в 2 ч. Ч.2 / науч. ред. С.А.Подлесный - Красноярск: СФУ, 2007 – С. 143-146

7. Вдовенко В.Г. Методология высшего профессионального образования: учеб.пособие/ СИБУП. – Красноярск, 2007. 248 с.

8. EUR-ACE (European Accredited Engineer.- http://www.feani.org/EUR_ACE/EUR_ACE_Main_Page.htm

9. Ассоциация инженерного образования России. - http://www.aeer.ru

ИДЕНТИФИКАЦИЯ УЧЕБНОГО МАТЕРИАЛА НА ОСНОВЕ ОТНОСИТЕЛЬНОЙ ВИРТУАЛЬНОЙ ВЕРБАЛЬНОЙ ИЗБЫТОЧНОСТИ

Котенко В.В., Жанкевич А.О.
ТРТУ
Таганрог, Россия

Интенсивное развитие информационных технологий объективно вызывает изменение требований к их защите. Одним из эффективных решений данной проблемы является поиск и исследование новых подходов решение задач аутентификации и идентификации. Исследования, проведенные авторами в этом направлении, позволили получить новый подход к идентификации текстов на основе виртуальной оценки информационных характеристик авторов, рассматриваемых в виде источников информации. Основа подхода составляет математическая модель вида:

$$m_B = \frac{H_{Bmax} - H_B}{H_{Bmax}}; G_B = \frac{H_B}{H_{Bmax} - H_B},$$

где H_{Bmax} - средняя виртуальная вербальная информационная емкость источника текста;

H_B - средняя виртуальная вербальная эмпирическая энтропия:

$$H_B = \frac{1}{N}\sum_{i=1}^{N} H_{Bi} \quad H_{B\max} = \frac{1}{N}\sum_{i=1}^{N} H_{B\max i}$$

Реализация данной модели в виде программного комплекса открывает принципиально новые возможности идентификации личности по тексту. На основе созданного комплекса исследовалась идентификация текстов ряда известных русских писателей. Результаты исследования приведены в таблице:

Таблица 1

Автор	$H_{B\max}$	H_B	m	G
А.А. Блок	8,722	7,575	0,132	6,576
А.П. Чехов	9,419	8,294	0,119	7,403
А.С. Пушкин	10,579	9,161	0.134	6.463
Н. В. Гоголь	12,133	10,130	0.165	5.061
И.С.Тургенев	12,518	10,079	0.195	4.128
М.Ф. Булгаков	11,633	9,397	0.192	4.208
М.Е.Салтыков – Щедрин	10,602	9,029	0,148	5,757
С. Есенин	11,199	9,286	0,171	4,848
Ф.М. Достоевский	12,435	9,818	0,210	3,762

Анализ приведенных результатов показывает, что каждому автору соответствует вполне определенные диапазоны значений m_B и G_B, которые могут быть использованы для идентификации. Данный вывод может быть обобщен для любого индивидуума. В данном случае в качестве объекта идентификации анализа целесообразно использовать написанное им сочинение, установленного объема, на произвольную тему.

Однако из результатов, приведенных в таблице 1, следует проблема, связанная с тем, что диапазоны виртуальной вербальной идентификации различных индивидуумов могут перекрываться. Следствием этого может являться неоднозначность идентификации. Данная проблема может быть решена путем применения подхода, основанного на определении средних значений результатов идентификации.

ОСОБЕННОСТИ ОЦЕНКИ ЭФФЕКТИВНОСТИ МЕТОДОВ СКРЕМБЛИРОВАНИЯ В ОБРАЗОВАТЕЛЬНЫХ СИСТЕМАХ

Котенко В.В., Румянцев К.Е., Евсеев А.С., Дергачев В.С.
Южный федеральный университет
Ростов-на-Дону, Россия

В основе применяемых в настоящее время подходов к оценке эффективности защиты аудиоинформации образовательных систем лежит 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.

Проведенные исследования показали, что одним из путей решения данной проблемы является виртуализация представления процесса защиты аудиоинформации, предусматривающая введение понятия виртуального шума скремблирования, определяемого как

$$\mathrm{e}_{c(i)} = VIR\left(\mathrm{x}\left(i\right) - \mathrm{y}\left(i\right)\right),$$

где $\mathrm{x}\left(i\right)$ – сообщение; $\mathrm{y}\left(i\right)$ – криптограмма.

