb.pdf (дата звернення: 30.08.2023).