УДК 004.4

І.А. Сорокін[1], А.О. Різуненко[2]

[1] *Військовий коледж сержантського складу військового інституту телекомунікацій та інформатизації Національного технічного університету України «КПІ», Полтава*
[2] *Військовий інститут телекомунікацій та інформатизації Національного технічного університету України «КПІ» (факультет засобів військового зв'язку), Полтава*

МОДУЛЬ ПРОГРАМНОГО ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Розглянуто проблему захисту програмного забезпечення від несанкціонованого копіювання. Запропоновано створення оптимального за ефективністю та вартістю програмного модуля захисту ПЗ. Наведені вимоги до сучасних систем захисту ПЗ, розглянуті способи створення систем захисту ПЗ та їх основні види. Обрано спосіб створення та розроблено програмний модуль захисту ПЗ із дотриманням усіх вимог до системи захисту програмних продуктів.

Ключові слова: *модуль, програмне забезпечення, система захисту.*

Вступ

У зв'язку із прогресивною комп'ютеризацією всіх сфер людської діяльності створюється все більше різнофункціонального програмного забезпечення (ПЗ). Разом із цим, не дивлячись на всі зусилля різних організацій, в останні роки зростає рівень комп'ютерного піратства. У середньому доля піратського ПЗ у глобальному масштабі складає 40%, тобто кожні чотири з десяти створених програм є вкраденими у авторів або творчих колективів, що позбавляє їх прибутку. При цьому Україна знаходиться на шостому місці у списку країн із найвищими показниками піратства, доля якого складає 83% [1].

Основний шлях боротьби з нелегальним розповсюдженням ПЗ – легітимний, тобто злам та незаконне копіювання ПЗ знайшли відображення у відповідних законах, і держава здійснює переслідування піратів та притягання їх до відповідальності. Іншим шляхом боротьби може бути економічний. Його сутність полягає в тому, що ціна на ПЗ настільки низька, що близька до вартості зламу. При цьому, як правило, покупець надасть перевагу ліцензійному продукту. Однак, цей спосіб неприпустимий для "серйозних" програмних продуктів великої вартості, тому їх розробники вдаються до третього шляху – захисту ПЗ від зламу та несанкціонованого копіювання.

Питанням захисту ПЗ приділяється багато уваги як у зарубіжних, так і у вітчизняних дослідженнях, таких авторів як: С.А. Середа, А.В. Чернов, О.В. Казарин, А. Новичков та Р. Сардарян. Проаналізувавши роботи даних вчених можна побудувати умовний графік залежності прибутку від продажу ПЗ у часі [2, 3].

Як видно із графіку, якщо ПЗ погано захищено, то його достатньо швидко ламають (рис. 1) і з'являється його дешева піратська версія, яка не дозволить ліцензійній версії "завоювати" свою долю ринку, а значить – швидко знизить об'єми продаж та позбавить розробників прибутку.

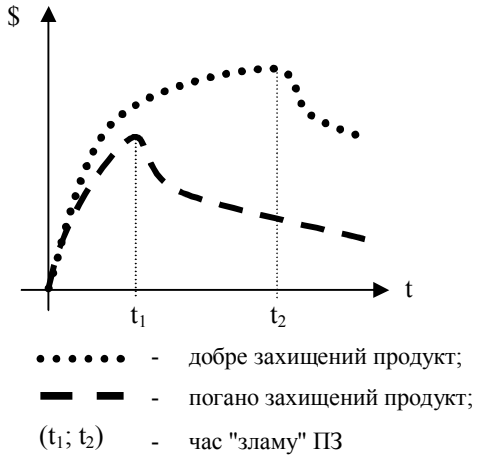

Рис. 1. Умовна залежність прибутку від часу функціонування ПЗ

Якщо захист буде ефективний, (наприклад, злам ПЗ піратами відбудеться через 4 – 5 місяців (рис. 1), а нова версія ПЗ виходить через 7 – 8 місяців), то комерційний успіх може бути повторений [4].

Основна частина

На сьогодні існує кілька систем захисту, різних за вартістю, складністю та призначенням. Метою даної статті є створення оптимального за ефективністю та вартістю програмного модуля як практичної реалізації системи захисту ПЗ.

Розглянемо основні вимоги до сучасних систем захисту.

1. Захист повинен бути з певним часовим запасом стійкості від зламу. Відомо, що абсолютного захисту не буває, але захист повинен забезпечувати

розробникам певний часовий запас, поки пірати не навчаться "ламати" ПЗ.

2. Прив'язка до апаратної частини повинна бути (за можливістю) відсутня, оскільки її окремі компоненти можуть замінюватися в процесі старіння.

3. Захист повинен за можливістю не використовувати апаратні засоби великої вартості.

4. Захист повинен використовувати оригінальні принципи захисту.

