Раздел I. Комплексная защита объектов информатизации

УДК 681.215

В.И. Васильев, В.А. Пестриков, А.С. Красько

ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ В ЭКСТРЕМАЛЬНЫХ СИТУАЦИЯХ НА ОСНОВЕ ВЫВОДА ПО ПРЕЦЕДЕНТАМ

Введение

Концепция «Безопасный город» представляет собой научно обоснованную систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты города от проявлений терроризма, экстремизма и других антиобщественных действий, а также чрезвычайных ситуаций природного и техногенного характера [1].

Актуальность постановки данной проблемы обусловлена серьезностью потенциальных угроз безопасности перечисленных объектов, масштабом и характером их последствий. Недостатками существующих подходов к реализации системы «Безопасный город» являются:

- завышение роли систем видеонаблюдения;
- узкая специализированность и малая интегрированность;
- плохая совместимость системных модулей различных производителей.

В последние годы внимание специалистов привлекают альтернативные способы противодействия угрозам террористического характера, направленные на повышение оперативности и эффективности работы правоохранительных органов и, как следствие, уменьшение потерь различных видов ресурсов, в том числе людских. Примером таких способов может служить использование разработанной американской компанией Safety Dynami устройства SENTRI (Smart Sensor Enabled Neural Threat Recognition and Identification) – интеллектуального нейронного сенсора, позволяющего распознавать и идентифицировать угрозы путем анализа звуковых сигналов [2].

Основная идея предлагаемого ниже подхода состоит в повышении достоверности и оперативности принятия решений по обеспечению безопасности в городе на основе их интеллектуальной поддержки с использованием принципов ситуационного управления и вывода по прецедентам.

1. Структура интеллектуальной системы мониторинга состояния территориально распределенных объектов и принятия решений при возникновении экстремальных ситуаций

Создаваемая система состоит из трех отдельных подсистем:

1) подсистема мониторинга состояния объектов контроля (на основе их предварительной паспортизации);
2) подсистема анализа оперативной ситуации, складывающейся на контролируемых объектах (с использованием вейвлет-преобразования аудио- и видеосигналов и нейросетевых технологий распознавания образов);

3) интеллектуальная система поддержки принятия решений на основе вывода по прецедентам (Case-Based Reasoning, CBR).

Общая структура информационных потоков, поступающих с распределенных датчиков, размещенных на объектах контроля и передаваемых на пульт централизованного контроля (ПЦК) по видео- и аудиоканалу (после их предварительной обработки на объектах контроля), показан на рис. 1.

Основные задачи, решаемые этой системой:

- сбор оперативной информации о состоянии объектов контроля (по видео- и аудиоканалу);
- уплотнение и передача информации на пульт централизованного контроля (ПЦК) с территориально распределенных объектов;
- обработка поступающей в режиме реального времени информации (анализ, распознавание источников угроз, формирование предупреждающих сигналов).

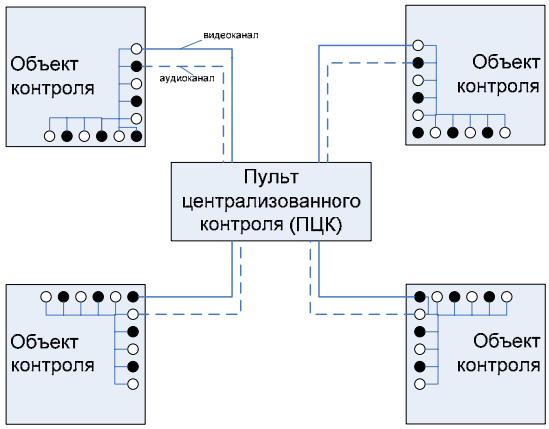

Рис. 1. Информационная система сбора и обработки информации

2. Этапы создания системы

Решение перечисленных выше задач осуществляется в два этапа:

1. Алгоритмический (математический) аспект:

- на основании информации, поступающей в реальном режиме от датчиков акустических сигналов $S_1^j, S_2^j, ..., S_{mj}^j$, (j=1,2,…n), где m_j – число датчиков на j-м объекте контроля; n – число объектов контроля., определить интенсивность, положение (координаты) и характер (тип) источника опасного сигнала (угрозы).

Особенности постановки и решения данной задачи включают в себя:

- учет диаграмм направленности и других характеристик датчиков;
- использование метода триангуляции для обнаружения координат местоположения источника звукового сигнала;
- оценку погрешности определения координат источника угрозы;
- анализ (преобразование) полученных сигналов с целью выявления их характерных признаков (атрибутов) источника угрозы;
- отнесение источника угроз к одному из типовых классов;
- принятие решения в ПЦК о необходимых действиях при обнаружении источника угрозы.

2. Технический (программно-аппаратный) аспект – связан с формулированием предложений (рекомендаций) по практической реализации алгоритмов обработки сигналов и принятия решений.

