Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 681.39

ВИКОРИСТАННЯ УЩІЛЬНЕННЯ ЧИСЛОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В. А. Каплун, старший викладач;
Т. М. Алєксєєва, студентка
Вінницький національний технічний університет
valuka@rambler.ru

Бурхливий розвиток інформаційних технологій і використання їх у різних областях людської діяльності привели до того, що крім задач передачі, збереження й обробки інформації виникла не менш, а в ряді випадків і більш важлива задача захисту інформації. Постали такі проблеми, як несанкціоноване використання алгоритмів, модифікація, поширення і збут програмних засобів. На сьогоднішній день системи захисту програмного забезпечення досить поширені і знаходяться в постійному розвитку завдяки поширенню ринку програмних продуктів і телекомунікаційних технологій.

У доповіді пропонуються використовувати методи захисту програм від несанкціонованого використання не тільки за допомогою прив'язки до деяких заздалегідь визначених характеристик комп'ютера, але й шляхом застосування подальшого ущільнення виконуваного модуля захищуваної програми. А для ущільнення обирати не стандартні словникові і імовірнісні методи, а методи, що базуються на обчисленні відхилень.

Суть захисту полягає в тому, що виконуваний модуль програми, яка підлягає захисту, розглядається як послідовність байтів і становить вхідне повідомлення F_{obj}. Ця

послідовність доповнюється ключем F_{key}. Ключем може бути як згенероване певним чином випадкове число, так і деяка ключова фраза (наприклад, пароль, логін тощо) або послідовність символів, отриманих як параметри складових комп'ютерної системи (серійні номера пристроїв, швидкісні характеристики, параметри файлової системи та ін.). В результаті злиття послідовностей F_{obj} і F_{key} отримуємо послідовність F, яка і становитиме вхідне повідомлення для ущільнення. Тепер це повідомлення, незалежно від його фактичного вмісту, представляємо у вигляді послідовності додатних цілих чисел певної розрядності. Далі здійснюємо ущільнення послідовності шляхом обчислення відхилень (від сусідніх чисел, від середнього значення, від центрів під діапазонів і т. д.). У результуючій послідовності F' початковим елементом буде ключова інформація F'_{key} (або її модифікована частина), яка є необхідною для однозначного відновлення модуля програми. При зберіганні отриманого файлу ключ F'_{key} відокремлюється від нього та може зберігатися на зовнішньому носії, бути прихованим у будь-якому файлі, генеруватись наново або знову отримуватись з параметрів комп'ютерної системи (в залежності від того, як він був початкове створений), а на диску залишається лише модифікований модуль програми F'_{obj}.

Після такої модифікації програмний модуль неможливо буде не тільки запустити на виконання, але й дослідити засобами статичного та динамічного аналізу. Для відновлення функціональних властивостей програми необхідно використати ключову інформацію і здійснити процес, зворотний обчисленню відхилень. Коректно відновитись і правильно функціонувати легальна версія програми зможе лише при наявності ключа.

Запропонований метод захисту може бути додатково посилений криптографічними методами або/і використанням антидампінгових засобів.