нение достаточно низко для изображений JPEG, несжатых изображений цифровых фотокамер, сканированных фотографий и изображений, обработанных при помощи общеизвестных алгоритмов обработки. Цветные изображения дают больший разброс по исходному отклонению, чем изображения в оттенках серого. Для сильно зашумлённых изображений разница между количеством обычных и одиночных групп весьма незначительна. Соответственно линии диаграммы пересекаются под малым углом, и точность стегоанализа снижается. То же самое относится и к некачественным изображениям, чрезмерно сжатым или просто малым изображениям (менее 400 точек по каждому измерению) вследствие недостатка статистических данных. Предлагаемый метод стегоанализа даёт более точные результаты в случае распределения скрытых данных по всему объёму изображения, чем при локализованном внедрении. В последнем случае алгоритм может быть модифицирован и применён последовательно к отдельным участкам изображения в пределах скользящего прямоугольного окна.

Библиографический список

1. *W. Bender D. Gruhl N. Morimoto A.* Lu Techniques for data hiding.- IBM SYSTEMS JOURNAL, vol 35, nos 3&4, pp. 313-315, 1996.

2. Jessica Fridrich, Miroslav Goljan Practical Steganalysis of Digital Images – State of the Art,- http://www.ssie.binghamton.edu/fridrich.

В.В. Котенко, К.Е. Румянцев, С.В. Поликарпов
Россия, г. Таганрог, ТРТУ

НОВЫЙ ПОДХОД К РЕШЕНИЮ ПРОБЛЕМ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕТОДОВ ЗАЩИТЫ АУДИОИНФОРМАЦИИ

Представление процесса защиты информации в виде двух уровней (логического и материального) открывает возможность решения проблем оценки эффективности методов защиты аудиоинформации с принципиально новых позиций. Прежде всего, взгляд на данные проблемы с этих позиций показывает целесообразность выделения двух областей анализа эффективности процессов защиты аудиоинформации:

- область анализа логического уровня представления процессов защиты;
- область анализа материального уровня представления процессов защиты.

Такое разделение единой до настоящего времени области анализа позволяет значительно снизить существующую неопределенность проблем анализа. Это объясняется возможностью разделения проблем анализа на две группы:

- проблемы анализа на логическом уровне, к которым можно отнести проблемы оценки качества криптографических методов, методов аутентификации и т.п.;
- проблемы анализа на материальном уровне, к которым относятся проблемы оценки качества методов скремблирования.

Даже достаточно общее ознакомление с современным состоянием исследований в области решения проблем анализа эффективности методов защиты аудиоинформации с этих позиций выявляет достаточно опасную тенденцию, заключающуюся в дисбалансе практических и научно-значимых решений в пользу проблем первой группы. Свидетельством этому является значительное число научных работ и эффективных практических результатов, относящихся к задачам оценки качества криптографических методов. При этом появление новых алгоритмов и систем оценки неизменно сопровождается исследованиями в направлении поиска более эффективных решений. Примером этому может служить система статических тестов NIST STS, специально разработанная Институтом Стандартов и Тех-

