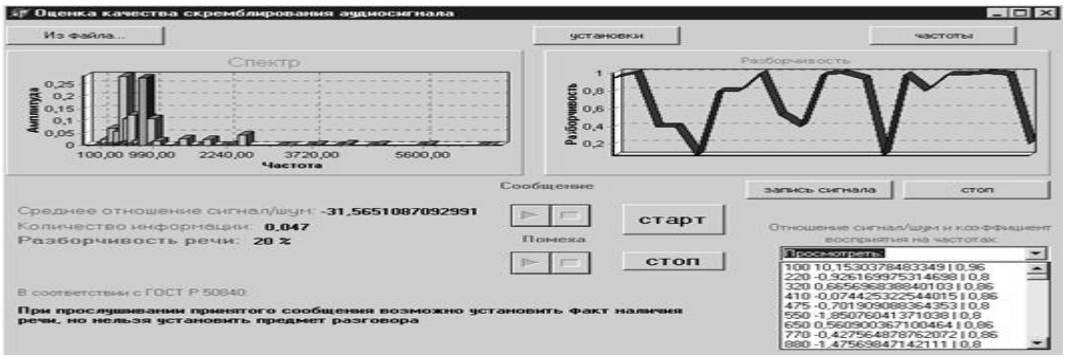

КОМПЬЮТЕРНАЯ ТЕХНОЛОГИЯ ВИРТУАЛЬНОГО ШИФРОВАНИЯ

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%)
Гряда-1М	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-

нималось только путем голосования участников Третьей Конференции (апрель 2000г.). Именно по результатам этого голосования (RIJNDAEL-86, SERPENT 59, TWOFISH-31, RC6-23, MARS-13) в качестве стандарта XXI века был рекомендован алгоритм RIJNDAEL, полученный в ходе реализации проекта AES.

Исследования, проведенные авторами, показали, что отмеченная проблема может быть решена с позиций подхода, предполагающего виртуальные представления процесса шифрования. Применение данного подхода позволило получить аналитические выражения для эффективности $D(\Phi,u)$ шифрования и создать программный комплекс оценки качества защиты информации (рис.1), к основным отличительным особенностям которого следует отнести: 1) возможность количественной оценки эффективности шифрования, в том числе в реальном масштабе времени; 2) учет статистических характеристик ансамблей сообщений, ключей и криптограмм, участвующих в процессе шифрования; 3) учет влияний информационных характеристик (в первую очередь избыточности) источников сообщений.

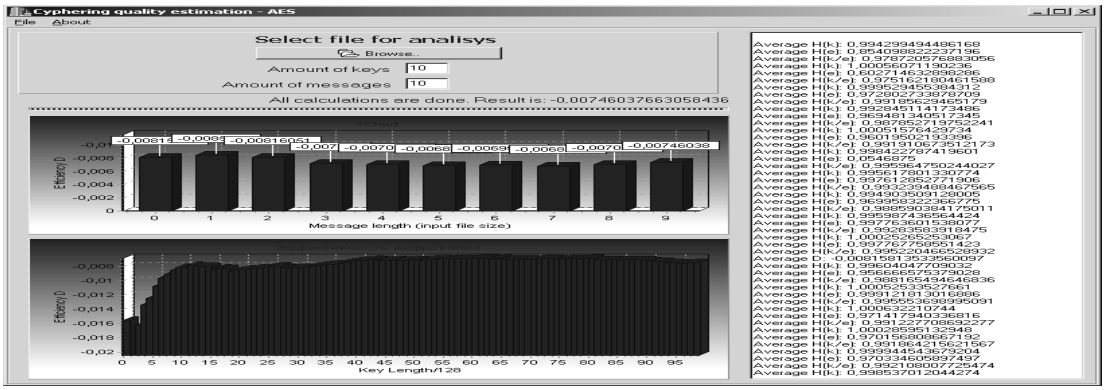

Рисунок 1

Применение созданного комплекса для оценки качества перечисленных выше шифров подсказало правомочность рекомендаций NIST. Так, эффективность алгоритма RIJNDAEL (рис. 1) составило для источников u_A английского языка:

$$D(\Phi,u_A) = -7.4604*10^{-3},$$

что соответствует более высокому качеству защиты по сравнению с алгоритмом SERPENT, у которого

$$D(\Phi,u_A) = -8.0781*10^{-3}.$$

Отрицательные значения $D(\Phi,u_A)$ означают, что эти алгоритмы не обеспечивают условия теоретической недешифруемости, которые восполняются при $D(\Phi,u\ ) \geq 0$. В данном случае более высокое качество шифрования характеризует приближенные значения $D(\Phi,u\ )$ к нулю в отрицательной области.

Применение предложенного подхода и созданного на его основе программного комплекса открывает принципиально новую область исследований в направлении оценки качества защиты информационных технологий. Приведенные результаты получены при поддержке гранта Министерства Образования РФ Т02-03.1-816.

ЭЛЕКТРОННОЕ УПРАВЛЕНИЕ ПЕРЕХОДОМ МЕТАЛЛ-ИЗОЛЯТОР В ДВУОКИСИ ВАНАДИЯ

Кулдин Н.А., Величко А.А., Стефанович Г.Б.,
Пергамент А.Л., Стефанович Д.Г.
Петрозаводский государственный университет, Петрозаводск

Переход металл-изолятор в оксидах переходных металлов перспективен для создания электронных устройств, реализующих в той или иной форме резкое пороговое изменение электрических и оптических свойств при достижении внешними параметрами определенного критического значения. Несмотря на универсализм поведения, системы с ПМИ условно могут быть разделены на две группы по начальному механизму нестабильности основного состояния [1]. В первой группе изменения в кристаллической решетке (структурный фазовый переход) приводят к расщеплению электронной зоны проводимости и, следовательно, к переходу в изоляторное состояние. В другой группе ПМИ удовлетворительно описывается в рамках чисто электронных моделей (переход Мотта).

Классическим объектом для изучения ПМИ является диоксид ванадия, в котором наблюдается фазовый переход 1 рода при достижении критической температуры перехода T_t=68^{o}C [1]. В ряде работ изучалось влияние электрического поля на ПМИ в планарных структурах на основе VO_2 [2,3], и было обнаружено влияние электрического поля на характеристики переключения или перехода, однако обнаруженные эффекты были слабыми и не поддавались однозначной интерпретации. В частности, влияние поля на температурную зависимость проводимости диоксида ванадия может быть объяснено сквозными