УДК 004.021

РАЗРАБОТКА ГПСЧ НА ОСНОВЕ ГЕНЕРАТОРА ХАОСА

Дольнов Д.Ю., Коблов А.Ю., Коновалова В.С. (Университет ИТМО, Санкт-Петербург)
Научный руководитель – к.т.н. Бибиков С.В.
(Университет ИТМО, Санкт-Петербург)

Введение. В век цифровых технологий различные вычислительные системы находят всё большее распространение, а вместе с ними растёт и количество информации, обрабатываемой и хранящейся на них. В связи с этим растёт и количество различной конфиденциальной информации, циркулирующей по вычислительным системам. С ростом количества конфиденциальных данных возрастает и количество людей, пытающихся незаконно получить доступ к этим данным.

Основная часть. Различные алгоритмы шифрования, призванные защитить конфиденциальность данных, становятся всё сложнее, старые алгоритмы становятся уязвимыми к взлому прямым перебором в связи с очень быстрым возрастанием вычислительной мощности систем злоумышленников. В основе большинства из используемых в настоящее время алгоритмов лежат ГПСЧ, которые имеют некоторую периодичность выдаваемых значений. Эту периодичность становится легче просчитать с возрастанием мощности вычислительных систем. Одним из подходов к решению этой проблемы является применение теории динамического хаоса для генерации случайных значений. Теория динамического хаоса основана на системе, поведение которой выглядит случайным, но в основе имеет строго определённые детерминистические законы. Поведение системы динамического хаоса зависит от начальных условий и параметров. Малое изменение начального условия со временем приводит к сколь угодно большим изменениям динамики системы.

Выводы. В ходе работы была создана модель ГПСЧ на основе генераторов хаоса. Были исследованы её достоинства и недостатки.
В качестве продолжения работы необходимо оптимизировать архитектуру генератора, провести более тщательное исследование криптостойкости и сравнить с аналогами.

Коблов А.Ю.

Бибиков С.В.