УДК 621.3

МЕША Д. М., ***РИСОВАНИЙ О.М.,*** к.т.н., доц.

ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ ЧИСЕЛ

Найважливіша характеристика генератора псевдовипадкових чисел - інформаційна довжина періоду, після якого числа або почнуть просто повторюватися, або їх можна буде передбачати. Ця довжина фактично визначає можливе число ключів системи і залежить від алгоритму отримання псевдовипадкових чисел. Необхідну довжину періоду визначає ступінь секретності даних. Чим довше ключ, тим важче його підібрати. Проте не тільки довжина ключа гарантує його стійкість до злому. В тому випадку, якщо зміст шифрованого повідомлення життєво важливо для держави і їм зацікавиться національна служба безпеки, то наперед потрібно бути готовим до невдачі в так нерівному змаганні. Люди із спецслужб легко знайдуть необхідний ключ своїми специфічними неджентльменськими методами, далекими від математики і криптографії. Швидше за все, ключ їм дасть сам власник на блюдці з голубою облямівкою і буде цьому щиро радий.

Друга проблема полягає в наступному: на підставі чого можна зробити висновок, що гамма конкретного генератора є непередбачуваною? Поки в світі немає ще універсальних і практично перевіряються критеріїв, що дозволяють затверджувати це. Невідома і загальна теорія криптоаналізу, яка могла б бути застосована для такого доказу, за винятком все зростаючої кількості конкретних чинів аналізу, вироблених для різних практичних цілей. Інтуїтивно випадковість сприймається як непередбачуваність. Щоб гамма вважалося випадковою, як мінімум необхідно, щоб її період був дуже великим, а різні комбінації біт певної довжини рівномірно розподілялися по всій її довжині. Отже, друга вимога до ряду полягає в підтверджуваній статистично подібності його властивостей справжньої випадкової вибірки. Кожний порядок елементів гамми повинен бути так само випадковий, як і будь-хто інший. Це вимога статистики можна тлумачити і як складність закону формування ряду псевдовипадкових чисел. Практично, якщо по достатньо довгій реалізації цей закон розкрити не вдається ні на статистичному рівні, ні аналітично, то цим потрібно задовольнитися. Чим довше необхідна довжина ряду, тим жорсткіше до нього вимоги.