ИССЛЕДОВАНИЕ МАТЕМАТИЧЕСКИХ ХАРАКТЕРИСТИК МАССИВОВ ДАННЫХ ДЛЯ ПОВЫШЕНИЯ КАЧЕСТВА МАСКИРОВАНИЯ ИНФОРМАЦИИ

Д. В. Сплюхин, А. А. Мартынов, Д. Б. Николаев

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Важное место в защите информационных систем занимает обеспечение конфиденциальности и целостности информации. Современными способами которых являются встраивание информации с целью ее скрытой передачи, построение и адаптация цифровых водяных знаков, формирование идентификационных номеров для защиты от копирования и несанкционированного использования. В качестве номинального элемента для обеспечения высокой криптографической стойкости при маскировании информации используются сформированные тестовые последовательности, начальные заполнения, которые определяют качество и заданные свойства информационной составляющей системы. Основой для формирования последовательностей являются генераторы псевдослучайных последовательностей (ПСП).

На рис. 1 рассмотрен генератор ПСП с входными/выходными величинами, условиями и средствами.

Рис. 1. Генератор ПСП как процесс

Генераторы случайных и псевдослучайных последовательностей являются связующим звеном в обеспечении информационной безопасности. Поскольку такие генераторы применяются во многих криптографических задачах, например, формировании случайных параметров и ключей систем преобразования информации, то требования, предъявляемые к ним, оказываются достаточно высокими.

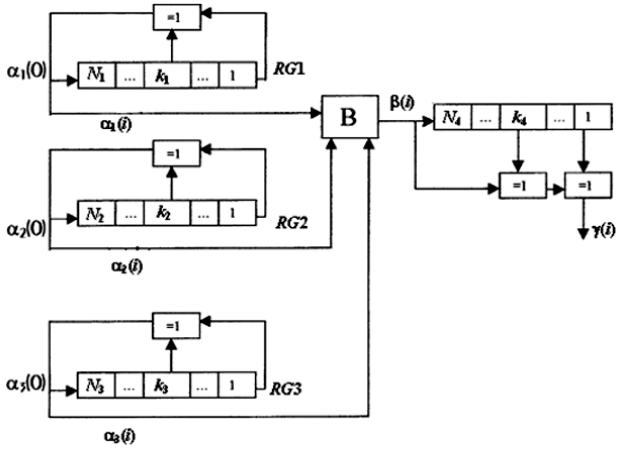
Генераторы ПСП широко используются при решении сложных статистических задач с начальными условиями, также находят применение в имитационном моделировании автоматизированных систем. Проверка качества (тестирование) генераторов ПСП, используемых в криптографических приложениях, является важной задачей как в практическом, так и в теоретическом плане. От качества выходной последовательности генератора ПСП зависит качество системы, в которой он используется, точность результатов моделирования, стойкость средств защиты информации. Существует необходимость в повышении качества маскирования информации, так как от него зависят криптографические свойства информационной системы, в которой используется данный механизм защиты информации. Отсюда и формируется цель данной работы: исследование математических характеристик массивов данных для повышения качества маскирования информации.

На начальном этапе проводился анализ генераторов псевдослучайных последовательностей, который показал и дал обоснование основным методикам разработки и проверки качества генераторов псевдослучайных последовательностей. В ходе работ и исследований разработан программный комплекс модульного типа для осуществления анализа исследуемых данных информационных выходных потоков гетерогенных псевдослучайных последовательностей, который отвечает самым высоким требованиям по универсальности применения, по эффективности и безопасности.

Для решения поставленной цели принято решение о проведении исследования информационных характеристик гетерогенных псевдослучайных последовательностей для выявления общих характеристик, различных оценок, факторов, по которым уже в дальнейшем следует анализировать генератор ПСП.

Для проведения исследования выбран и программно реализован генератор ПСП, построенный на регистрах сдвига, формируемый последовательность максимального период выходной ПСП ~$(2^{98}–1)$. Генератор ПСП, построенный на регистрах сдвига обладает следующими свойствами: простота реализации, прозрачность эксперимента, показательность. Структурная схема генератора ПСП представлена на рис. 2.

На следующем этапе работы выбрано изображения для дальнейшего маскирования ПСП размерностью 10^6 символов (~120 КБайт), проведено несколько операций маскирования линейными и нелинейными ПСП с целью выявления качества маскирования. Выбрано несколько информационных характеристик ПСП для проверки результатов маскирования: гистограммы вероятностей появления комбинаций длиной 1–5 бит в исходном и маскированном изображениях, коэффициент взаимной корреляции исходного и маскированного изображений, величина преобладания «0» и «1» в маскированном изображении, а также визуальный просмотр изображения.



