

## РОЗРОБКА СТІЙКИХ ДО ЛІНІЙНОГО ТА ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ ЗАСОБІВ ШИФРУВАННЯ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ.

Яровенко А.О.

Науковий керівник – к.т.н., доц. Бевз О. М.

На сьогоднішній день швидкими темпами відбувається впровадження новітніх інформаційних технологій, все більші об'єми інформації передаються по незахищених відкритих лініях зв'язку. Тому з'явилося широке різноманіття методів захисту інформації від небажаного доступу, чільне місце серед яких займають криптографічні методи захисту інформації. Метою даного дослідження є підвищення стійкості шифрування блочного шифру на основі криптографічного перетворення, що реалізується SPN-мережею, за рахунок підвищення криптографічних показників нелінійного перетворення та вибору оптимальної структури лінійного перетворення.

SPN-шифри обов'язково включають етапи додавання раундового ключа, підстановки (substitution, що реалізується за рахунок використання S-боксів) та перестановки (permutation). Було розроблено програмні додатки, для побудови таблиці лінійної апроксимації за заданими S-боксами. Було проаналізовано такі таблиці для полів Галуа, піднесених до різних степенів. Варіант S-боксу для  $(GF(2^4))^9$ , виявився найбільш вдалим. Для даного S-боксу було визначено розподіл значень кореляційних коефіцієнтів, що дало змогу оцінити кількість відкритих текстів для результативного проведення лінійного криптоаналізу, що становила - 1141, що краще на 3% за результат для шифру AES.

Було визначено, що для реалізації даного шифру, буде використана гніздова структура підстановочно-перестановочної мережі, що включає 3 рівні перестановки. На нижньому рівні буде застосований код  $KMB_H$ , на середньому рівні код –  $KMB_C$ , і на верхньому рівні –  $KMB_B$ . Було чисельно оцінено кількість активних S-боксів при різних їх комбінаціях цих перетворень. Серед SPN мереж, в яких розмір S-боксу становить 8 біт максимальну кількість активних S-боксів формує SPN мережа з  $KMB_B = (2,1,2)$ ,  $KMB_C = (2,1,2)$  та  $KMB_H = (32,16,17)$ , і ця кількість становить - 85. В SPN мережі з S-боксами розміром 16 біт максимальна кількість активних S-боксів буде реалізована SPN мережею з  $KMB_B = (2,1,2)$ ,  $KMB_C = (2,1,2)$  та  $KMB_H = (16,8,9)$ , і ця кількість становить – 45, що у 1,8 разів більше ніж у шифрі Rijndael. Було розраховано імовірності лінійної  $P$  та диференційної  $Q$  характеристик раунду, утвореного трьохрівневого гніздового