На данном этапе решаются такие вопросы, как:

- выбор конкретных типов датчиков аудиосигналов с учетом особенностей объектов контроля;
- выбор способов предварительной обработки (преобразования и уплотнения) и передачи сигналов от датчика на ПЦК;
- выбор способов и программного обеспечения для обработки полученных сигналов в ПЦК на основе предложенных алгоритмов;
- решение вопросов интеграции предполагаемого подхода с существующей системой мониторинга территориально распределенных объектов на основе видеонаблюдения;
- технико-экономическое обоснование эффективности предложенных решений.

3. Виды объектов контроля

Для правильного выбора мест установки датчиков, методов и средств обработки полученных с них сигналов и оперативного принятия решений с целью формирования адекватных действий при возникновении экстремальных ситуаций необходимо разработать нормативно-правовые документы (и их электронные варианты), характеризующие уровень защищенности критически важных объектов (паспорта безопасности).

Паспорт безопасности объекта должен устанавливать основные требования к структуре, составу и характеру необходимых действий для обеспечения безопасности объекта в случае возникновения экстремальных ситуаций, проявлений терроризма и других антиобщественных явлений [3].

Паспорт безопасности должен предусматривать решение следующих задач:

- определение возможности возникновения указанных ситуаций;
- оценку возможных последствий этих ситуаций;
- определение показателей риска для населения, проживающего на прилегающей территории, и других объектов;
- разработку мероприятий по снижению риска и смягчению последствий экстремальных (чрезвычайных) ситуаций.

На основании результатов анализа предлагается выделить несколько типов (классов) объектов контроля.

Первый класс объектов – это оживленные городские автомагистрали. Целью мониторинга является оценка ситуационной (оперативной) обстановки на основных транспортных магистралях города. Экстремальные ситуации, возникающие на автомобильных магистралях города, чреваты возникновением большого числа “пробок”, невозможностью проезда машин спецслужб города. Данные события могут носить как случайный, так и преднамеренный характер со стороны злоумышленников, с целью блокирования и создания напряженности на автомагистралях или в каких-либо районах города.

Второй класс объектов контроля – места массового отдыха горожан и проведения общегородских мероприятий. Объектами наблюдения являются одиночные (подозрительные) граждане и различные по численности группы граждан (толпа).

Третий класс объектов контроля – театрально-развлекательные комплексы. Объектами наблюдения являются большие скопления людей, находящиеся в ограниченном замкнутом пространстве.

Объем паспорта безопасности будет зависеть от полноты классификации критериев и характеристик, определяющих обстановку на объекте контроля.

4. Выбор технических средств мониторинга и вейвлет-анализа аудиосигналов

Решение данной задачи предполагает:

- выбор направленных микрофонов, анализ совместимости их с техническими характеристиками систем наружного наблюдения;
- выбор способа размещения микрофонов на объекте;
- использование стандартных (существующих) интерфейсов и каналов передачи информации на ПЦК;
- использование различных видов преобразований (БФП, вейвлет) для анализа сигналов, поступающих с датчиков в реальном времени.

Как показывают исследования, эффективное распознавание акустических сигналов возможно с помощью нейросетевых технологий основанных на использовании вейвлет-преобразований [4]. Известно, что традиционный аппарат представления сигналов в виде рядов Фурье оказывается малоэффективным для сигналов с локальными особенностями, в частности для импульсных сигналов. Это связано с тем, что базисная функция рядов Фурье – синусоида – определена во времени и в пространстве от $-\infty$ до $+\infty$ и является строго периодической функцией. Такая функция принципиально не способна описать произвольные сигналы, наблюдаемые в реальной жизни.

Если исследуемый процесс отличается нестационарностью, что характерно для реальных звуковых сигналов с непостоянной шумовой составляющей, применение спектрального анализа не дает эффективных результатов, особенно если нестационарность во времени значительно меньше анализируемого временного интервала. Это обстоятельство наглядно проявляется для исследуемой задачи.

Для иллюстрации вышесказанного рассмотрим два сигнала – информационный, соответствующий одиночному выстрелу (рис. 2, a) и шум (рис. 2, b), аналогичный шумовой составляющей сигнала на рис.2,a. Полученные Фурье-спектры (рис. 2, c, d) этих двух сигналов весьма похожи. На участках от 0 до 500 Гц выявляются пики, относящиеся только к шумовой составляющей сигнала, видны пики с частотой менее 100 Гц. Информационную составляющую сигналов можно пытаться определить на частотах (900-2500 Гц), где отличие обоих файлов максимально. В то же время анализ спектров, полученный с помощью преобразования Фурье, не позволяет выявить важной особенности исходного сигнала – момента времени, когда меняется состав исходного сигнала.

