Міністерство освіти і науки України
Вінницький національний технічний університет
Національний технічний університет України "КПІ"
Інститут кібернетики НАНУ
Південний Федеральний Університет (Росія)

Тези доповідей першої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації"

м. Вінниця, Україна
15-17 травня 2007 року

Тезисы докладов первой Международной научно-практической конференции "Методы и средства кодирования, защиты и сжатия информации"

г. Винница, Украина
15 - 17 мая 2007 года

ВНТУ 2007

УДК 681.32+621.391
М54

Відповідальний редактор В.А. Лужецький

Матеріали статей опубліковані в авторській редакції

М54 **Методи та засоби кодування, захисту й ущільнення інформації.** Тези доповідей першої Міжнародної науково-практичної конференції. м. Вінниця, 15-17 травня 2007 року. – Вінниця: ВНТУ, 2007. – 140 с.

Збірка містить матеріали доповідей першої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за чотирма основними напрямками: методи та засоби кодування інформації; методи та засоби захисту інформації; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації

УДК 681.32+621.391

УДК 681.32

ШИФРОВАНИЕ ДАННЫХ ПРИ ИХ СЖАТИИ

В. П. Майданюк, к.т.н., доцент
Винницкий национальный технический университет
e-mail: maydan2000@mail.ru

Основной целью кодирования или сжатия данных является превращение входного потока символов в поток битов минимальной длины. Однако, при сжатии данных некоторыми методами существует возможность одновременного шифрования данных почти без дополнительных вычислительных затрат.

Среди известных алгоритмов сжатия наибольшие преимущества с точки зрения применения их к шифрованию данных имеют два алгоритма:

- сжатие методом MTF (Move To Front);
- вероятностный метод сжатия.

Основной особенностью этих алгоритмов является формирование таблицы символов перед выполнением сжатия данных. Если сформировать эту таблицу с использованием, например, конгруэнтного генератора псевдослучайных чисел у которого начальное значение равно ключу шифра, а потом выполнить сжатие с использованием одного из этих методов, то получим зашифрованное сообщение. Дополнительные затраты отсутствуют, поскольку генерация символов алфавита выполняется в любом случае. К тому же эти алгоритмы являются адаптивными, то есть не требуют передачи дополнительной информации, которая могла быть использована злоумышленниками для взлома шифра, а также характеризуются простой технической реализацией.