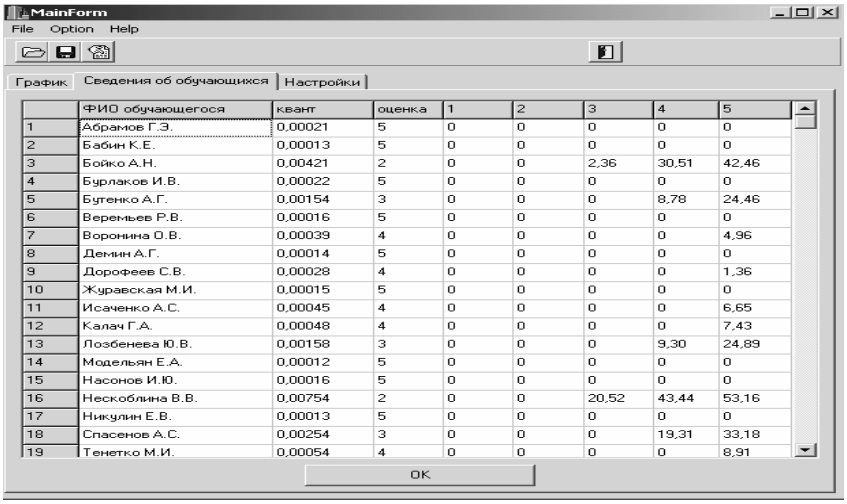

	ФИО обучающегося	квант	оценка	1	2	3	4	5
1	Абрамов Г.З.	0,00021	5	0	0	0	0	0
2	Бабин К.Е.	0,00013	5	0	0	0	0	0
3	Бойко А.Н.	0,00421	2	0	0	2,36	30,51	42,46
4	Бурлаков И.В.	0,00022	5	0	0	0	0	0
5	Бутенко А.Г.	0,00154	3	0	0	0	8,78	24,46
6	Веремьев Р.В.	0,00016	5	0	0	0	0	0
7	Воронина О.В.	0,00039	4	0	0	0	0	4,96
8	Демин А.Г.	0,00014	5	0	0	0	0	0
9	Дорофеев С.В.	0,00028	4	0	0	0	0	1,36
10	Журавская М.И.	0,00015	5	0	0	0	0	0
11	Исаченко А.С.	0,00045	4	0	0	0	0	6,65
12	Калач Г.А.	0,00048	4	0	0	0	0	7,43
13	Лозбенева Ю.В.	0,00158	3	0	0	0	9,30	24,89
14	Модельян Е.А.	0,00012	5	0	0	0	0	0
15	Насонов И.Ю.	0,00016	5	0	0	0	0	0
16	Нескоблина В.В.	0,00754	2	0	0	20,52	43,44	53,16
17	Никулин Е.В.	0,00013	5	0	0	0	0	0
18	Спасенов А.С.	0,00254	3	0	0	0	19,31	33,18
19	Тенетко М.И.	0,00054	4	0	0	0	0	8,91

Рис. 2. Шкала оценок

3. Комплексная информация о характеристиках оценки формируемой программно-аппаратными комплексами системой (показатели активной оценки, фазовое пространство групповой оценки, среднее количественное пространство групповой оценки, энтропийное пространство принятия решения, среднее энтропийное пространство групповой оценки) обеспечит возможность адаптивной модернизации образовательных программ и методик образования как в обычных системах, так и в системах дистанционного образования в области инновационного менеджмента наукоемкой продукции с позиций теории виртуального познания.

УДК 621.391.037

Котенко В.В., Евсеев А.С., Румянцев К.Е.

НОВЫЙ ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ И КАЧЕСТВА СКРЕМБЛИРОВАНИЯ НА ОСНОВЕ ОПРЕДЕЛЕНИЯ ИДЕНТИЧНОСТИ ВИРТУАЛЬНЫХ ВЕРБАЛЬНЫХ РЕЧЕВЫХ ОБРАЗОВ

