УДК 004.056.53

Борка М. Ю.
Каплун В. А.

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАХИСТУ ПРОГРАМ

Вінницький національний технічний університет

Анотація

Досліджено основні методи захисту програмного забезпечення, які використовуються для зменшення незаконного поширення та найбільш використовувані методи розповсюдження програмного забезпечення. Пропонується такий підхід до проблеми захисту програм, як використання сучасних хмарних технологій.

Ключові слова: програмне забезпечення, неліцензійний контент, хмарні технології.

Abstract

The basic methods of protection software used for reducing the illicit spread and most used methods of software distribution. Proposed approach to the problem for applications the use of modern cloud.

Keywords: software, unlicensed content, cloud technologies.

Вступ

За останні 30 років технологія захисту програмного забезпечення постійно розвивалася і еволюціонувала. З появою нових і недосліджених способів захисту програмного забезпечення з'являлися і нові методи обходу даних методів. Через високу кількість незаконно поширеного програмного забезпечення є постійна потреба у створенні нових технологій і методів захисту програмного забезпечення.

Результати дослідження

У статті розглянуто методи захисту програмного забезпечення, які є популярними на сьогоднішній день [1]. Серед них основні:

- прив'язка до фізичного носія (HARD-, Flash-, CD-, DVD- дисків);
- використання програмно-апаратних захистів за допомогою електронних ключів;
- активація програмних засобів через Інтернет;
- обфускація джерельного коду програм;
- використання псевдокоду;
- доступ до програмного забезпечення через «хмару».

Прив'язка до фізичного носія. У цьому методі використовується спеціальний ключ, який записаний на фізичному носії. Для роботи з додатком, який використовує таку прив'язку необхідний безпосередньо сам фізичний пристрій. Даний методи найчастіше використовується для широко тиражованих продуктів.

Електронні ключі захисту. Такий апаратний спосіб захисту використовується для прив'язки ключа до обладнання. У цьому методі використовуються криптографічні алгоритми, що зменшують ймовірність успішного використання емуляторів. На сьогоднішній день цей метод є одним з найкращих за стійкістю до злому і найбільш розповсюджених [2].

Інтернет-активація. При такому способі захисту використовується активація програмного продукту через мережу Інтернет. Цей метод у сьогоденні часто використовується через дешевизну та легкість підтримки і супроводження.

Обфускація коду. При такому способі захисту використовується заплутування коду з метою приховування алгоритмів, зменшення ймовірності декомпіляції та збільшення швидкості роботи програми.

Псевдокод. Даний метод перетворює код додатку у машинні інструкції та приховує алгоритм. Проте даний він не захищає додаток від нелегального копіювання [3].

Доступ через «хмару». У даному методі використовується доступ до програмного застосунку з використанням «хмарних технологій». Перевагою є можливість працювати з додатком з будь-якого пристрою без необхідності встановлення самого додатку на цей пристрій. Проте без доступу до інтернету такої можливості не буде.

Вибираючи захист для свого програмного продукту, необхідно враховувати безліч факторів: канали дистрибуції, вартість захисту, вимоги до надійності і відмовостійкості.

Наразі хмарні технології використовуються для сховища даних на сервері, який може знаходитись у будь якій точці планети, без необхідності збереження самих даних на комп'ютері. А доступ до цього сховища можна отримати з будь якого комп'ютера.

Суть запропонованого способу захисту програм з використанням «хмари» полягає у тому, що користувач може отримати доступ до даних лише після введення логіну та паролю.

Для збереження даних може використовуватись база даних, доступ до якої отримують лише авторизовані користувачі. База даних використовується для забезпечення надійності та цілісності даних, логування та спільного використання даних.

Висновки

Отже, у результаті дослідження було здійснено загальну класифікацію методів захисту програмного забезпечення, виявлено переваги та недоліки кожного з них.

Запропоновано для захисту програм використовувати такий сучасний інструмент, як хмарні технології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Daniel Mellado. IT Security Governance Innovations: Theory and Research. – IGI Global, 2012.
2. Derrick Grover. The Protection of Computer Software - its Technology and Applications. – Cambridge University Press, 1989.
3. Методи захисту програм [Електронний ресурс]. – Режим доступу: URL: http://www.ultimatepp. org/srcdoc $Protect$SoftwareProtection$en-us.html/ - Назва з екрану.

Борка Микола Юрійович – студент групи БС-14б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: finage4@gmail.com.

Каплун Валентина Аполінаріївна, старший викладач кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: valuka8379@gmail.com.

Borka Mykola - student group SS-14, Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: finage4@gmail.com.

Kaplun Valentyna, senior lecturer in information security, Vinnytsia National Technical University, Vinnytsia, email: valuka8379@gmail.com.