5. Захист не повинен перешкоджати копіюванню даних (копіювання можливе, несанкціонований запуск неможливий).

6. Вартість захисту повинна співвідноситись із вартістю ПЗ.

Система захисту може бути реалізована трьома способами:

– програмним (без урахування фізичних характеристик компонентів персонального комп'ютера (ПК) та спеціального обладнання);

– апаратним (спеціальне обладнання для ПК, електронні ключі, ключові дискети);

– комбінованим.

Умовно системи захисту можна класифікувати за наступними типами:

1. Стійкість до прямого копіювання.

Найбільш ефективний спосіб реалізації даного захисту – носій можна вільно копіювати, але запуск ПЗ відбудеться тільки при наявності оригінального носія. Подібний тип захисту заснований на тому, що будь-який диск (CD/DVD/R/RW) має ряд унікальних характеристик, властивих тільки йому, і при копіюванні ці характеристики втрачаються. Їх реалізації у конкретних системах (Star-Force, Tages) залишаються комерційною таємницею.

2. Стійкість до зламу.

У випадку, коли фізичне копіювання неможливе, особі, що здійснює злам, необхідно за допомогою механізмів дезасемблювання та відладки просканувати ПЗ, виділити логіку захисту та нейтралізувати її.

3. Апаратні ключі.

Апаратні ключі є розвинутою та порівняно дорогою системою захисту, яка дозволяє розміщувати всередині модуля ключа різні процедури, додаткові ключі, а також:

– керувати доступом до різних програмних модулів та пакетів;

– призначати кожному користувачеві унікальний номер;

– здавати програми в оренду та розповсюджувати демо-версії із обмеженою кількістю запусків;

– зберігати у ключі паролі, фрагменти програм та іншу важливу інформацію.

4. Ліцензування.

Сутність ліцензування полягає в тому, що після встановлення ПЗ на локальному ПК користувач повинен отримати у розробника ключ, який був (бажано, але не обов'язково) прив'язаний до ПК користувача. У ролі ключа може виступати звичайний пароль. Ліцензії бувають:

– тимчасові (обмежені в часі, необмежені по кількості користувачів);

– постійні (необмежені в часі, обмежені за кількістю ПК для встановлення).

Для ідентифікації ПК використовують велику кількість способів. Прикладами прив'язок можуть бути: серійний номер жорсткого диску, MAC-адреса мережної плати, контрольна сума BIOS та інші характеристики апаратної частини.

Виходячи із описаних вище положень, авторами статті було розроблено модуль авторизації програмного забезпечення, який зображено на рис. 2.

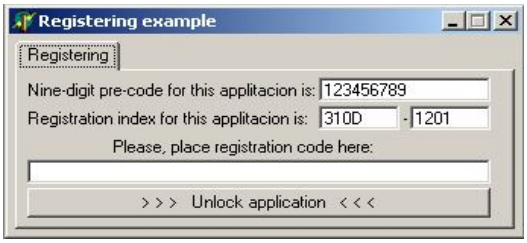

Рис. 2. Вікно модуля авторизації ПЗ

При створенні модуля було використано середовище програмування Borland Delphi 5.5. При цьому були дотримані всі вимоги до системи захисту, викладені вище. Створений модуль за типом системи захисту містить в собі "ліцензування" (4 тип) та "стійкість до зламу" (2 тип), оскільки решта типів систем захисту ПЗ передбачає наявність спеціального обладнання для створення унікальних за фізичними властивостями та вмістом носіїв інформації.

Сутність захисту полягає в наступному (рис. 3): кожному програмному комплексу надається унікальний ідентифікаційний номер у форматі "9 цифр" (nine-digit pre-code: ????????? (рис. 3)). При запуску ПЗ на ПК користувача програма сканує певні апаратні параметри та пропонує свій реєстраційний індекс у форматі "4 цифри - 4 цифри" (registration index: ????-???? (рис. 3)) для цього ПК. Реєстраційні ідентифікатори повідомляються розробнику, який за допомогою певних перетворень генерує реєстраційний код (registration code (рис. 3)) та повідомляє його користувачеві [5]. Слід відмітити, що перетворення застосовуються до рядкових об'єктів та числових величин великої протяжності (40-70 знаків), для чого авторами був розроблений спеціальний числовий тип даних.

У випадку копіювання зареєстрованого ПЗ на інший ПК під час першого запуску програма знову сканує апаратні параметри, та, у випадку невідповідності їх введеному коду, знову пропонує діалог реєстрації. У випадку знищення операційної системи при встановленні копії ПЗ отриманий раніше реєстраційний код буде вірним [6].

