УДК 621.391.7

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПІДВИЩЕННЯ БЕЗПЕКИ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Каменчук О.О.
Науковий керівник – проф., к.т.н. Яремчук Ю.Є.

Збільшення кола користувачів систем і розподіл завдань, що виконуються за допомогою мереж, призвели до усвідомлення першочергової важливості проблем, пов’язаних із забезпеченням інформаційної безпеки під час міжмережевої взаємодії, перш за все з використанням відкритих каналів передавання даних, які створюють потенційну можливість для дій зловмисника.Однією з важливих галузей досліджень у системах, мережах і пристроях ІТ є дослідження та розроблення нових методів захисту інформації та забезпечення інформаційної безпеки систем, мереж і пристроїв. Захист інформації значною мірою базується на використанні криптографічних методів, пов'язаних із шифруванням даних.

Широкого практичного застосування отримали симетричні системи шифрування інформації, побудовані на основі блокових або потокових шифрів із секретним ключем. Серед них шифр Вернама застосовується у системах, де пропускна здатність відкритого та закритого каналів є однаковою. При цьому готують два однакових рядки з випадковими цифрами ключа таким чином, що ключовий рядок повинен просуватися абсолютно синхронно зі своїм дублікатом, використовуваним для шифрування.

Недоліком даного шифру є те, що для кожного біта інформації, що передається, повинен бути заздалегідь підготовлений біт ключової інформації, причому ці біти повинні бути випадковими. Під час шифрування великого обсягу даних це є серйозним обмеженням, тому така система використовується тільки для передавання повідомлень найвищої секретності.

Щоб вирішити проблему попереднього передавання секретного ключа великого обсягу, було придумано багато схем генерації дуже довгих потоків псевдовипадкових чисел із кількох коротких потоків, що застосовуються за певним алгоритмом. Одержувача шифрованого повідомлення при цьому необхідно забезпечити таким саме генератором, як і у відправника.

Одним із підходів до побудови подібних генераторів може бути використання двох або більше бітових рядків, з яких зчитані дані побітно складаються для отримання «змішаного» потоку. Таким чином кілька коротких рядків замінюють один довгий, але виходить, що при цьому внутрішні періодичності можуть допомогти аналітику в розкритті шифру.

Розглянуто можливість використання такого підходу до вдосконалення шифру Вернама із забезпеченням при цьому підвищення рівня безпеки криптографічних систем.