



КОМПЬЮТЕРНАЯ ТЕХНОЛОГИЯ ВИРТУАЛЬНОГО ШИФРОВАНИЯ

Котенко В.В., Румянцев К.Е., Поликарпов С.В.,
Левендян И.Б.

*Таганрогский государственный радиотехнический
университет, Таганрог*

Существующие шифры не в состоянии обеспечить теоретическую недешифруемость. Проведенные исследования показали, что одним из путей решения этой проблемы является виртуализация процесса шифрования. Применение данного подхода позволило получить целый ряд шифров, потенциально способных обеспечить теоретическую недешифруемость. На основе компьютерной реализации этих шифров был

разработан программный комплекс защиты информации. Экспериментальное исследование эффективности этого комплекса, проведенное с использованием набора статистических тестов NIST STS (табл. 1), показало его преимущество по отношению к существующим шифрам, в том числе и по отношению к шифру Rijndael, разработанному в рамках AES и рекомендованному в качестве стандарта шифрования XXI века. Так, даже при длине ключа 1 бит (примитивный вариант) обеспечивается качество шифрования, аналогичное качеству современных шифров, использующих длину ключа 128 бит и более. Причём, даже незначительное увеличение длины ключа (до 4 бит) позволяет значительно улучшить эти показатели.

Таблица 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%)
Гряды-1M	130 (68,8%)	184 (97,4%)
Примитивный вариант	134 (70,8%)	189 (100%)
Простой вариант	150 (79,4%)	189 (100%)

Необходимо подчеркнуть, что приведённые результаты следует рассматривать только как отражение динамики роста эффективности вариантов реализации комплекса в зависимости от роста длины (числа) исходных ключей и в ни коей мере – как однозначное подтверждение преимуществ, заключающихся в малом значении этой длины. В общем случае, длина исходных ключей будет соизмерима с длиной исходных ключей в современных шифрах. Это объясняется тем, что в состав исходного ключа должны включаться биты, задающие вид дискретной формы виртуального выборочного пространства, а также параметры дискретизации, квантования и масштабирования.

В целом, из результатов исследования комплекса следует, что его реализация в режиме генератора случайных последовательностей потенциально способна обеспечить показатели значительно превосходящие показатели известных аналогов. Учитывая, что выработка случайной (псевдослучайной) последовательности составляет основу формирования развёрнутого ключа, характеристики которого в конечном итоге определяют качество шифрования, полученный вывод может быть обобщён на все режимы применения разработанного программного комплекса.

Приведенные результаты получены при поддержке гранта Министерства Образования РФ Т02-03.1-816.

НОВЫЙ ПОДХОД К КОЛИЧЕСТВЕННОЙ ОЦЕНКЕ КАЧЕСТВА ЗАЩИТЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Котенко В.В., Румянцев К.Е., Поликарпов С.В.,
Левендян И.Б.

*Таганрогский государственный радиотехнический
университет, Таганрог*

Развитие информационных технологий в настоящее время сталкивается с достаточно серьезной проблемой количественной оценки качества их защиты в телекоммуникационных системах. В первую очередь эта проблема проявляется в значительной неопределенности основных критериев оценки качества шифров. Характерным проявлением этого явилось определение так называемого стандарта шифрования XXI века, которое проводилось в рамках серии конференций Национального Института Стандартов и Технологий (NIST) США в 1997-2000гг. Показательным является тот факт, что решение о лучшем шифре при-