УДК 004.056.55

МЕТОД БЛОКОВОГО ШИРФРУВАННЯ НА ОСНОВІ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ КРИПТОПРИМІТИВІВ

В.А. Лужецький, д.т.н., професор,
А.В. Остапенко, аспірант
Вінницький національний технічний університет
asja87@gmail.com

Потреба вирішення проблеми захисту електронної інформації обумовлює актуальність розробки програмних шифрів та перспективи їх розвитку. Пропонується будувати блоковий шифр використовуючи псевдовипадкову (з точки зору криптоаналітика) послідовність криптопримітивів. Ідея цього методу полягає в тому, що перетворення на кожному із раундів складається з елементарних перетворень набір і послідовність виконання яких визначаються ознаками, що формуються з ключової інформації .

Входячи з вищесказаного пропонується модель блокового шифру:

$$\sum=\{\mathbf{M}, \mathbf{K}, \mathbf{F_E}, \mathbf{F_D}, \mathbf{Q}, \mathbf{B}, \mathbf{C}\},$$

де $\mathbf{M}=\{m_i\}$ – множина відкритих повідомлень;
$\mathbf{K}=\{k_i\}$ – множина ключів;
$\mathbf{F_E}=\{F_{Ei}\}$ – множина функцій зашифрування;
$\mathbf{F_D}=\{F_{Di}\}$ – множина функцій розшифрування;
$\mathbf{Q}=\{q_i\}$ – множина ознак;
$\mathbf{B}=\{b_i\}$ – множина базових операцій;
$\mathbf{C}=\{c_i\}$ – множина криптограм.

Запропонована множина **Q**, залежно від ознаки $q \in Q$, на базі використання визначених операцій **B**, буде