О СТАТИСТИЧЕСКОМ ТЕСТИРОВАНИИ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ

Деркач М. Ю., Харин Ю. С.

НИИ ППМИ БГУ, Минск, Беларусь, e-mail: kharin@bsu.by

Проблема защиты информации затрагивает практически все сферы деятельности человека. Среди способов защиты информации важнейшим является криптографический [1]. Надежность любой системы криптографической защиты информации в значительной степени определяется качеством используемых генераторов случайных и псевдослучайных последовательностей. Поэтому возникает задача статистического тестирования таких последовательностей, состоящая в оценивании их близости к модели равномерно распределенной случайной последовательности (РРСП). Для обнаружения отклонения от модели РРСП используются статистические тесты. И в данной статье представляются эффективные алгоритмы статистического анализа выходных последовательностей, основанного на оценивании таких Марковских моделей как, однородная цепь Маркова, однородная цепь Маркова S-ого порядка, скрытая марковская модель, двойная марковская модель.

Основной целью являлась разработка программного комплекса, позволяющего проводить тестирование выходных последовательностей генераторов, основанного на марковских моделях.

Использовались следующие математические модели выходных последовательностей $x_t \in A$:

M_1: Однородная цепь Маркова.

M_2: Однородная цепь Маркова S-ого порядка.

M_3: Скрытая марковская модель.

M_4: Двойная марковская модель.

Для статистического оценивания параметров этих моделей использовались следующие алгоритмы:

1. Алгоритм оценки максимального правдоподобия для моделей M_1, M_2.
2. Алгоритм статистического бутстрэпа для моделей M_1, M_2.
3. Алгоритм сглаживания оценки максимального правдоподобия для моделей M_1, M_2.
4. Обобщенный EM-алгоритм (алгоритм Баума-Велша) для моделей M_3, M_4.

Для проверки гипотез $H_0 = \{$выходная последовательность – РРСП$\}$, $H_1 = \overline{H_0}$ использовались следующие критерии:

1. Критерий согласия Пирсона
2. Критерий отношения правдоподобия

Программный комплекс реализован на языке высокого уровня C(C99).

Эксперименты проводились на модельных и реальных данных.

Библиографические ссылки

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.