УДК 681.322:621.391

В.В. Богачук
В.В. Карпінець

РОЗРОБКА МОДУЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ

Вінницький національний технічний університет

Анотація

Розглянуто розробку модуля захисту програмного забезпечення.

Ключові слова: *Інформація, захист, модуль, інтернет, доступ, ключ, програмування, алгоритм.*

Abstract

The development of the software protection module was considered.

Kaywords: *Information, protection, module, internet, access, key, programming, algorithm.*

Вступ

У даному дослідженні представлено аналіз існуючих систем захисту програмного забезпечення від несанкціонованого копіювання та вибір оптимального шляху вирішення проблеми, розробку модуля захисту від несанкціонованого копіювання (НСК) шляхом використання серверу активації на основі протоколу TCP.

Результати дослідження

Захист інформації перетворюється сьогодні на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження. Необхідність використання систем захисту СЗПЗ обумовлена рядом проблем. Існуючі системи захисту програмного забезпечення можна класифікувати по ряду ознак, які різняться між собою. Для захисту ПЗ використовується ряд методів: алгоритми заплутування, мутації, компресування та шифрування даних, методи ускладнення дизассемблювання та налагодження, емуляція процесів, тощо. Системи захисту від несанкціонованого копіювання здійснюють «прив'язку» ПЗ до дистрибутивного носія (гнучкий диск, CD і ін.). Даний тип захистів заснований на глибокому вивченні роботи контролерів нагромаджувачів, їх фізичних показників, нестандартних режимах розбивки, читання/запису, тощо. Метод захисту від несанкціонованого копіювання шляхом використання серверу активації є досить поширеним, оскільки даний метод дозволяє безперешкодно тиражувати продукт, тобто можливе розповсюдження через мережу Інтернет без передачі власне фізичного носія з програмою. Взаємодія між комп'ютерами в інтернеті здійснюється за допомогою мережевих протоколів, що представляють собою узгоджений набір певних правил, відповідно до яких різні пристрої передачі даних обмінюються інформацією. Протокол TCP/IP включає в себе також протоколи UDP, SMTP, ICMP, FTP і не тільки. Ці та інші протоколи TCP/IP забезпечують найбільш повноцінну роботу мережі Інтернет.

Суть розробки програми захисту від несанкціонованого копіювання доцільно розробляти у вигляді інтегрованого модуля програми та серверу активації, який буде знаходитися у локальній мережі. Для того, аби активувати програму, користувач повинен ввести ключ активації, який надається разом із програмою. Захист буде здійснюватися шляхом генерації ключа активації на основі унікального ідентифікатора за допомогою алгоритму RSA. Далі ключ активації програми та серійний номер процесора передаються на сервер. Якщо ж користувач намагається отримати доступ до ліцензійного програмного забезпечення не маючи вірного ключа то генерується помилковий цифровий підпис який не дає запустити захищену програму. Після генерації підпису він відправляється клієнту.

Клієнтський додаток повинен контролювати наявність коду активації у вигляді зображення. Контролювати дешифрування коду активації з зображення в масив байт та перевірку його вірності. Також він повинен контролювати взаємодію з сервером у разі потреби отримання коду активації у випаду відсутності або невірності коду активації та зберігати отриманий код активації у вигляді зображення.

Висновок

Було розглянуто теоретичні відомості про несанкціоноване копіювання інформації, розглянуто види загроз та шляхи для їх перешкодження**.** Для розробки була використана об'єктно-орієнтована мова програмування C# у середовищі розробки Visual Studio. Розроблено алгоритм модуля захисту програми від несанкціонованого копіювання.

Список використаної літератури

1. Класифікація систем захисту програмного забезпечення [електронний ресурс] – Режим доступу до ресурсу: http://e-rentier.ru.studopedia.net/
2. Основи C# [електронний ресурс] – Режим доступу до ресурсу: http://www.znannya.org/
3. Протокол TCP/IP [електронний ресурс] – Режим доступу до ресурсу: http://kasner.kiev.ua/
4. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)

Богачук Вікторія Володимирівна, студентка групи УБ-16б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Карпінець Василь Васильович***, доцент кафедри МБІС, Вінницький національний технічний університет, Вінниця.

Bogachuk Viktoria, student of group UB-16b, faculty of management and information security, Vinnytsia National Technical University, Vinnytsia.

Scientific supervisor***: Vasily Karpinets***, associate professor of the department of MBIS, Vinnitsa National Technical University, Vinnytsia.