В настоящее время постоянно возрастающая роль информационных и телекоммуникационных технологий сопровождается возрастающими требованиями к защите информации. Решение этой проблемы, в свою очередь, требует поиска новых подходов к оценке качества защиты информации. Основу применяемых в настоящее время подходов к оценке эффективности защиты аудиоинформации составляет определение разборчивости (ГОСТ Р 50840-95, ГОСТ Р 51061-97) или производного от нее параметра неразборчивости. В данном случае существует довольно серьезная проблема, связанная с тем, что даже при условии нулевой разборчивости в криптограммах может присутствовать избыточность, что оказывает негативное влияние на эффективность защиты аудиоинформации. Предложенный в [4, 5] подход к оценке эффективности защиты аудиоинформации на основе комплексного определения разборчивости и избыточности в основном позволяет решить эту проблему. Однако, природная нестационарность исходных речевых сигналов не позволяет в полной мере оценить эффективность защиты аудиоинформа-

ции даже при использовании этого подхода. Это объясняется тем, что значения избыточности и разборчивости криптограмм в данном случае будут изменяться во времени и, как показали исследования, зависеть от индивидуальных и вербальных характеристик реальных источников речевой информации. Для решения этой проблемы предлагается подход, основанный на формировании информационных виртуальных вербальных речевых образов [1, 2].

С позиций этого подхода общий алгоритм определения оптимальной оценки количества информации *J**, минимизирующей средний квадрат ошибки, определяется как:

$$J^* = \int_{-\infty}^{\infty} J P_{ps}(J) dJ \,, \tag{1}$$

где $P_{ps}(J)$ - апостериорная плотность вероятностей.

Для интервалов квантования во времени t ($t_i < t < t_{i+1}$) апостериорная плотность вероятностей может быть определена дифференциальным уравнением Фокера-Планка-Колмогорова [3]:

$$\frac{dP(J(t),t)}{dt} = \alpha \frac{d}{dJ}\left\{\left[J(t) - h_0\right]P(J(t),t)\right\} + \frac{g^2}{4} N_J \frac{d^2}{dJ^2} P(J(t),t) \,, \tag{2}$$

где α, g, N_J определяется из дифференциального уравнения состояния источника

$$\frac{dJ(t)}{dt} = -\alpha(t, J(t)) + g(t) n_J(t) \tag{3}$$

в предположении его стационарности, гауссовости и марковости, когда (3) принимает вид

$$\frac{dJ(t)}{dt} = -\alpha(J(t) - h_0) + g n_J(t) \,, \tag{4}$$

где $n_J(t)$ - стационарный гауссовский белый шум со спектральной плотностью N_J.

Таким образом, при получении наблюдения $J_\psi(t_i) = J_\psi(i)$ апостериорная плотность вероятностей скачком устанавливается равной $P_{ps}(J(i))$, а затем экстраполируется по закону (2). Исходя из этого, задача определения оценки $J^*(t)$ по квантовой последовательности $J_\Psi(i)$ разделяется на две задачи: задачу определения последовательности оценок $J^*(t_i) - J^*(i)$ и задачу сглаживания полученной последовательности $J^*(i)$. Если эта оценка формируется на полуинтервале наблюдения (t_i, t_{i+1}) по одному наблюдению $J_\psi(i)$, то справедливо выражение

$$J^*(t) = J^*(i) e^{-\alpha(t - t_i)} \,. \tag{5}$$

Задача определения оценки $J^*(i)$ в общем случае является задачей, которая может быть решена на основании (1) путем определения рекуррентного выражения для апостериорной плотности вероятностей [2]. Результатами этого решения является рекуррентный алгоритм вида:

$$J^*(i) = e^{-\alpha T} J^*_{(i-1)} + K_i^{(k)}\left[J_\Psi(i) - e^{-\alpha T} J^*_{(i-1)} - h_0\right] + h_0, \tag{6}$$

где k-индекс области квантования, к которой относятся $J_\Psi(i)$; $K_i^{(k)}$ - коэффициент усиления.

Определение оценки $J^*(t)$ является основой для формирования оценки информационного вербального образа:

$$S_J^*(\omega) = \int_0^\infty J^*(t) e^{-j\omega t} dt \quad . \tag{7}$$

Выражения (5)-(7) представляют собой математическую модель оценки информационного вербального речевого образа. Реализация данной модели применительно к задачам оценки процессов скремблирования и создание на ее основе программных и программно-аппаратных комплексов позволили сформулировать следующую постановку задачи дальнейших исследований: определение новых показателей процесса защиты речевой информации с позиций формирования и определения идентичности информационных вербальных образов до и после скремблирования.

