ЭФФЕКТИВНОСТЬ ПРИМИТИВНОГО ВИРТУАЛЬНОГО ШИФРОВАНИЯ

Румянцев К.Е., Котенко В.В., Миргородский С.В., Поляков А.И.

Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru, rke2004@mail.ru

Для определения потенциальных возможностей виртуальных шифров (ВШ), впервые предложенных В.В. Котенко, исследовалась «мини-версия» этих шифров, характеризующая нижнюю границу эффективности виртуального шифрования. В качестве такой «мини-версии» выступает примитивный метод виртуального шифрования на базе гармонических функций. Целью исследования являлось определение качества формирования ключевых последовательностей пакетом NISTSTSв режиме генератора случайной последовательности (ГСП) и генератора псевдослучайной последовательности (ГПСП) и сравнение полученных результатов с имеющимися аналогами.

Исследовалась примитивная реализация виртуального шифрования, предполагающая использование исходного ключа единичной длины ($n_{Ки} = 1$), задающего примитивное одноэлементное выборочное пространство исходного ключа, которое свёртывалось в примитивную одноэлементную дискретную форму выборочного пространства ансамбля виртуализации, задающего частоту (f_c) гармонического колебания $K_V(t) = 10 \cdot \cos(2\pi f_C t)$, определяющего виртуальный ключ, в результате развёртывания которого, путём дискретизации и равномерного квантования на N_1 уровней, выделения шума цифрового представления и квантования последнего на два уровня, формировалась двоичная последовательность, которая подвергалась тестированию. При этом учитывалось, что при дискретизации формируется функция вида

$$s_i = 10 \cdot \cos(2\pi f_C T_i),$$

где $T_i = I / f_д$; i – номер отсчёта, $f_д$ – частота дискретизации. При тестировании пакетом NISTSTS выбиралось $\alpha = 0{,}01$ и количество тестируемых последовательностей $N_m = 100$, длиной 10^6 бит каждая. Параметры формирования последовательностей определялись как: $N_{quant} = 10^{12}$, $f_д = 1000{,}01$ Гц, $f_C = (10 + m)$ Гц, где m – номер последовательности (m = 0, 1, 2, ..., 99)). Проведено сравнение полученных результатов с результатами аналогичного тестирования широко применяемых в настоящее время генераторов: генератора псевдослучайных чисел BBS (Blum-Blum-Shub) и аппаратного датчика Гряда-1М. В табл. 1 обобщены данные по прохождению тестов по правилу 1. В табл. 2 сведены результаты прохождения тестов по правилу 2.

Таблица 1

Результаты прохождения тестов по правилу 1

Генератор	Количество тестов, у которых тестирование прошли более 99% последовательностей	Количество тестов, у которых тестирование прошли более 96% последовательностей
BBS	134 (70,8%)	189 (100%)
Гряда-1М	130 (68,8%)	184 (97,4%)
Примитивный вариант ВШ	134 (70,8%)	189 (100%)

Таблица 2

Результаты прохождения тестов по правилу 2

Генератор	Количество тестов, в которых $P \leq 0{,}01$	Количество тестов, в которых $P \leq 0{,}001$
BBS	0	0
Гряда-1М	1	0
Примитивный вариант ВШ	0	0

Анализ результатов тестирования пакетом NISTSTS, приведенных в таблицах, убедительно подтверждает вывод о том, что нижняя граница эффективности виртуального шифрования не уступает эффективности известных методов защиты дискретной информации. При этом приведенные результаты можно рассматривать, как отражение потенциала роста эффективности виртуального шифрования в ходе последующей реализации методов с последовательным и параллельным усложнением виртуальных выборочных пространств ансамбля ключей.

Список литературы

1. Котенко В.В. Оптимизация стратегии шифрования на основе виртуализации информационных потоков // Информационное противодействие угрозам терроризма. Науч.–практ. журн. – 2005. – №5. – С. 57-58.

2. Котенко В.В. Новый взгляд на условия обеспечения абсолютной недешифруемости с позиции теории информации // Информационное противодействие угрозам терроризма. Науч.-практ. журн. – 2004. – №2. – С. 36-43.