Харківський національний економічний університет
Університет ЛІОН 2 ім. Люм'єра
Віденський університет прикладних технічних наук
Представництво «Microsoft Україна»
Асоціація «Інформаційні технологій України»
Співтовариство ІТ-директорів України
АО «СПАЭРО плюс»

ПЕРША МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ПРОБЛЕМИ Й ПЕРСПЕКТИВИ РОЗВИТКУ ІТ-ІНДУСТРІЇ»

м. Харків, 18–19 листопада 2009 р.

Матеріали конференції

Харків
2009

УДК 004

Проблеми й перспективи розвитку IT-індустрії: *матеріали 1-ї Міжнародної науково-практичної конференції [«Проблеми й перспективи розвитку IT-індустрії»], (Харків, 18 – 19 листоп. 2009 р.) / редкол.: В.С. Пономаренко (відп. ред.)* – Харків: ХНЕУ, 2009. – 360 с.

Опубліковані матеріали, що охоплюють широке коло проблем, пов'язаних з інформаційними системами та технологіями. Представлені результати теоретичних та експериментальних досліджень в області моделювання бізнес-процесів, геоінформаційних технологій, захисту інформації, технологій мультимедійних видань, дистанційній освіті.

Матеріали публікуються в авторській редакції.

Проблемы и перспективы развития IT-индустрии: *материалы 1-й Международной научно-практической конференции [«Проблемы и перспективы развития IT-индустрии»], (Харьков, 18-19 ноября 2009 г.) / редкол.: В.С. Пономаренко (отв. ред.)* – Харьков: ХНЭУ, 2009. – 360 с.

Опубликованы материалы, охватывающие широкий круг проблем, связанных с информационными системами и технологиями. Представлены результаты теоретических и практических исследований в области моделирования бизнес-процессов, геоинформационных технологий, защиты информации, технологий мультимедийных изданий, дистанционного образования.

Материалы публикуются в авторской редакции.

Problems and prospects of the development of IT industry: materials of 1-st International scientifically-practical conference [«Problems and prospects of development of IT-industry»], (Kharkov, November, 18-19th, 2009) / Khark. Nation. Econ. Univ.; editor: V.S. Ponomarenko [etc.]. – Kh.: Publish house SevNTU, 2009. – 360 p.

The materials, covered the wide content of problems, which are gathered with information technologies are published in this article. The results of theoretical and practical discoveries in the analysis and synthesys of managered and information systems, systems of support of given decisions are represented here.

The matherials are published in the author's redaction.

Друкується за рішенням вченої ради ХНЕУ,
протокол №2 від 26.10.2009 р.

УДК 681.39

В.А. Лужецький, д.т.н., професор
зав. каф. захисту інформації,
Вінницький національний технічний університет
м. Вінниця, Україна
В.А. Каплун, ст. викладач
Вінницький національний технічний університет
м. Вінниця, Україна
valuka58@gmail.com

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ МЕТОДІВ УЩІЛЬНЕННЯ

Проблема захисту інформації, що зберігається у комп'ютерних системах, є досить актуальною в наш час, оскільки піратство, несанкціонована модифікація, збут, крадіжка і копіювання програмних продуктів набувають масового характеру. Для вирішення цієї проблеми існує велика кількість методів, - це і різноманітні методи прив'язки, антиналгоджувальні і антидампінгові прийоми, пакування виконуваних модулів, обфускація програм, методи, шифрування та ущільнення інформації і т.і.

Автори доповіді пропонують використовувати для захисту програм та інших файлів підхід, що має в основі методи ущільнення, які базуються на обчисленні відхилень. Вихідний файл, що підлягає захисту, пред¯ставляється у вигляді послідовності цілих додатних чисел, перетворений – у вигляді послідовності відхилень

елементів початкової послідовності від певним чином вибраних величин. Саме спосіб вибору цих величин і обумовив створення класифікації методів ущільнення, що базуються на такому підході. У цій класифікації виділено дві групи:

1) методи, що не вимагають обчислення числових характеристик чисел вхідної послідовності (відхилення від сусідніх елементів, від констант, від значень апроксимуючої функції);

2) методи, що використовують статистики (відхилення від центрів піддіапазонів, від середніх, мінімальних або максимальних значень у групах або піддіапазонах, від накопиченого середнього).

