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

$$\hat{u}_i = \Phi_k^{-1}\left\{e_i^* - \Phi_k\left\{\Phi_k^{-1}\left\{e_{i-n}^*\right\} - \left[\hat{u}_{i-m} - \left(\Phi_k^{-1}\left\{e_{i-k}\right\} - \hat{u}_{i-l}\right)\right]\right\}\right\}, \qquad (2)$$

где *n, k, l* число тактов задержки.

Программная реализация приведенных алгоритмов позволила разработать программный комплекс адаптивного амплитудного скремблирования.

Особенностью данного комплекса является отсутствие источника ключевых последовательностей. В данном случае изменения u_i по закону ключа осуществляется виртуально, путем задания значений задержек *n, k, l.*

Результаты экспериментальных исследований эффективности предложенного комплекса показывают, что он обеспечивает более чем трехкратный выигрыш в разборчивости по сравнению с обычным амплитудным скремблированием.

Анализ результатов проведенных исследований позволил выявить особенность предложенного комплекса, состоящую в существенном уменьшении избыточности, по сравнению с обычным аналоговым скремблированием. Так, если средняя избыточность амплитудного скремблирования составляет 0,35, то при применении разработанного комплекса 0,089 – 0,101. При этом следует обратить внимание, что на величины разборчивости и избыточности оказывают влияния значения задержек. Таким образом, подбором значений задержек может достигаться требуемая эффективность скремблирования.

СПИСОК ЛИТЕРАТУРЫ:

1.Котенко В.В., Румянцев К.Е., Поликарпов С.В. Новый подход к оценке эффективности способов шифрования с позиций теории информации. Вопросы защиты информации: Науч.–практ. журн./ ФГУП «ВИМИ», 2004, №1. С. 16-22.

ПРОБЛЕМЫ МАТЕМАТИЧЕСКОЙ ПОДГОТОВКИ В ЭКОНОМИЧЕСКОМ ВУЗЕ

Пустобаева О.Н.
Сызранский филиал Самарского государственного экономического университета
Сызрань, Россия

Анализ содержания научно-теоретической и предметно-практической деятельности специалиста на примере основных экономических специальностей: коммерция, финансы и кредит, бухгалтерский учет и аудит, экономика и управление на предприятии, - позволяет выделить основные направления профессиональной деятельности экономиста информационного общества. К ним относятся:

- проектно-исследовательская;
- планово-финансистская;
- информационно-аналитическая;
- диагностическая;
- организационно-управленческая;
- экономически-инновационная;
- методически-консультационная;
- образовательная деятельности.

В основе выполнения перечисленных видов деятельности лежат математические знания из различных разделов математики: линейной алгебры, аналитической геометрии, интегрального и дифференциального исчислений, теории вероятности и математической статистики и т.д.

Однако чаще всего экономисты используют прикладные экономико-математические модели: оптимизационные модели; трендовые модели экономической динамики на основе одномерных временных рядов; балансовые модели в статистической и динамической постановке; эконометрические и многофакторные модели, главным образом линейные модели парной и многофакторной регрессии; модели спроса и потребления, управления запасами и систем массового обслуживания; теории игр; стохастические модели и др. [2], которые позволяют осуществлять анализ, прогнозирование, поиск и выбор оптимальных решений в различных областях экономики. Для структурирования, более компактного и обозримого представления имеющейся модели, быстрой ее обработки используются компьютерные программы.

На основе анализа математической составляющей в содержании профессиональной деятельности специалиста в области экономики можно утверждать, что базой для подготовки экономистов является математическая подготовка.

Математическая подготовка студентов состоит в изучении классической и прикладной математики, а также ее использовании при изучении других дисциплин.

Согласно учебным планам и программам вузовского обучения студентов экономических специальностей преподавание математики осуществляется у учащихся первого и второго курсов. На первом курсе экономических вузов рассматривается общий курс высшей математики, на втором – экономико-математические методы и модели, а также теория вероятности и математическая статистика.

Заметим, что специальные предметы, в основе которых используются математические знания, методы и модели, изучаются на старших курсах, поэтому никакие экономические проблемы в процессе преподавания математики рассматриваются на поверхностном уровне. Углубленное изучение экономических проблем с точки