два режима работы комплекса: 1) режим формирования рабочего и виртуального идентификаторов; 2) режим аутентификации. Главными особенностями предложенного подхода являются:

1. Для санкционированного доступа корреспондента к системе непосредственно используется только виртуальный идентификатор, который формируется корреспондентом в аналоговом виде самостоятельно. Это абсолютно исключает возможность подделки.

2. Рабочий идентификатор используется только в качестве эталона для сравнения, что снимает необходимость его специальной защиты.

3. При желании корреспондент может оперативно изменить виртуальный идентификатор, представляя соответствующий ему рабочий идентификатор в систему.

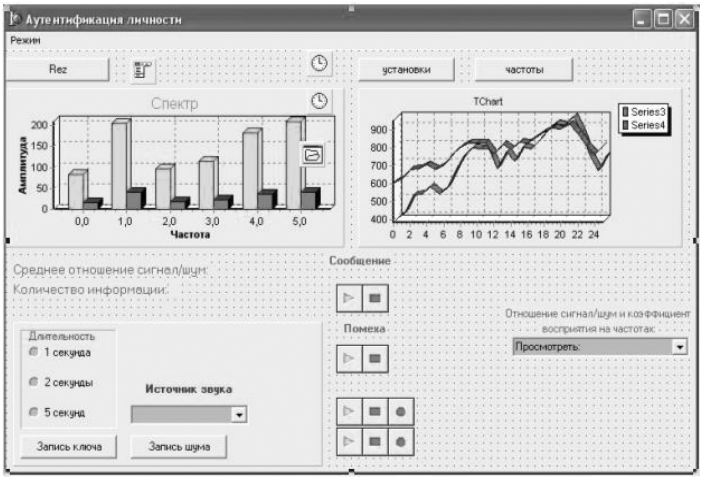


Рисунок 1

Предложенный подход и его реализация открывает принципиально новую **область** совершенствования информационных и банковских систем в направлении защиты от несанкционированного доступа к информации в системах. Приведенные результаты получены в ходе исследований при поддержке гранта Министерства Образования РФ Т02-03.1-816.

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОЦЕНКИ КАЧЕСТВА МЕТОДОВ СКРЕМБЛИРОВАНИЯ

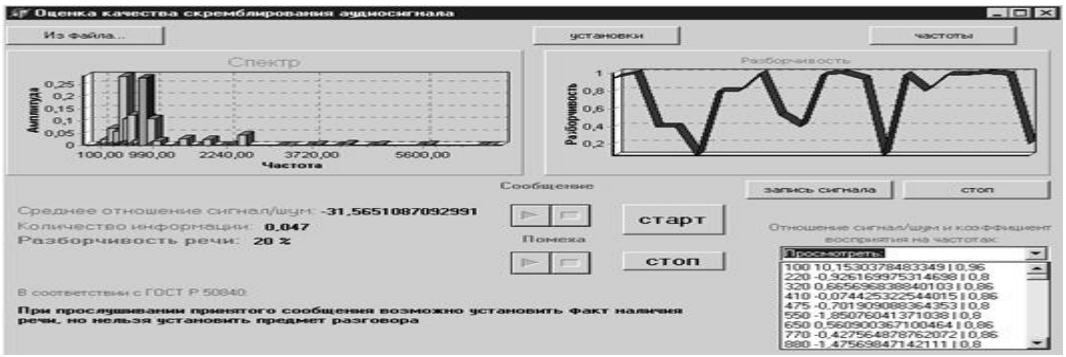
Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б.
Таганрогский государственный радиотехнический университет, Таганрог

Даже достаточно общее ознакомление с современным состоянием исследований в области анализа эффективности методов защиты аудиоинформации выявляет достаточно опасную ситуацию, заключающуюся в отсутствии на сегодняшний день общего подхода к решению задач данного класса. Это закономерно влечет за собой многообразие различных невзаимосвязанных методов оценки качества скремблирования, практическая ценность которых оставляет желать лучшего. Неопределенность используемых при этом критериев оптимальности оценки часто ставит исследователя в условия, когда он вынужден принимать эмпирические решения, приводящие обычно к довольно сомнительным результатам. Вызванные этим попытки использования критериев, предусматривающих разделение методов скремблирования на вычислительно стойкие и безусловно стойкие, хотя в ряде случаев и оправдывают себя, однако в целом вносят дополнительную неопределенность. Все это способствует формированию ситуации, в которой преобладающим становится мнение о том, что уровень и степень секретности систем скремблирования речи являются понятиями весьма условными. Решить эту проблему позволяет введение понятия виртуального шума скремблирования. С учетом этого понятия процесс скремблирования может быть представлен как процесс изменения речевого сигнала $S(t)$ виртуальным шумом $V(t)$. Проекция этого представления на реальную область определяется выражениями вида

$$E(t) = F[S(t), \Pi V(t)], \quad \Pi V(t) = \Phi[S(t), E(t)] \quad (1)$$

где: $E(t)$ –скремблированный сигнал; $\Pi V(t)$ – проекция виртуального шума. Выражения (1) определяют общую математическую модель оценки эффективности методов скремблирования. Исследования в направлении реализации данного подхода дают вполне обнадёживающие результаты. Свидетельством этому явилось создание программно-аппаратного комплекса текущего контроля качества защиты аудиоинформации.

Комплекс предназначен для контроля качества защиты аудиоинформации в реальном масштабе времени. Для этих целей впервые применены виртуальные алгоритмы оценки. Это позволило использовать для оценки качества защиты аудиоинформации традиционно применяемые для этих целей характеристики: разборчивость и среднее количество информации. На основании этого предусмотрена возможность выдачи рекомендаций пользователям по организации ведения служебных переговоров. Приведенные результаты получены при поддержке гранта Министерства Образования РФ Т02-03.1-816.



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-