нологий США для подробного анализа качества криптографических методов. NIST STS использует 189 тестов, каждый из которых предназначен для определения соответствующей глобальной или локальной оценки. Широкое внедрение NIST STS показывает исключительную эффективность данной системы. Однако, несмотря на это, не прекращается поиск более эффективных решений. На фоне этого ощутимого прогресса положение в области анализа эффективности методов скремблирования выглядит особенно неприглядно. Отсутствие на сегодняшний день общего подхода к решению задач данного класса 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 логической области анализа, предусматривающие 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. Таким образом, складывается весьма парадоксальная ситуация, когда исследования в направлении поиска оптимальных оценок качества скремблирования изначально ограничиваются условием априорной неопределенности параметров критериев оптимальности этих оценок. По-видимому, как попытку выхода из этой ситуации, следует рассматривать стандартизацию ГОСТ Р 50840-95 шкалы оценок качества скремблирования, основным параметром которой является разборчивость (W). Конкретизацию критерия максимально допустимой разборчивости путем установления выше определенных значений его параметра, предпринятую в, несомненно, можно рассматривать как шаг на пути выхода из создавшейся кризисной ситуации. Однако дальнейшее продвижение в данном направлении наталкивается на довольно серьезную преграду, связанную с несовершенством существующих методик оценки разборчивости. Это объясняется тем, что практически все известные в настоящее время методики оценки разборчивости основываются на определении отношения сигнал/шум, что неприемлемо для методов скремблирования ввиду невозможности представления искажений, вносимых скремблированием в виде шума в прямой постановке. Исключение составляет лишь амплитудное скремблирование, часто трактуемое как зашумление или маскировка речевого сигнала. В данном случае есть возможность определения параметров шума. Именно этот факт во многом является определяющим того, что практически все исследования в направлении поиска оптимальных оценок качества скремблирования проводятся в основном применительно к аналоговому скремблированию. Однако и эти исследования сталкиваются с целым рядом нерешенных проблем, к которым следует отнести:

- необеспеченность оценок качества скремблирования инструментальными средствами контроля;
- невнимание к угрозам компенсации излучаемых аппаратурой защиты помех и перехвата содержания скрываемых переговоров при поверхностном соблюдении норм и требований по защите информации;
- недооценку опасности выхода из строя (по различным причинам) аппаратуры защиты информации.

Проведенный анализ проблем оценки эффективности методов защиты аудиоинформации показывает исключительную актуальность исследований в направле-

нии поиска общего подхода к оценке эффективности методов скремблирования, открывающего выход на универсальные методики этой оценки. Решить эту проблему позволяет подход предполагающий рассмотрение процессов защиты информации с позиции виртуального познания. С этих позиций переход в область виртуального представления позволяет ввести понятие виртуального шума скремблирования. Под виртуальным понимается некоторый возможный при определенный условиях шум, способный изменить речевой сигнал по закону, соответствующему закону его изменения методом скремблирования. С учетом этого понятия процесс скремблирования может быть представлен как процесс изменения речевого сигнала виртуальным шумом. Проекция этого представления на реальную область определяется выражением вида

$$E(t) = F[S(t), \not{H}V(t)], \qquad (1)$$

где: $E(t)$ – скремблированный сигнал;

$\not{H}V(t)$ – проекция виртуального шума скремблирования $V(t)$; $S(t)$ – входной сигнал.

Таким образом, решение отмеченной проблемы сводится к определению проекции виртуального шума скремблирования на область реальных представлений:

$$\not{H}V(t) = \Phi[S(t), E(t)]. \qquad (2)$$

Совокупность выражений (1)-(2) определяет общую математическую модель разрабатываемой методики оценки эффективности методов скремблирования. Достоинством настоящей методики будет ее универсальность. Она потенциально может быть обобщена на всю область анализа методов защиты, включая методы криптографической защиты. Расширение возможностей разработанной методики в данном случае достигается путем включения в ее состав процедуры оценки качества ключа (К). Для этих целей могут использоваться апробированные методы оценки криптографических методов, предусматривающие оценку эффективности ключа, такие как NIST STS и т.п.

Начатые в этом направлении исследования уже на начальном этапе показали, что подход к решению проблем оценки качества защиты аудиоинформации с позиций теории виртуального познания даёт вполне обнадёживающие результаты. Свидетельством этому явилось создание опытного варианта программно-аппаратного комплекса текущего контроля качества защиты аудиоинформации на объекте.

