УДК 004.056.5 : 519.728

КОМБІНОВАНИЙ МЕТОД УЩІЛЬНЕННЯ ТА ШИФРУВАННЯ ДАНИХ

[1]В. А. Лужецький, д.т.н., професор;
[2]Т. М. Чеборака, магістрант
Вінницький національний технічний університет
[1]lva_zi@mail.ru, [2]altamira_90@mail.ru

З кожним роком зростають обсяги інформації, яка передається та зберігається. Це в свою чергу вимагає збільшення обсягів пам'яті і наявності високошвидкісних каналів передавання в сучасних інформаційних системах. Однак це призводить до постійного збільшення вартості таких систем. Для зменшення обсягів інформації, що зберігається і передається, економічно вигідним є застосування методів ущільнення. Крім того, інформація, що зберігається і передається часто має певну цінність, і тому виникає потреба у її захисті. Отже, актуальним є розробка методів перетворення інформації, які забезпечують одночасно не лише зменшення обсягу інформації, але й її захист від несанкціонованого доступу.

В роботі пропонується комбінований метод ущільнення та шифрування даних, що базується на поєднанні процедур ущільнення та шифрування.

Суть цього методу така. Спочатку вхідна інформація перетворюється із застосуванням певного набору методів ущільнення, а потім шифруванню підлягають тільки окремі дані, що визначають правила відновлення інформації і без знання яких неможливо відновити інформацію на основі частини ущільнених даних. Вхідна інформація розбивається на блоки

розрядності n. Кожен блок аналізується на предмет використання найкращого методу ущільнення на основі відкидання послідовності однакових символів: у старших розрядах, у молодших розрядах, у молодших і старших розрядах. Можливий також і випадок, коли жоден із методів не зменшує обсяг вихідного блоку даних. Тоді цей блок не ущільнюється і залишається без змін. Таким чином можливі чотири варіанти блоків даних в ущільненій послідовності. З метою розпізнавання цих блоків в кінець ущільненої послідовності записується ознака перетворення кожного блоку, яка вказує на присутність перетворення та варіант використаного методу ущільнення (рис. 1).

Поле перетворених блоків	Поле ознак перетворення

Рисунок 1 – Структура ущільненої послідовності даних

Після проведення ущільнення вихідної послідовності даних виконується процедура зашифрування лише послідовності ознак перетворення ущільненої послідовності, що містить необхідну інформацію для відновлення вихідної послідовності даних. Для реалізації процедури зашифрування використовується будь-який блоковий шифр.

Перевагами запропонованого методу є:

– зменшення обсягу вихідного файлу;

– швидка реалізація процедур зашифрування та розшифрування, оскільки ці процедури застосовуються лише до частини ущільненої послідовності даних і їх швидкодія пропорційна розміру поля ознак перетворення, що є меншим від вихідної послідовності у $D \big/ 2\lceil D/n \rceil$ раз, де D – розмір вихідної послідовності даних в бітах, n – розрядність ущільнюваних блоків.