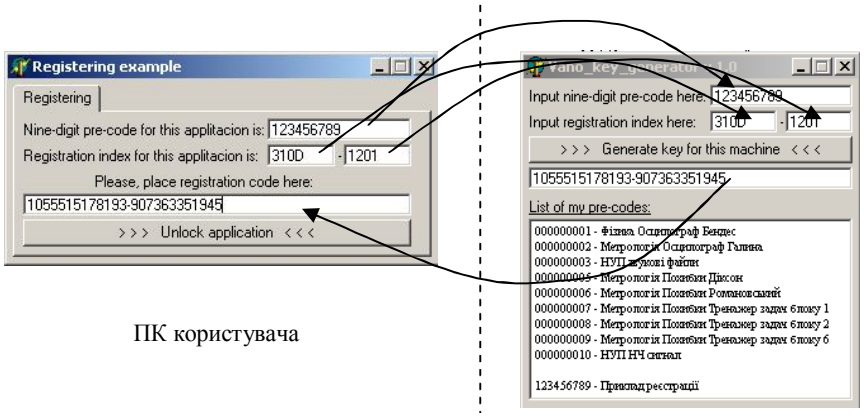

Рис. 3. Механізм реєстрації (приклад)

Таким чином, запропонована система захисту створена комбінованим (апаратно-програмним) способом. В системі захисту присутня прив'язка до апаратної частини, оскільки вона гарантує авторизацію на конкретному окремому ПК. Спеціальні апаратні засоби не використовуються. Алгоритм перетворення коду ПЗ та реєстраційного індексу в реєстраційний код оригінальний та унікальний. Створена система захисту не перешкоджає копіюванню, а тільки несанкціонованому запуску ПЗ.

Висновки

Доречність використання системи захисту залежить від ступеня збереження в таємниці повноцінного релізу ПЗ до його офіційної появи. Якщо "ламана" версія вийде в продаж раніше офіційної, компанія-розробник не отримає жаданого прибутку.

Враховуючи це, було розроблено модуль авторизації ПЗ, який відповідає усім вимогам до сучасних систем захисту ПЗ.

З метою подальшого розвитку планується:

1. Вдосконалення алгоритму шифрування реєстраційних ідентифікаторів.
2. Підвищення маскування шифрувальних процесів.
3. Збільшення ступеня інтеграції модуля до ПЗ, що розробляється.

Список літератури

1. В Украине 85% компьютерного ПО – пиратское [Електронний ресурс] / Источник УНИАН // Читай. Думай. Делай! БИЗНЕС. – 2012. – №8 (995) – Режим доступу до газети: http://www.business.ua/articles/companies/14510/.

2. Семьянов П.В. Анализ средств противодействия исследованию программного обеспечения и методы их преодоления / П.В. Семьянов, Д.П. Зегжда // Компьютер-Пресс. – 1993. – №11. – С. 37-39.

3. Черней Г.А. Безопасность автоматизированных информационных систем / Г.А. Черней, С.А. Охрименко, Ф.С. Ляху. – Кишинев: Ruxanda, 1996. – 186 с.

4. Расторгуев С.П. Искусство защиты и раздевания программ / С.П. Расторгуев, Н.Н. Дмитриевский. – М.: Совмаркет, 1991. – 94 с.

5. On cryptosystems untrustworthiness [Електронний ресурс] / Pavel V. Semjanov // Information security centre, St. Petersburg Technical University – 2006. – Режим доступу до ресурсу: psw@ssl.stu.neva.ru.

6. Защита программного обеспечения: под ред. Д. Гроувера; пер с англ. / Д. Гроувер, Р. Сатер, Дж. Фипс и др. – М.: Мир, 1992. – 286 с.

Надійшла до редколегії 2.03.2012

Рецензент: д-р техн. наук, проф. М.В. Галай, Полтавський Національний технічний університет імені Юрія Кондратюка, Полтава.

МОДУЛЬ ПРОГРАММНОЙ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

И.А. Сорокин, А.А. Резуненко

Рассмотрена проблема защиты программного обеспечения от несанкционированного копирования. Предложено создания оптимального по эффективности и стоимости программного модуля защиты ПО. Приведены требования к современным системам защиты ПО, рассмотрены способы создания систем защиты ПО и их основные виды. Избран способ создания и разработан программный модуль защиты ПО с соблюдением всех требований к системе защиты ПО.

Ключевые слова: *модуль, программное обеспечение, система защиты.*

THE MODULE OF PROGRAM PROTECTION AGAINST UNAPPROVED COPYING OF THE SOFTWARE

I.A. Sorokin, A.A. Rezunenko

The software copy protection problem was examined. The creation of low-price and effective software copy protection module was offered. The requirements to the modern software protection systems were put. The ways of software protection systems creation and there main forms were examined. The way of creation was selected and software copy protection module was created. All requirements to the software protection systems was observed.

Keywords: *module, software, system of protection.*