RG1, RG2, RG3 – регистры сдвига с обратной связью (РЛЗ);

B - узел реализации операции выборки;

RG1 задан многочленом вида $x^{60}+x^{11}+1$;

RG2 задан многочленом вида $x^{79}+x^{19}+1$;

RG3 задан многочленом вида $x^{98}+x^{27}+1$;

$N_4 = 32$;

$k_4 = 17$.

Рис. 2. Структурная схема выбранного для исследования генератора ПСП

При маскировании исходного изображения равновероятной линейной ПСП получены следующие результаты: коэффициент взаимной корреляции исходного и замаскированного изображения равен «0,001212», величина преобладания «1» не превышает «0,0011213», визуально маскирование проведено успешно. Исходное изображение и результат маскирования равновероятной линейной ПСП показан на рис. 3.

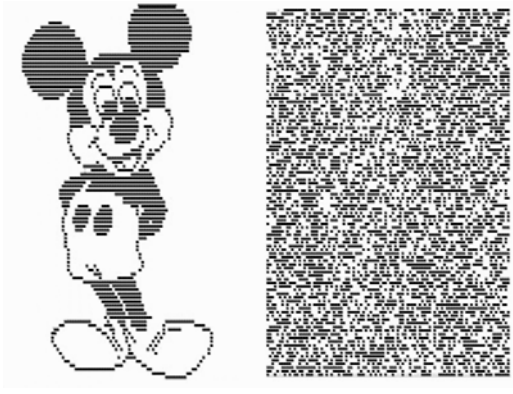


Рис. 3. Исходное изображение и результат маскирования равновероятной линейной ПСП

Для получения нелинейной ПСП из равновероятной линейной ПСП внесено преобладание величины «1» в исходную ПСП с шагом 8 и с шагом 3. Внесение величины преобладания в равновероятную линейную ПСП можно считать гетерогенной опасной неисправностью. При маскировании исходного изображения нелинейными ПСП получены следующие результаты: коэффициент взаимной корреляции исходного и замаскированного изображения при внесении преобладания «1» с шагом 3 равен «–0,324444», с шагом 8 равен «–0,113333», при внесении преобладания «1» с шагом 3, величина преобладания не превышает «0,19596», а с шагом 8 не превышает «0,066868», визуально маскирование проведено неуспешно (заметен контур изображения при внесении преобладания «1» с шагом 3). Результат маскирования нелинейной ПСП с внесением преобладания «1» с шагом 8 и с шагом 3 представлен на рис. 4.

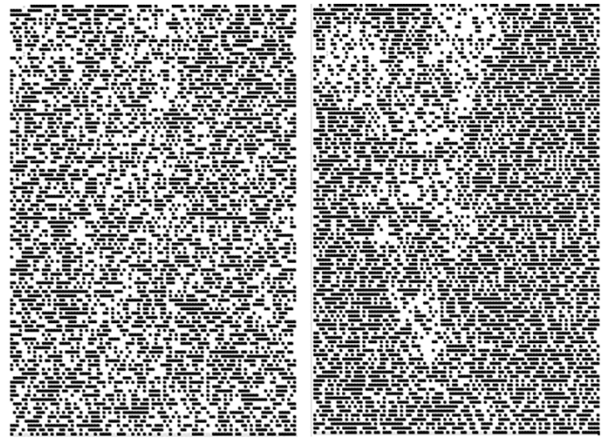


Рис. 4. Результат маскирования нелинейной ПСП с внесением преобладания «1» с шагом 8 и с шагом 3

В ходе работы проведен анализ влияния математических характеристик массивов данных на качество маскирования информации, разработано программное обеспечение для анализа исследуемых данных математических характеристик гетерогенных массивов данных, проведены маскирования гетерогенными массивами данных и представлены визуальные примеры гетерогенных маскирований информации. В ходе исследования проводились про-

граммные маскирования информации при применении криптографических операций: побитовая операция сложения по модулю два, операция перестановки бит, операция замены бит. На основе вычисленных характеристик построены гистограммы, отражающие распределение полученных математических величин на различных объемах выборки.

По полученным результатам можно сказать, что при отсутствии гетерогенных опасных неисправностей, информационный массив вырабатываемой ПСП близок по своим свойствам к идеальной случайной последовательности. При возникновении опасных гетерогенных неисправностей происходит значительное снижение криптографической стойкости информационного массива реализуемой ПСП.

Результаты, полученные на практике, будут использованы при построении программно-методического комплекса анализа псевдослучайных последовательностей с линейными и нелинейными характеристиками.

Литература

1. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2013. – 416 с.: ил.

2. Чугунков И. В., Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: «КУДИЦ-ОБРАЗ», 2003.

3. Теоретико-числовые методы в криптографии: Учебное пособие / Е. Б. Маховенко. – М.: Гелиос АРВ, 2006. 320 с., ил.