УДК 004.056.055

# КЛАСИФІКАЦІЯ БЛОКОВИХ ШИФРІВ, ЩО ВИКОРИСТОВУЮТЬ ПСЕВДОНЕДЕТЕРМІНОВАНУ ПОСЛІДОВНІСТЬ КРИПТОПРИМІТИВІВ ЗА БАЗОВИМИ ОЗНАКАМИ

**А. В. Остапенко, асистент**
**Вінницький національний технічний університет**
**asja87@gmail.com**

На сьогоднішній день при розробці нових підходів до побудови симетричних блокових шифрів (СБШ) для покращення їх основних характеристик проводяться дослідження процедури розгортання ключа, режимів блокового шифрування та операцій, що використовуються у функціях раундового перетворення.

Одним із сучасних напрямів розробки СБШ підвищеної швидкості є створення недетермінованих шифрів де формування алгоритмів шифрування відбувається під керуванням секретного параметра.

Для впровадження ефекту недетермінованості в процес конструювання СБШ доцільно розглянути основні складові елементи блокового шифру.

Для будь якого СБШ можна визначити його базові ознаки:

1. Ознака структури блоку
2. Ознака функції раунда перетворення (ФРП).

Структура блоку в свою чергу характеризується ознакою його розрядності та ознакою кількості підблоків на які розбивається блок на раундах шифрування.

ФРП характеризується послідовністю застосувань деяких операцій із набору базових операцій СБШ.

Значення ознак можуть бути постійними (*C*) та змінними (*V*).

В свою чергу постійні значення означають незмінність значення ознаки на протязі усіх раундів шифрування та можуть бути:

- залежні від секретного параметра(*Ck*): конкретне значення ознаки певним чином визначається з ораного секретного параметра;
- незалежні від ключа (*C*): конкретне значення ознаки не залежить від значення ключа.

Змінні значення ознак означають зміну значень ознаки на всіх (або деяких) раундах шифрування та можуть бути:

- змінними залежними від секретного параметра (V);
- умовно змінним (Vc), коли значення ознаки змінюється відповідно до заданої умови, що не є секретом.

Виходячи із розглянутих базових ознак запропонована класифікація СБШ, що враховує можливість побудови шифрів із змінними значеннями базових ознак.

Розглядаючи представників сучасних СБШ можна казати, що більша їх частина відноситься до класу (С, С, С). Тобто усі значення ознак є постійними та заданими для всіх ітерацій. СБШ з керованими операціями відносяться до класу (С, С, V) так як структура ФРП є змінною та залежною від ключових параметрів. СБШ з гетерогенною структурою можна віднести до класу (С, С, *Ck*).

Отже, враховуючи класи можливості яких вже частково реалізовані, запропонована класифікація дозволяє описати нові класи СБШ, що використовують псевдонедетерміновану послідовність криптопримітивів для подальшого їх дослідження.