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 621.391

УЩІЛЬНЕННЯ ДАНИХ ЯК МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ

В. П. Майданюк, к.т.н., доцент
Вінницький національний технічний університет
maydan2000@mail.ru

У роботі К.Шеннона “Теорія зв’язку в секретних системах” (1949р.) було показано, що для деякого випадкового шифру кількість знаків шифротексту, отримавши який криптоаналітик при необхідних обчислювальних ресурсах зможе відновити ключ (тобто розкрити шифр), становить:

$$n = \frac{H(Z)}{r \log N},$$

де H(Z) – ентропія ключа, r – надлишковість відкритого тексту, N-обсяг алфавіту. З виразу видно, що зниження надлишковості (ущільнення даних) може значно збільшити криптостійкість навіть для коротких ключів.

Донедавна алгоритми ущільнення даних і криптографічного захисту розвивались окремо, що призводило до значних обчислювальних витрат, оскільки при передачі і зберіганні файлів виникає необхідність в подвійному перетворенні інформації - спочатку ущільнення, а потім шифрування ущільненого файлу. Тому актуальною є розробка таких алгоритмів шифрування даних, які б за один прохід виконували шифрування інформації з її одночасним ущільненням. Головним критерієм при виборі алгоритму ущільнення для шифрування даних є мінімум затрат на адаптацію його до розв’язування нових задач. С цієї точки зору заслуговують на увагу алгоритми ущільнення, які форму-

ють масиви символів перед виконанням ущільнення, що може бути використано при реалізації алгоритму шифрування. Іншими важливими критеріями є адаптивність алгоритму ущільнення, коефіцієнт ущільнення, простота технічної реалізації. Аналіз основних алгоритмів ущільнення даних без втрат показав,що найбільші переваги, з точки зору застосування їх до шифрування даних, мають два алгоритми: ущільнення методом MTF (Move To Front); ймовірнісний метод ущільнення.

Ці алгоритми передбачають формування таблиці символів перед виконанням ущільнення даних, яка може бути сформована за ключем шифру з використанням, наприклад, генератора псевдовипадкових чисел. До того ж ці алгоритми є адаптивними, тобто не вимагають передачі додаткової інформації, яка могла бути використана зловмисниками для злому шифру, а також характеризуються простою технічною реалізацією.

Для одночасного ущільнення і шифрування даних може використовуватись така схема:

- з використанням генератора псевдовипадкових чисел за ключем шифру генерується алфавіт повідомлення;
- виконується ущільнення згідно з наведеним методом.

Додаткові затрати відсутні, оскільки генерація символів алфавіту виконується в будь-якому випадку. При незначних додаткових затратах можливо застосувати комбінацію методів, яка включає два основні етапи:

- етап1. Кодування за ступенем новизни для стиснення і шифрування методом багатоалфавітної підстановки.

етап2. Шифрування за допомогою додаткового генератора ПВЧ з довжиною псевдовипадкової послідовності більшої довжини файлу.