Оценка эффективности скремблирования при использовании предложенного подхода осуществляется путем определения идентичности информационных виртуальных вербальных речевых образов до и после скремблирования. На рис. 1 – 3 приведены информационные виртуальные вербальные речевые образы и результаты оценки коэффициентов идентичности информационных образов до и после скремблирования (коэффициентов идентичности процесса скремблирования K_{uc}) для классического цифрового скремблирования (рис.1), виртуального скремблирования [5] (рис.2) и адаптивного виртуального скремблирования (рис.3).

Из приведенных ниже рисунков видно, что предложенный подход позволяет осуществлять визуальный экспресс-контроль эффективности скремблирования по степени изменения виртуального образа в процессе защиты аудиоинформации: чем больше изменение – тем выше эффективность скремблирования. При этом для количественной оценки эффективности могут использоваться коэффициенты идентичности этих образов.

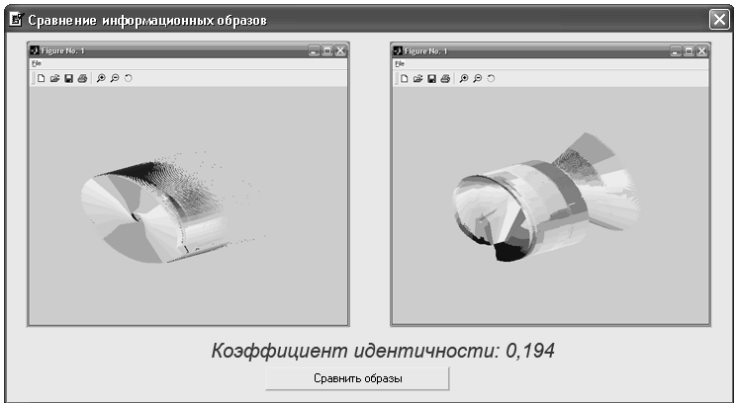

Рис. 1. Идентичность процесса классического скремблирования

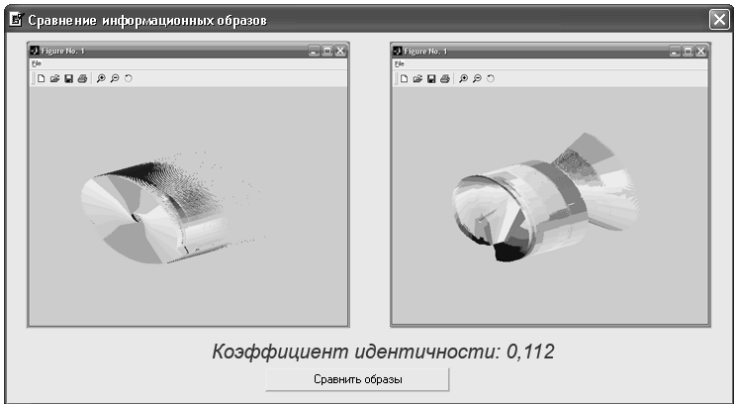

Рис. 2. Идентичность процесса виртуального скремблирования

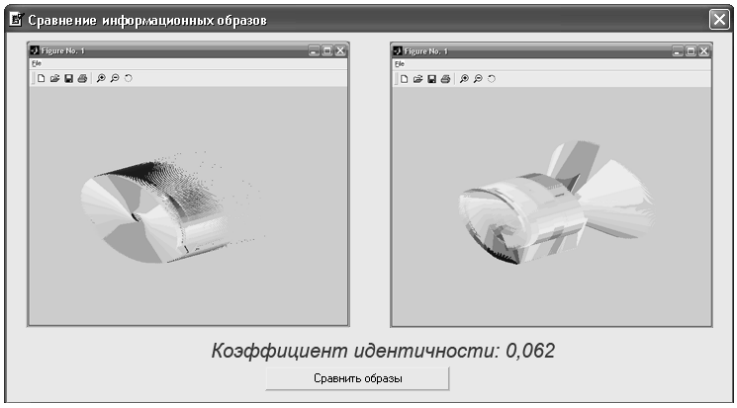

Рис. 3. Идентичность процесса адаптивного виртуального скремблирования

Как показали исследования, в данном случае коэффициенты идентичности процесса скремблирования $K_{ис}$ будут зависеть от индивидуальных и вербальных характеристик источника речевой информации и их изменения во времени. С одной стороны, это позволяет учесть эти изменения при оценке эффективности скремблирования, с другой стороны, изменение $K_{ис}$ делает весьма затруднительным его применение в качестве параметра эффективности скремблирования. Используя общепринятый подход к решению аналогичных проблем в качестве показателя скремблирования предлагается использовать величину обратную математическому ожиданию $K_{эс}$:

$$K_{эс} = \frac{1}{\mathrm{M}\left[K_{ис}\right]} \tag{8}$$

Результаты экспериментальных исследований $K_{эс}$ для классического, виртуального и адаптивного виртуального скремблирования приведены в таблице 1.

