Сметанін К. В., к.т.н.
Житомирський військовий інститут ім. С.П. Корольова

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОЇ ДЕКОМПІЛЯЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ МЕТОДІВ БЛОКУВАННЯ

Актуальність. Сучасні цифрові прилади та комп'ютерні мережі, які володіють потужними обчислювальними, інформаційними і телекомунікаційними можливостями, створюють великі можливості для діяльності людини, яка ж сама їх удосконалює та вирішує які вони будуть виконувати завдання. Основним технічним інструментом для цього є програмне забезпечення (далі ПЗ), яке разом з інтелектом людини, його навиками і знаннями, дає можливість створювати цікаві та складні комп'ютерні програми. ПЗ сучасних комп'ютерних систем є достатньо складним та багатофункційним виробом, при створенні якого активно використовуються автоматизовані засоби його розробки і загальносистемне ПЗ, об'єм і складність якого можуть перевищувати прикладне ПЗ на порядки. Як правило, забезпечення стовідсоткової якості програмних продуктів є практично нерозв'язним завданням, що є причиною того, що жодний розробник не гарантує повноцінного захисту, надійності та цілісності створюваного програмного продукту. *Тому* виникає питанням, чи є така можливість разом з правовим і організаційним забезпеченням процесу створення і експлуатації програм, здійснити науково-технічні заходи, що дозволяють створити захищену систему від подібних зловмисних дій та надати необхідну інформацію про можливий злом ПЗ.

Постановка задачі. Створити максимально захищену систему забезпечення та декомпіляції програмного рішення з використанням методів блокування. Це дозволить зменшити рівень впливу на програмне рішення сторонніми особами та зробить програму більш захищеною.

Основні положення. Захист інформації є суттєвою проблемою для багатьох розробників найсучаснішого ПЗ. Одним з основних видів правопорушень щодо програмного забезпечення є контрафакція, різновидами якої є відтворення, розповсюдження та використання програмного забезпечення без дозволу власника авторських прав на ці твори (комп'ютерне піратство). Для створення захисту програного забезпечення від шахраїв створюють своєрідну систему безпеки ПЗ, яка включає в себе: шифрування, обфускацію, контроль цілісності, захист даних, а також ключ захисту та ліцензію.

Крім захисту від шахрайства (піратства), перед кожним розробником програмного забезпечення виникає ще одне не менш важливе завдання щодо захисту програмного коду від аналізу і підробки. В цьому випадку недобросовісні конкуренти можуть відносно легко декомпілювати програмний додаток і вкрасти всі реалізовані науково-технологічні новинки, зробивши всі інноваційні переваги розробника марними. Існує чимало методів програмного блокування, деякі з них представлені на рис 1.

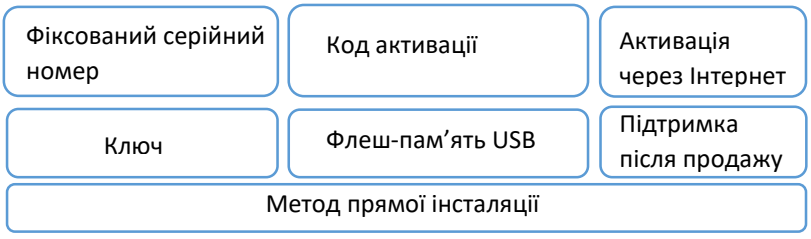

Рис.1 – Методи програмного блокування

Найчастіше під зломом ПЗ розуміють його модифікацію для видалення або вимкнення функцій, які вважаються особливо небажаними.

Злом може здійснюватися: повторним введенням серійного номеру, key-gen, patch, loader.

Найпоширеніший злом програмного забезпечення полягає у модифікації двійкового файлу програми, щоб викликати або запобігти виконанню певної частини програми. Це досягається шляхом зворотного проектування.

Це можна зробити*:*

- запустити програмний код за допомогою debugger, доки зловмисник не досягне підпрограми, яка містить основний метод захисту програмного забезпечення.
- перетворення або декомпіляція виконавчого файлу(exe, com).

Розробники програмного забезпечення постійно створюють нові, або вдосконалюють відомі методи таки як обфускація коду, шифрування та самозаміни коду, щоб ускладнити читання виконавчого файлу. Тому застосовані методи ускладнюють декомпіляцію коду.

Висновки. При створені ПЗ обов'язково необхідно зменшити ризики несанкціонованої декомпіляції, це досягається використанням методів обфускації програмного коду та методів програмного блокування.