В усіх цих методах ущільнення досягається за рахунок того, що відхилення, за певних умов, можуть бути мен¬ши¬ми, ніж самі елементи почат¬кової послідовності. Але для однозначного відновлення інформації необхідно зберігати певну додаткову інформацію, властиву кожному із запропонованих методів.

Для реалізації захисту файлу F він доповнюється ключем K, отриманим будь-яким чином: це може бути і згенероване певним чином випадкове число, деяка ключова фраза, послідовність символів, отриманих як параметри складових комп'ютерної системи (серійні номера пристроїв, дати і версії виготовлення моделей, швидкісні характеристики, параметри процесора та ін.). Отриманий файл F` розглядається як послідовність байтів і, перетворений у послідовність n-розрядних цілих додатних чисел, становить вхідне повідомлення Qпоч.. При цьому розрядність n може обиратися довільно або співпадати з розрядністю самого ключа K.

Таким чином, ключ тепер входить до складу вхідного повідомлення:

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

Вихідне повідомлення Q`. буде послідовністю відхилень між елементами вхідної послідовності і сусідніми числами.

$$Q' = \{d_1; d_2; ...; d_N\}, \text{ де } \; d_1 = q_1 = K; d_i = q_i - q_{i-1}, \; i = \overline{2 \div N} .$$

При зберіганні результуючої послідовності ключ відокремлюється від неї, тобто, отримуємо послідовність:

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

Ця послідовність відхилень у вигляді потоку байтів зберігається на носії інформації у вигляді файлу F``. Ключова інформація може зберігатися окремо від захищеного файлу: у тілі програми, у спеціальних числових файлах, у резервних або збійних секторах, у системному реєстрі, після ознаки кінця одного з файлів на диску, на зовнішньому носії (у випадку використання деякої складної комбінації) і т.д. При необхідності ключ може генеруватись заново або знову отримуватись з параметрів комп'ю¬терної системи. Отже, легальна версія програ-

ми може коректно відновитись і правильно функціонувати лише при наявності ключа. Сам процес відновлення початкового файлу здійснюється у зворотному порядку: ключ К об'єднується з файлом F``; отриманий файл F` представляється у вигляді послідовності n-розрядних цілих додатних чисел; за відомими відхиленнями і при наявності першого елемента відновлюються члени послідовності Q, що відповідають файлу F:

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

Тепер, видаливши ключ, знову отримуємо початковий файл, готовий до запуску. Для реалізації цього процесу може бути розроблено окремий модуль, який і запускатиме програму на виконання, а після її відпрацювання знову модифікувати її і зберігати у захищеному вигляді.

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.

Список літератури: 1. Балашов К.Ю. Сжатие информации: анализ методов и подходов. – Минск: Инт техн. Кибернетики НАН Беларуси, №6, 2000. – 42 с.2. 2. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ, 2003. -384с.

УДК 004.738.5.057.4

А.А. Засядько, д.т.н., професор,
кафедра вищої математики та інформаційних технологій
Черкаський інституту банківської справи
Університету банківської справи Національного банку України
О.В. Клювак, аспірант,
Університет банківської справи Національного банку України
м.Київ, Україна
oksana_klyuvak@bigmir.net

АНАЛІЗ МЕХАНІЗМУ ДІЇ ПРОТОКОЛІВ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ ПОБУДОВІ ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМ НА ОСНОВІ БАНКІВСЬКИХ КАРТОК

Аналіз механізму дії протоколів в електронній комерції, зокрема на прикладі SET та SSL, тобто алгоритмів, що визначають порядок взаємодії учасників транзакції (власника карти, торгівельної точки, обслуговуючого банку, банку-емітента, центру сертифікації) і формати повідомлень, якими учасники під час електронних