ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Бєрбєр О.В.

Науковий керівник – зав. каф. Інформаційної безпеки

док. техн. наук, проф. Мазурков М.І.

При гамуванні великих повідомлень і потоків даних використовуються генератори псевдовипадкових послідовностей (ПВП).

Генератор псевдовипадкових чисел - алгоритм, що генерує послідовність чисел, елементи якої майже незалежні один від одного і підкоряються заданого розподілу (зазвичай рівномірному). Вони класифікуються на: криптографічні (з використанням функцій E_K потокових шифрів, функцій E_K блокових шифрів, односторонніх функцій, блоків стохастичного перетворення) і не криптографічні (конгруентні, на регістрах зсуву з зворотними зв'язками, що функціонують на кінцевих полях).

Генератор ПВП, орієнтований на використання в системах захисту інформації, повинен відповідати таким вимогам: криптографічна стійкість, гарні статистичні властивості (ПВП за своїми статистичними властивостями не повинна відрізнятися від істинно випадкової послідовності), великий період формованої послідовності, ефективна апаратна і програмна реалізація.

При використанні крипто стійкого генератора ПВП три наступні завдання для противника обчислювально-неможливо розв'язати:

- визначення (*i-1*)-го елемента γ_{i-1} послідовності на основі відомого фрагмента гами $\gamma_i\gamma_{i+1}\gamma_{i+2}.....\gamma_{i+b-1}$ кінцевої довжини *b;*

- визначення (*i+1*)-го елемента γ_{i+1} послідовності на основі відомого фрагмента гами $\gamma_i\gamma_{i+1}\gamma_{i+2}.....\gamma_{i+b-1}$ кінцевої довжини *b;*

- визначення ключової інформації за відомим фрагментом гами кінцевої довжини.

Статистично безпечний генератора ПВП повинен задовольняти наступним вимогам: жоден статистичний тест не виявляє в ПВП будь-яких закономірностей, при ініціалізації випадковими значеннями генератор породжує статистично незалежні ПВП, нелінійне перетворення F_k, що залежать від секретної інформації (ключа k).

Для аналізу статистичної безпеки генераторів ПСП використовуються дві групи тестів:

- графічні тести. Статистичні властивості послідовностей відображаються у вигляді графічних залежностей (перевірка серій, перевірка на монотонність, графічний спектральний тест);
- оціночні тести. Статистичні властивості послідовності визначаються числовими характеристиками (тести Кнута, “DIEHARD”).

Список використаної літератури

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стенографии // Москва Горячая линия-Телеком 2010г.

2. Иванов М.А., Чугунков И.В. Теория, применения и оценка качества генераторов псевдослучайных последовательностей // Москва 2003 г.