УДК 658.012.011.56:681.3.06
Огородник Л.–ст. гр. КСМм-51
Тернопільська академія народного господарства

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ НА ОСНОВІ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Науковий керівник: к.т.н., доцент Трембач Р.Б.

Криптографія є важливою частиною всіх інформаційних систем. На даний час реалізовані алгоритми шифрування DES та RC5.

Головна задача розроблюваного макету - забезпечити можливість дослідження впливу зовнішніх дестабілізуючих факторів на шифратор гамування, що містить генератор псевдовипадкових чисел побудований на базі лінійних рекурентних співвідношень у регістрах зсуву.

Досліджуваним пристроєм вибрано апаратну реалізацію алгоритму гамування. Суть алгоритму гамування в тому, що на відкритий текст, представлений у вигляді бітової послідовності, накладається гама ключем. У даному випадку накладання - виконання операції XOR із вхідними даними (біти) вхідного повідомлення на ключ. XOR - виключаюче OR - приймає значення в '1' тоді і тільки тоді, коли один із операндів має значення '1', а інший '0', в іншому випадку — '0'.

Одним із ключових функціональних вузлів даного макету є генератор псевдовипадкових послідовностей. Результати роботи даного вузла використовуються як ключ шифрування.

Дослідження статистичних характеристик генератора дозволяє оптимізувати проведення диференційного аналізу і дає базу для досліджень параметрів впливу зовнішніх дестабілізуючих факторів на досліджуваний пристрій.

Для симуляції роботи генератора ПВП (псевдовипадкових послідовностей) на базі лінійних рекурентних співвідношень у лінійних регістрах зсуву з оберненим зв'язком розроблено алгоритмічне забезпечення.

Алгоритмічне забезпечення складається з ініціалізації та імітації роботи. Перша частина алгоритмічного забезпечення проводить діалог із користувачем, з метою отримання ініціалізуючих значень генератора. Друга частина імітує саме роботу ЛРР (лінійних рекурентних регістрів) (для цього проводиться ініціалізація даних, запит параметру кількості проведення ітерації генерування, процедура генерування наступного псевдовипадкового значення).