Уніфікація схеми блоків кодування і декодування в шифрувальних пристроях

Бурмістров С. В., *аспірант*
Черкаський державний технологічний університет, м. Черкаси

Одними із найбільш розповсюджених шифрувальних пристроїв (ШП) є апарати, призначені для посимвольного кодування текстової інформації. Досить тривалий термін експлуатації даних ШП в комерційних мережах вказує на достатньо високий рівень захисту даного методу шифрування в модифікованому вигляді.

Метою даної роботи є створення уніфікованої схеми прийомної (ПрЧ) і передаючої частини (ПдЧ) ШП пристрою для посимвольного кодування текстової інформації в модифікованому вигляді.

Ідея посимвольного методу шифрування в модифікованому вигляді полягає в тому, що на кожний наступний передаваємий символ використовується новий ключ – поточний фіксований ключ кодування (ПФКК). Основною проблемою, що виникає в процесі проектування вказаного ШП, є те що ПФКК не дорівнює поточному фіксованому ключу декодування (ПФКД). Процес уніфікації ПдЧ і ПрЧ в ШП полягає в тому, що вони складаються з аналогічних блоків. Єдина відмінність, так як між ПФКК і ПФКД існує чітка відповідність, пропонується в схемі ПрЧ використовувати додатковий блок – блок обчислення ПФКД на основі ПФКК. Даний блок отримують шляхом зведення розв'язку задачі до процесу мінімізації системи частковозначених булевих функцій. З метою отримання максимальної швидкодії блоку кінцева схема має вигляд 2-рівневої комбінаційної схеми логічних елементів. В порівнянні з використанням аналогічної схеми на основі стандартної програмованої логічної матриці отримано ущільнення схеми в 5,63 рази.

Науковий керівник: Рудницький В.М., *професор*