ISSN 2542-081X (Online)

Вопросы науки и образования

№ 26 (38), 2018

Москва
2018

ISSN 2542-081X (Online)

Вопросы науки и образования

№ 26 (38), 2018

НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ
HTTPS://SCIENTIFICPUBLICATION.RU
EMAIL: INFO@SCIENTIFICPUBLICATIONS.RU

Главный редактор
КОТЛОВА А.С.

Издается с 2016 года. Выходит 2 раза в месяц
Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство ПИ № ФС77 – 65699

ISSN 2542-081X

Содержание

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И СТОХАСТИЧЕСКИЕ АЛГОРИТМЫ В ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

Арзиева Ж.Т.

Арзиева Жамила Тилеубаевна – ассистент,
кафедра прикладной математики,
Каракалпакский Государственный Университет, г. Нукус, Республика Узбекистан

Аннотация: *в этой статье рассматриваются задачи генераторов псевдослучайных последовательностей и стохастические алгоритмы защиты информации.*
Ключевые слова*: псевдослучайных последовательностей (ПСП), компьютерных систем (КС), стеганографический метод, аутентичности, стохастические алгоритмы, криптография, хэш–генератор.*

Методы защиты информации, основанные на использовании генераторов псевдослучайных последовательностей (ПСП), будем называть стохастическими. При этом стоит отметить, что иногда термин «стохастические алгоритмы» применяется и в узком смысле тогда, когда речь идет об алгоритмах, предполагающих использование стохастических сумматоров, т.е. сумматоров с непредсказуемым результатом работы, зависящим от заполнения ключевой таблицы. Впервые эти устройства были предложены С.А. Осмоловским и использованы для создания стохастических кодов [1, с. 5].

Можно выделить следующие задачи, требующие решения при построении системы защиты компьютерных систем (КС) ответственного назначения:

1. обеспечение работоспособности компонентов КС и системы в целом при наличии случайных и умышленных деструктивных воздействий;
2. обеспечение секретности информации или наиболее важной ее части;
3. обеспечение аутентичности информации (целостности, подлинности и пр.);
4. обеспечение юридической значимости пересылаемых электронных документов;
5. защита прав собственников информации.

Первая задача решается с применением методов автономного и встроенного диагностирования; контролепригодного и отказоустойчивого проектирования; контроля хода выполнения программ с использованием сторожевых процессоров; помехоустойчивого кодирования; разграничения доступа к ресурсам и компонентам системы; внесения неопределенности в работу средств и объектов защиты.

Вторая задача решается в большой степени криптографическими (шифрование) и в меньшей степени стеганографическими методами (скрытие самого факта хранения или передачи секретной информации).

Третья и четвертая задачи решаются применением криптографических протоколов распределения ключей, аутентификации абонентов, электронной подписи, доказательства с нулевым разглашением знаний и пр.

Решение пятой задачи в настоящее время основано на применении стеганографической технологии цифровых водяных знаков [3, с. 32].

Во всех перечисленных случаях генераторы ПСП применяются либо непосредственно, либо на их основе строятся генераторы случайных последовательностей (СП) и хэш - генераторы (рис. 1). При этом качество защиты в значительной степени определяется качеством используемых алгоритмов генерации ПСП.

Рис. 1. Стохастические алгоритмы в задачах защиты информации

Выводы:

1. Все наиболее эффективные методы защиты информации с полным основанием должны называться стохастическим, так как предполагают прямое или косвенное использование генераторов ПСП.

2. Качество алгоритмов генерации случайных последовательностей и хеширования в первую очередь определяется качеством используемых генераторов ПСП.

3. В этой ситуации возрастает значимость задачи построения эффективных алгоритмов генерации ПСП, а также статистических методов оценки их качества.

Список литературы

1. *Осмоловский С.А.* Стохастическая информатика. «Радиоэлектроника и управление». № 10-12, 2003.
2. *Шеннон К.* Математическая теория связи. В сборнике «Работы по теории информации и кибернетике». ИИЛ. Москва, 1963.
3. *Осмоловский С.А.* Основополагающие работы Шеннона и их использование в современных инфокоммуникациях. // Радиоэлектроника и управление. № 1-3, 2003.