УДК 004.421.5

ЭКСТРАКТОРЫ СЛУЧАЙНОСТИ КАК ВАЖНЕЙШИЙ КОМПОНЕНТ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Грозов В.А.
(*Университет ИТМО, Санкт-Петербург*)
Научный руководитель: к.т.н., доцент факультета БИТ Будько М.Ю.
(*Университет ИТМО, Санкт-Петербург*)

Аннотация: В работе рассматриваются экстракторы случайности – важный компонент генераторов случайных последовательностей, необходимых при организации защиты данных криптографическими методами. Для оценки степени случайности последовательностей на основе min-энтропии используются рекомендации NIST 800-90.

Введение. Киберфизические системы (КФС) находят все более широкое применение во многих областях человеческой деятельности. Большую угрозу для безопасности таких систем представляют атаки на каналы связи, направленные на получение несанкционированного доступа к передаваемым данным. Поэтому важной проблемой при организации работы КФС является обеспечение защиты данных. Эффективную защиту информации обеспечивают криптографические методы, в которых ключевыми компонентами являются генераторы случайных (ГСП) и псевдослучайных (ГПСП) последовательностей, во многом определяющие их надежность.

Основная часть. Комплексный подход к построению криптографически стойких ГСП представлен в новых рекомендациях NIST 800-90 (National Institute of Standards and Technology), часть C (Recommendation for Random Bit Generator (RBG) Constructions). Для получения качественных ПСП перспективными являются комбинированные генераторы, в состав которых входит как недетерминированный генератор – источник энтропии, так и алгоритмический ГПСП, производящий выходные ПСП высокой степени криптостойкости с требуемыми статистическими свойствами.

Однако выходные последовательности недетерминированного генератора, как правило, далеки от требований, предъявляемых к качественным СП: для них характерны наличие сдвигов, корреляций, а также неравномерность распределения. Для исправления таких недостатков используются специальные процедуры постобработки, например, экстракторы.

Целью настоящей работы является изучение существующих методов экстракции, классификация разработанных экстракторов и обоснованный выбор алгоритмов, наиболее подходящих для практической реализации в условиях КФС малой мощности.

Экстрактором называется алгоритм, который, получая на вход необработанную последовательность случайных битов, преобразует ее в последовательность меньшего объема, но избавленную от указанных выше недостатков. Математическая теория экстракторов в настоящее время активно развивается, но далеко не все ее результаты реально применимы на практике.

Для оценки качества последовательностей случайных битов используют энтропию как меру возможности угадывания и непредсказуемости. В качестве численной характеристики случайности рекомендуется использовать min-энтропию (частный предельный случай энтропии Реньи).

Для оценки min-энтропии предлагается использовать подход NIST 800-90, часть B (Recommendation for the Entropy Sources Used for Random Bit Generation), основанный на применении предикторов – специальных алгоритмов, способных предсказывать последующее значение генерируемой последовательности на основе ее предшествующих

значений. Предиктор содержит модель, которая обновляется по мере последовательной обработки выборок. Для каждой выборки модель предлагает прогноз, получает выборку и затем обновляет ее внутреннее состояние на основе наблюдаемого значения выборки, чтобы улучшить свои будущие прогнозы. Итоговой оценкой min-энтропии считается минимальная (худшая) из всех полученных оценок.

Выводы. Представлены сведения об экстракторах и практике их применения на основе результатов анализа как научных публикаций, так и патентных источников. Дальнейшие исследования потребуют выполнить оценку эффективности различных алгоритмов экстракции и их сравнение. Для этого предполагается использовать методы оценки min-энтропии при помощи пакета тестов, введенных в NIST 800-90 B.