УДК 681. 32

БЛОКОВИЙ ШИФР НА ОСНОВІ ПЕРЕСТАНОВОК ТА ПІДСТАНОВОК

Горбенко І. С.
Науковий керівник – д.т.н., проф.. Лужецький В. А.

Існуючі блокові шифри не завжди забезпечують належну стійкість, а їх ускладнення з метою її підвищення призводять до зниження ефективності – збільшення часу роботи та обсягів апаратних витрат.

Запропонований алгоритм заснований на базових операціях шифрування – заміни та перестановки, а особливістю алгоритму є застосування нових криптографічних підходів – використання блоків різної довжини та зчитування цих блоків з файлу у випадковому порядку.

Файл розбивається на блоки різної довжини за повною або локальною випадковістю. В першому випадку псевдовипадкові числа від 0 до 7 визначають розрядності послідовних блоків (1 ÷ 8 машинних одиниць). Такі числа визначають трьома послідовними бітами станів генератора на регістрі зсуву зі зворотнім зв'язком (РЗЗЗ). В другому – весь файл розбивається на рівні блоки і кожен блок ділиться на підблоки різної довжини.

Наступна операція – підстановка. Нехай множина блоків: $B = \{b_i\}$.

Тоді блок-результат: $b_i^* = b_i \oplus r_i$, де r_i – випадкові числа (розрядністю мінімальної або максимальної довжини блока).

Кількість блоків ***N*** підраховується лічильником за значеннями довжин блоків, або за довжиною файлу (в байтах), лінійним конгруентним генератором формуються адреси бітів, що послідовно вибираються.

Перестановка блоків: множина блоків: $B = \{b_i\}$; $i = \overline{1 \div N}$.

Лінійний конгруентний генератор: $x_i = (a \cdot x_{i-1} + c) \bmod N$.

Новий порядок блоків: $b_1^* = b_{x_0}$, $b_2^* = b_{x_1}$.

Ключ має три основні складові: параметри генератора РЗЗЗ, що формує довжини блоків (*S* (32 біти), *P(x)* (16 бітів)), параметри для перестановок – лінійний конгруентний генератор (*a*, *c* (по 32 біти), x_0 (64 біти)) та параметри генератора РЗЗЗ для підстановок. Таким чином, розрядність використовуваного ключа складає 224 біти.

Розроблений метод підвищує криптографічну стійкість за рахунок блоків різної довжини (більшої кількості можливих комбінацій) та зменшує час шифрування та апаратні витрати за рахунок невеликої кількості операцій.