С этих позиций на основании подхода, предложенного в [1], коэффициент избыточности ансамбля аудиосообщений X, присутствующий в ансамбле соответствующих им криптограмм Y может быть представлен в виде:

$$m_{\mathrm{y}}\left[\mathrm{X}\right] = 1 - \left(1 - \overset{\mathrm{o}}{\mathrm{I}}\left[\mathrm{X};\mathrm{Y}\right]\right)\frac{\mathrm{H}\left[\mathrm{X}\right]}{\mathrm{H}_{\max}\left[\mathrm{X}/\mathrm{Y}\right]},\ \overset{\mathrm{o}}{\mathrm{I}}\left[\mathrm{X};\mathrm{Y}\right] = \mathrm{I}\left[\mathrm{X};\mathrm{Y}\right]/\mathrm{H}\left[\mathrm{X}\right] \qquad (1)$$

Нормированное среднее количество информации $\overset{\mathrm{o}}{\mathrm{I}}\left[\mathrm{X};\mathrm{Y}\right]$ для речевых сообщений может быть определенно путем подхода предложенного в [1], как

$$\mathrm{H}\left[\mathrm{X}\right] = -\mathrm{W}\cdot\log\mathrm{W} - \frac{1-\mathrm{W}}{\mathrm{M}-1}\log\left(\frac{1-\mathrm{W}}{\mathrm{M}-1}\right) \qquad (2)$$

$$\mathrm{H}_{\max}\left[\mathrm{X}/\mathrm{Y}\right] = \frac{1-\mathrm{W}}{\mathrm{M}-1}\log\left(\mathrm{M}-1\right) - \frac{1-\mathrm{W}}{\mathrm{M}-1}\log\left(\frac{1-\mathrm{W}}{\mathrm{M}-1}\right) - \mathrm{W}\cdot\log\mathrm{W}, \qquad (3)$$

где W – разборчивость; M – количество логических элементов сообщений в выборочном пространстве ансамбля X.

Выражения (1) – (3) определяют математическую модель оценки эффективности защиты аудиоинформации на основе комплексного определения разборчивости и избыточности. Программная реализация данной модели позволила создать программный комплекс оценки эффективности скремблирования.

Проведенные исследования разработанного комплекса показывают, что предложенный подход открывает принципиально новую область возможностей оценки эффективности защиты аудиоинформации в первую очередь при значениях разборчивости близких к нулю. Кроме этого, открывается возможность применения для оценки эффективности защиты речевой информации известных и апробированных подходов оценки эффективности дискретной информации, основанных на определении избыточности.

СПИСОК ЛИТЕРАТУРЫ:

1. Величкин А.И. Передача аналоговых сообщений по цифровым каналам. М.: Радио и связь, 1983. 240 с.

НОВЫЙ ПОДХОД К ЗАЩИТЕ АУДИОИНФОРМАЦИИ В ОБРАЗОВАТЕДБНЫХ СИСТЕМАХ НА ОСНОВЕ ВИРТУАЛЬНОГО АДАПТИВНОГО АМПЛИТУДНОГО СКРЕМБЛИРОВАНИЯ

Котенко В.В., Румянцев К.Е., Евсеев А.С.
Южный федеральный университет
Ростов на Дону, Россия

Перспективным направлением реализации подхода, основанного на виртуализации информационных потоков в образовательных системах, является виртуальное амплитудное скремблирование, состоящее в рекуррентном формировании виртуальных криптограмм e_i^* из преобразованных по заданному правилу $\Phi_k\left\{\mathbf{g}\right\}$ сообщений и обратных преобразований $\Phi_k^{-1}\left\{\mathbf{g}\right\}$ криптограмм e_i^* и e_i по следующему алгоритму

$$\mathrm{e}_i^* = \Phi_k\left\{\mathrm{u}_i\right\} + \left[\Phi_k^{-1}\left\{\mathrm{e}_{i-n}^*\right\} - \left(\mathrm{u}_{i-m} - \left(\Phi_k^{-1}\left\{\mathrm{e}_{i-k}\right\} - \mathrm{u}_{i-l}\right)\right)\right]. \qquad (1)$$

При этом алгоритм дескремблирования определяется как