Міністерство освіти і науки України

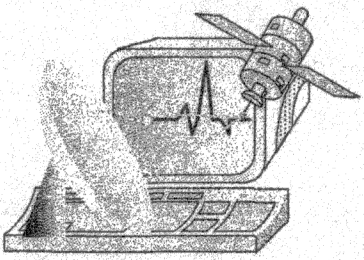
Вінницький національний технічний університет

Вінницька філія ВАТ „Укртелеком"

Інститут кібернетики ім. В.М. Глушкова НАНУ

Вінницьке обласне науково-технічне товариство
радіотехніки, електроніки та зв'язку

Ліга радіоаматорів України



СПРТП-2009

**Матеріали IV Міжнародної
науково-технічної конференції**

СУЧАСНІ ПРОБЛЕМИ РАДІО-ЕЛЕКТРОНІКИ, ТЕЛЕКОМУНІКАЦІЙ ТА ПРИЛАДОБУДУВАННЯ (СПРТП-2009)

*Присвяченої 40-річчю
Факультету радіотехніки та телекомунікацій
Інституту радіотехніки, зв'язку
та приладобудування ВНТУ*

Частина 1

**м. Вінниця, Україна
8 – 10 жовтня 2009 року**

УДК 621.38+621.39+681.2
С 91

Друкується за рішенням Вченої Ради Вінницького національного технічного університету Міністерства освіти і науки України

Відповідальний редактор Н.Г. Курилова

Матеріали статей опубліковані в авторській редакції

С 91 **Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП-2009).** Матеріали IV міжнародної науково-технічної конференції. м. Вінниця, 8 – 10 жовтня 2009 року. Частина 1. – Вінниця, 2009. – 108 с.

Збірка містить матеріали доповідей IV Міжнародної науково-технічної конференції з сучасних проблем радіоелектроніки, телекомунікацій та приладобудування за такими основними напрямками: теорія кіл, математичне моделювання, захист інформації та програмне забезпечення радіоелектронних, телекомунікаційних та біотехнічних систем; обробка сигналів і зображень в радіоелектронних та телекомунікаційних системах; пристрої радіоелектроніки та засоби телекомунікацій; радіотехнічні, телекомунікаційні та оптоелектронні комплекси та системи; радіоелектронні засоби в біомедичній інженерії; радіовимірювальні пристрої та системи; сучасні аспекти розвитку радіоаматорства

УДК 621.38+621.39+681.2

УДК 681.39

Лужецький В., Каплун В., Алєксєєва Т. (Україна, м.Вінниця)

ЗАХИСТ ПРОГРАМ З ВИКОРИСТАННЯМ ОБЧИСЛЕННЯ ВІДХИЛЕНЬ ЧИСЕЛ ВХІДНИХ ПОСЛІДОВНОСТЕЙ

Швидке зростання темпів розповсюдження персональних комп'ютерів, розвиток засобів обробки інформації, розширення кола користувачів, що мають безпосередній доступ до інформації – це все призвело до необхідності вирішення проблеми захисту. Ця проблема є особливо актуальною в наш час, оскільки піратство, несанкціонована модифікація, збут, крадіжка і копіювання програмних продуктів набувають масового характеру.

Автори доповіді пропонують методи, які дозволять захищати програмні продукти від несанкціонованого доступу, копіювання та використання.

Суть методу захисту полягає в тому, що виконуваний модуль програми, яка підлягає захисту, розглядається як послідовність байтів і становить вхідне повідомлення $Q_{поч.}$. Для реалізації запропонованого захисту це вхідне повідомлення доповнюється ключем K, отриманим певним чином. Ключем може бути як згенероване певним чином випадкове число, так і деяка ключова фраза (наприклад, пароль) або послідовність символів, отриманих як параметри складових комп'ютерної системи (серійні номера пристроїв, дати та версії виготовлення моделей, швидкісні характеристики, параметри файлової системи та ін.).

Таким чином, ключ тепер входить до складу вхідного повідомлення. Далі отримане повідомлення представляється у вигляді послідовності Q додатних цілих чисел певної розрядності, незалежно від їх фактичного вмісту:

$$Q = \{q_1, q_2, ..., q_N\},\ q_1 = K\ .$$

Вихідне повідомлення $Q_{рез.}$ буде являти собою послідовність відхилень між елементами вхідної послідовності і сусідніми числами.

$$Q_{рез.} = \{d_1; d_2; ...; d_N\},$$

$$d_1 = q_1 = K; d_i = q_i - q_{i-1},\ i = \overline{2 \div N}\ .$$

У результуючій послідовності початковим елементом буде перше число вхідної послідовності, яке є необхідним для однозначного відновлення початкового повідомлення. При зберіганні результуючої послідовності ключ відокремлюється від неї, тобто, отримуємо послідовність:

$$Q'_{рез.} = \{d_2; d_3; ...; d_N\}.$$

Правильне відновлення виконуваного файлу програми без знання ключа неможливе. А сам ключ для відновлення може зберігатися або на зовнішньому носії (у випадку використання якоїсь складної комбінації), або прихованого у деякому файлі (у випадку використання пароля або ключової фразу), або генеруватись наново, або знову отримуватись з параметрів комп'ютерної системи. А отже, легальна версія програми може коректно відновитись і правильно функціонувати лише при наявності ключа.

Запропонований метод захисту може бути використаний для кола програм певного призначення і дозволить обмежити несанкціоноване використання програм зловмисниками. Він не потребує застосування додаткових апаратних і програмних засобів. А у поєднанні з іншими методами може посилити стійкість і ефективність захисту.