Таблица 1

Скремблирование	$K_{эс}$	W_p	μ_y
Классическое	5,154	0,132	0,211
Виртуальное	8,896	0,094	0,164
Адаптивное виртуальное	16,129	0,027	0,081

Из таблицы видно, что значения $K_{эс}$ достаточно точно согласуются с общепринятыми показателями, такими как разборчивость W_p и избыточность μ_y, в части результатов оценки эффективности приведенных методов скремблирования.

К особенности предложенного подхода следует отнести открывающуюся возможность оценки качества скремблирования. Под качеством скремблирования с позиций формирования виртуальных образов в данном случае понимается исключение индивидуальных признаков в образах результатов скремблирования. С физической точки зрения это означает отсутствие необходимой информации у несанкционированного пользователя для дескремблирования при постоянном поступлении идентичных образов. Для оценки качества скремблирования может быть использован коэффициент идентичности виртуальных образов результатов скремблирования (коэффициент идентичности защиты $K_{из}$). На рис. 4 – 6 приведены результаты сравнения идентичности виртуальных образов криптограмм, полученных в процессе скремблирования источника речевой информации для классического цифрового скремблирования (рис.4), виртуального скремблирования (рис.5) и адаптивного виртуального скремблирования (рис.6).

Из приведенных рисунков видно, что предложенный подход позволяет осуществлять визуальный экспресс-контроль качества скремблирования по степени идентичности виртуальных образов криптограмм. При этом, более высокая степень идентичности будет отражать более высокое качество скремблирования.

