ИНФОРМАЦИОННО–ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Козлова В. В., Савиных В. В.
Ульяновский государственный технический университет, Ульяновск

Для эффективного управления антропогенным воздействием на окружающую среду система экологической безопасности территории должна иметь следующие уровни: предприятие, муниципальное образование, субъект Федерации, Российская Федерация.

На каждом уровне система экологической безопасности состоит из трех стандартных модулей: комплексной экологической оценке территории, подсистемы экологического мониторинга и подсистемы управленческих решений. Содержание модулей на каждом уровне отличается масштабом районирования территории, функциями подсистемы экологического мониторинга, адресностью управленческих решений.

В работе предложены пути решения проблем по внедрению системы экологической безопасности Ульяновской области. Особое внимание уделено решению научно-методической и технической проблем. В научно-методическом плане в первую очередь необходимо разработать общие методологические принципы проведения комплексной экологической оценки территорий. Следующей сложной научно-методической задачей является разработка методики составления и ведения кадастров источников воздействия на окружающую среду. В ее основе должна лежать методология экологического риска с учетом устойчивости компонентов окружающей среды к антропогенному воздействию.

Техническая проблема создания системы экологической безопасности Ульяновской области заключается в выборе геоинформационной системы (ГИС), способной обеспечить сбор и анализ огромного массива разрозненной информации, поддерживать набор карт по оцениваемой территории и привязку результатов математического моделирования. В 2003 году в Ульяновском государственном техническом университете был разработан электронный вариант Экологического Атласа Ульяновской области (http://www.eco.ulstu.ru). Основными разделами этого документа являются: краеведение; законы; организации; кадастр; Красная книга. В состав тематических карт экологического атласа входит: климатическая карта, геологическая карта, карта растительности, карта рельефа, карта почв, центры переработки неметаллических полезных ископаемых, месторождения строительных материалов, карта Ульяновской области, схема минеральных источников и т. д.

В январе 2004 года была проведена спутниковая съемка Ульяновской области с космического аппарата, используемого для дистанционного зондирования Земли Terra, MODIS. MODIS (Moderate Resolution Imaging Spectroradiometer) – один из инструментов, находящихся на борту космического аппарата Terra, запущенного в декабре 1999 года. Сенсор MODIS осуществляет постоянную съемку поверхности Земли с периодом от 1 до 2 дней, обрабатывая данные в 36 спектральных каналах. Два канала (1, 2) имеют пространственное разрешение 250 метров, 5 каналов (3–7) имеют разрешение 500 метров, остальные каналы (8–36) обладают пространственным разрешением 1000 метров. Полоса обзора сенсора MODIS составляет 2330 километров.

В работе показано, что эффективное функционирование системы экологической безопасности Ульяновской области возможно только при знании природных свойств компонентов окружающей среды на территории области, наличии эффективной и регулярной системы контроля за воздействием природопользователей на окружающую среду и действенной системы управленческих решений.

АУТЕНТИФИКАЦИЯ КОРРЕСПОНДЕНТОВ ИНФОРМАЦИОННЫХ И БАНКОВСКИХ СИСТЕМ НА ОСНОВЕ ФОРМИРОВАНИЯ ВИРТУАЛЬНЫХ ИДЕНТИФИКАТОРОВ

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

Быстро прогрессирующее развитие информационных и компьютерных технологий открывает новый качественный уровень возможностей для дальнейшего совершенствования информационных и банковских систем. К сожалению, эффективность реализации этих возможностей сегодня сталкивается с целым рядом проблем, ставящих под угрозу функционирование самих систем. Одной из них выступает неуклонное возрастание угроз несанкционированного доступа к идентификаторам корреспондентов систем, наблюдаемое в последнее время. Сложившаяся ситуация осложняется тем, что существующие подходы к реализации задач аутентификации не в состоянии обеспечить решение данной проблемы.

Проведенные авторами исследования показывают, что данная проблема может быть решена путем применения подхода, состоящего в виртуализации выборочных пространств ансамблей идентификаторов. Содержание данного подхода состоит в использовании двух видов идентификаторов: виртуального и рабочего. Виртуальные идентификаторы находятся у корреспондентов и формируются ими. Особенностью предполагаемого подхода является то, что выборочные пространства ансамблей виртуального идентификатора X* является непрерывным, в результате чего обеспечивается его бесконечная энтропия ($H[X^*] = \infty$) для несанкционированного пользователя. Переход от непрерывной формы выборочного пространства виртуальных идентификаторов к дискретной форме, обязательной в системах, осуществляется путем применения программного комплекса аутентификации, разработанного и запатентованного авторами (рис.1). Основу функционирования комплекса составляет определение среднего количества информации и разборчивости. Численные значения комбинации этих параметров могут использоваться в качестве рабочего идентификатора. Предполагается

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.

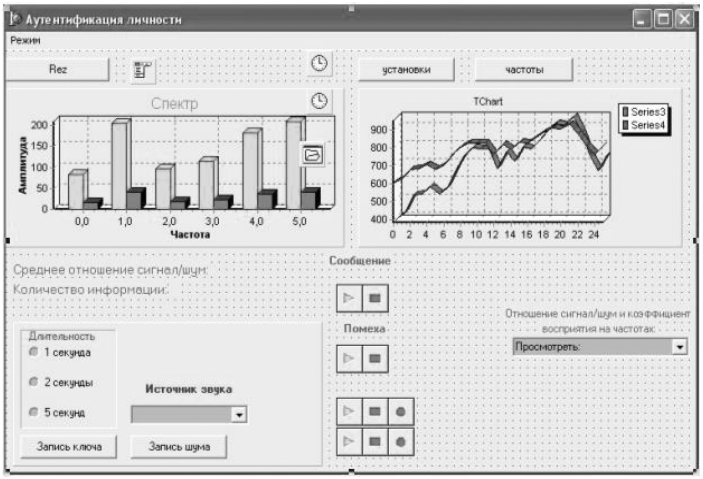

Рисунок 1

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.