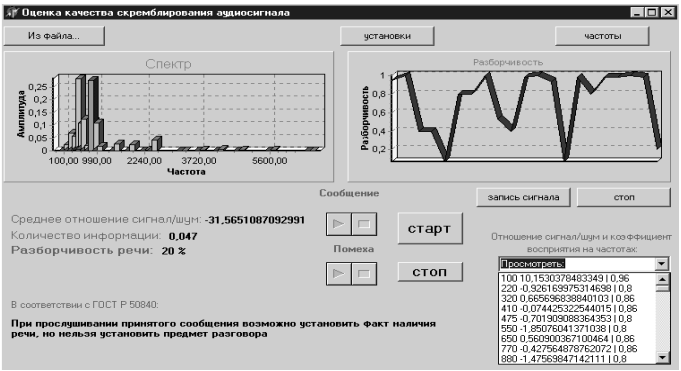

Рис.1. Принцип работы программно-аппаратного комплекса текущего контроля качества защиты аудиоинформации на объекте

Комплекс предназначен для контроля качества защиты аудиоинформации на объекте в реальном масштабе времени. Для этих целей впервые применены виртуальные алгоритмы оценки. Это позволило использовать для оценки качества защи-

ты аудиоинформации традиционно применяемые для этих целей характеристики: разборчивость и среднее количество информации. На основании полученных результатов в соответствии с ГОСТ Р 50840 предусмотрена возможность выдачи рекомендаций пользователям по организации ведения служебных переговоров. Принцип работы комплекса отражён на рис.1.

П. П. Кравченко, А. И. Дордопуло
Россия, г. Таганрог, ТРТУ,

АЛГОРИТМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА ОСНОВЕ ОПТИМИЗИРОВАННЫХ ДЕЛЬТА-ПРЕОБРАЗОВАНИЙ ВТОРОГО ПОРЯДКА

Возрастающие требования к качеству передаваемой информации (цифровых аудио и видеосигналов) приводят к увеличению количества хранимых и обрабатываемых данных и ставят задачи сжатия и защиты информации. Совместное использование традиционных алгоритмов сжатия информации и итеративных блочных шифров затруднено высокой ресурсоемкостью и неудовлетворительной скоростью шифрования. В связи с этим необходимо использовать высокопроизводительные алгоритмы компрессии и защиты. Одним из перспективных методов сжатия информации с потерями является дельта-преобразование (Д-преобразование) второго порядка [1], представляющее собой аппроксимацию модулируемой функции в дискретные моменты времени, при котором значения вторых разностей на интервале преобразования принимают значения из ограниченного множества величин и представляют собой постоянные по модулю и отличающиеся знаком кванты модуляции. Отличительными особенностями Д-преобразования являются простота и высокое быстродействие, особенно алгоритмов демодуляции. Важными свойствами Д-преобразований с точки зрения защиты информации являются близкое к равномерному распределение выходной дельта-последовательности (Д-последовательности), предельно короткая длина используемых значений (1 бит) и разрушение сигнала при изменении дельта-бит (Д-бит) [4], что обеспечивает возможность построения более простых и более быстродействующих алгоритмов защиты информации [2]. Будем рассматривать следующую структуру сигнала: в защищаемом сжатом сигнале выделяется *блок кадров* – текущий результат преобразования, представляемый в виде линейного массива кадров сигнала. Длина блока составляет $\boldsymbol{M}$ кадров. Кадр – структура данных, содержащая блок начальных условий и последовательность Д-бит. Длина кадра составляет $\boldsymbol{L}$ бит, длина блока начальных условий - $\boldsymbol{S}$ бит и длина Д-последовательности - $\boldsymbol{N}$ бит: $\boldsymbol{L = S + N.}$

Заполнение блока производится по порядку следования кадров исходного сигнала. Разрабатываемые алгоритмы защиты информации должны обеспечивать устойчивость к известным видам атак и обладать некоторыми свойствами (такими, как нелинейность, перемешивание и рассеивание).

Использование существующих блочных алгоритмов для защиты Д-последовательности нецелесообразно из-за их высокой трудоемкости, низкой скорости и большого числа раундов для обеспечения удовлетворительных характеристик перемешивания и рассеивания. Поэтому, исходя из свойств Д-последовательности и характеристик криптографических преобразований [3], для защиты можно использовать более простые операции, обладающие высокими показателями перемешивания и рассеивания, которые в сочетании со свойствами Д-последовательностей позволяют достичь высокой стойкости при низкой трудоемкости. Для раунда шифрования в качестве таких операций можно использовать