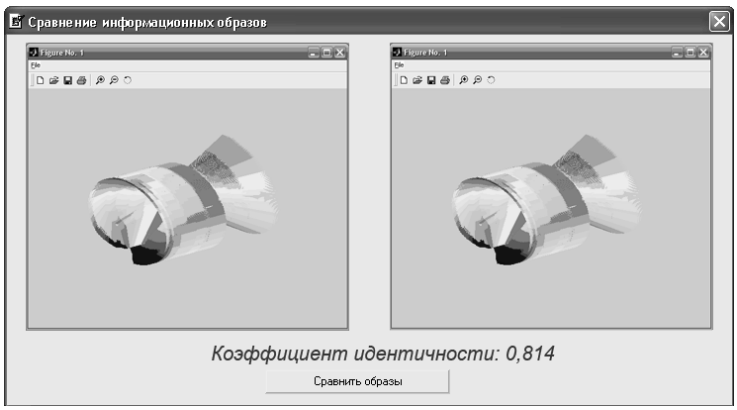

Рис. 4. Коэффициент идентичности защиты классического скремблирования

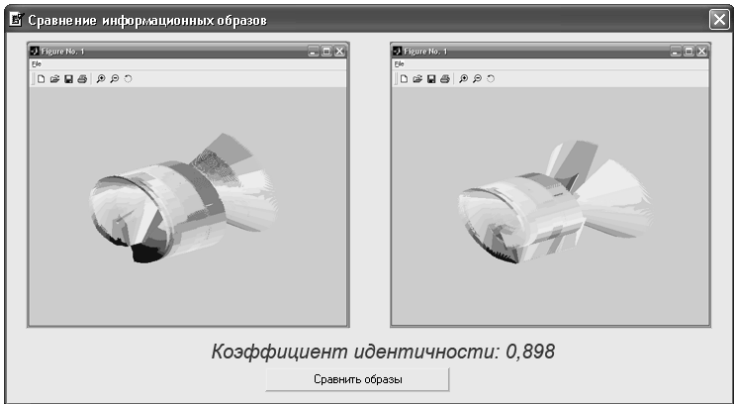

Рис. 5. Коэффициент идентичности защиты виртуального скремблирования

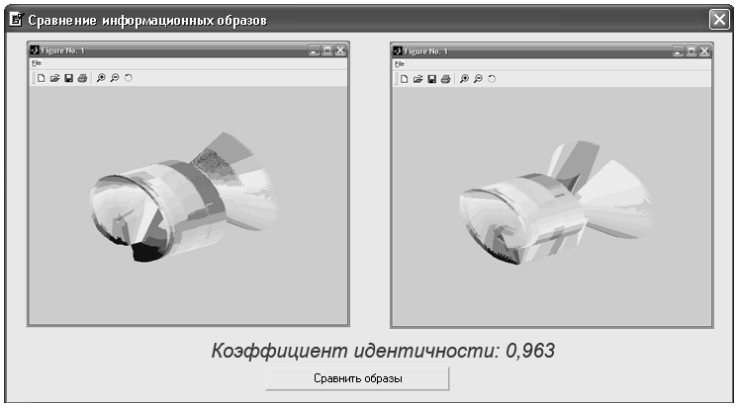

Рис. 6. Коэффициент идентичности защиты адаптивного виртуального скремблирования

Количественная оценка качества скремблирования в данном случае может быть произведена путем определения математического ожидания $K_{из}$ и среднего квадратического отклонения $K_{из}$ и последующего вычисления показателя качества скремблирования $K_{кс}$ по формуле:

$$K_{кс} = \frac{\mathrm{M}\left[K_{из}\right]}{\sigma\left[K_{из}\right]} \tag{9}$$

Таблица 2

Скремблирование	$K_{из1}$	$K_{из2}$	$K_{из3}$	$K_{кс}$
Классическое	0,814	0,861	0,798	13,085
Виртуальное	0,898	0,916	0,941	21,357
Адаптивное виртуальное	0,963	0,997	0,971	28,735

В таблице 2 приведены результаты экспериментальных исследований $K_{кс}$ для классического, виртуального и адаптивного виртуального скремблирования. Из таблицы 2 следует, что значение $K_{кс}$ достаточно точно отражает результаты экспериментальных исследований приведенных методов скремблирования на основе применения общепринятых параметров разборчивости и избыточности.

Предложенный подход открывает принципиально новую область возможностей оценки эффективности и качества скремблирования. Дальнейшие исследования в этом направлении представляют научный и практический интерес.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Котенко В.В. Идентификация и прогноз сознательных и подсознательных поведенческих форм личности с позиций формирования виртуального вербального образа.// Известия ТРТУ, 2006, №4.
2. Котенко В.В. Оценка информационного образа исследуемого объекта с позиций теории виртуального познания. Известия ТРТУ. Таганрог: Изд-во ТРТУ, 2005. №4
3. Котенко В.В., Евсеев А.С. Компьютерная технология оценки эффективности скремблирования на основе определения разборчивости и избыточности. // Информационное противодействие угрозам терроризма: научн-практ. журн. /ФГПУ НТЦ гос. рег. №0320600189, Москва. 2007, №9
4. Котенко В.В., Евсеев А.С. Новый подход к оценке эффективности защиты аудиоинформации на основе комплексного определения разборчивости и избыточности. // “Информационная безопасность”. Сборник трудов девятой международной научно-практической конференции. ТРТУ 2007.
5. Котенко В.В., Евсеев А.С. Компьютерная технология оценки эффективности скремблирования на основе определения разборчивости и избыточности. // Информационное противодействие угрозам терроризма: научн-практ. журн. /ФГПУ НТЦ гос. рег. №0320600189, Москва. 2007, №9. С.35-40.

УДК 621.391.037

Котенко В.В., Евсеев А.С., Румянцев К.Е.

ВЛИЯНИЕ ИНДИВИДУАЛЬНЫХ ХАРАКТЕРИСТИК ИСТОЧНИКОВ РЕЧЕВОЙ ИНФОРМАЦИИ НА ЭФФЕКТИВНОСТЬ И КАЧЕСТВО СКРЕМБЛИРОВАНИЯ

Применение подхода, основанного на формировании информационных виртуальных вербальных речевых образов [1, 2], предполагает применение новых показателей для оценки методов защиты аудиоинформации, таких, как эффективность и качество скремблирования. В отличие от применяемого в настоящее время показателя разборчивости, это позволяет дать более полную характеристику процессов скремблирования. Прежде всего, это относится к открывающейся возможности оценки влияния индивидуальных характеристик источников речевой информации на процесс скремблирования.

На рис.1 – 9 и в таблице 1 приведены результаты анализа идентичности процессов скремблирования с позиций формирования виртуальных образов для трех