Важным достоинством вейвлет-преобразования является возможность представлять нестационарные сигналы, состоящие из разных компонент, действующих в различные промежутки времени. Вейвлет-спектрограммы позволяют выявить тончайшие локальные особенности сигналов с привязкой их ко времени и координатам пространства, что позволяет использовать их при решении задач мониторинга состояния территориально распределённых объектов.

Подсистема, осуществляющая вейвлет-анализ сигналов, т.е. их разложение на аппроксимирующие и детализирующие коэффициенты, позволяет выделить информационную составляющую сигнала его последующего распознавания. В случае, если выявлено увеличение коэффициентов разложения по сравнению с их усредненными значениями, включается нейросетевая подсистема распознавания сигналов.

При этом данные о максимальных пиках разложения сигналов, поступают на входы нейронной сети, которая после обучения может распознавать поступающие

сигналы, присваивать им тот или иной класс опасности и преобразовывать полученную информацию для ввода в систему поддержки и принятия решений (СППР).

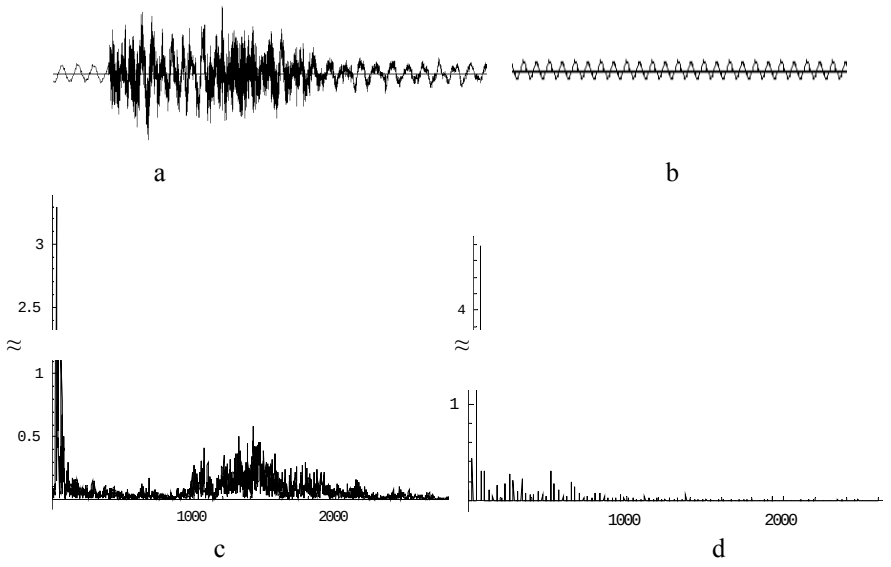

Рис. 2. Сигналы и их Фурье-спектры

Результат вейвлет-преобразования акустического сигнала, представленного на рис. 2,а, приведен на рис. 3.

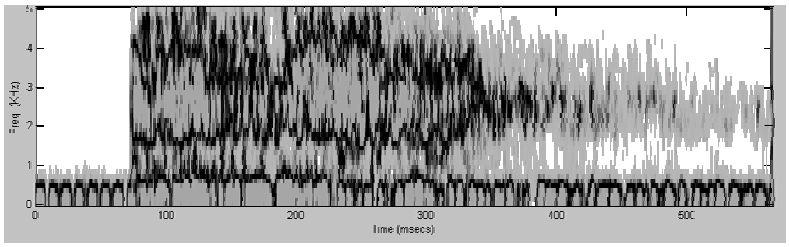

Рис. 3. Вейвлет-разложение сигнала

5. Распознавание ситуации на основе прецедентов и принятие решения

В связи с тем, что оперативность и корректность принятия решений напрямую зависит от объема информации, поступающей от средств контроля обстановки в особо ответственных местах города, скорости передачи данных по каналам связи и т.п., причем процесс принятия решений во многом носит субъективный характер (поскольку на лицо, принимающее решение, влияют такие факторы, как его образование, опыт, психологическое состояние и т.д.), то целесообразность разработки и внедрения СППР сегодня не вызывает сомнения у специалистов [5].

Системы вывода, основанного на прецедентах (рис. 4), оказываются в данном случае предпочтительнее по сравнению с экспертными системами, основанными на правилах. Для оценки текущей ситуации при этом используется информация о том, как в подобных случаях поступали раньше, т.е. производится анализ преце-

дентов. Прецедент – это описание проблемы или ситуации с подробным указанием действий, предпринимаемых в аналогичной ситуации для решения аналогичной проблемы. Подход, основанный на прецедентах, сводится к выполнению следующего алгоритма:

- получение информации о признаках текущей ситуации;
- сопоставление этой информации с признаками прецедентов, хранящихся в базе знаний, для выявления аналогичных прецедентов;
- выбор прецедента, наиболее близкого к текущей ситуации;
- адаптация выбранного решения к текущей проблеме, если это необходимо;
- проверка эффективности полученного решения;
- занесение информации о новом прецеденте в базу знаний (прецедентов).

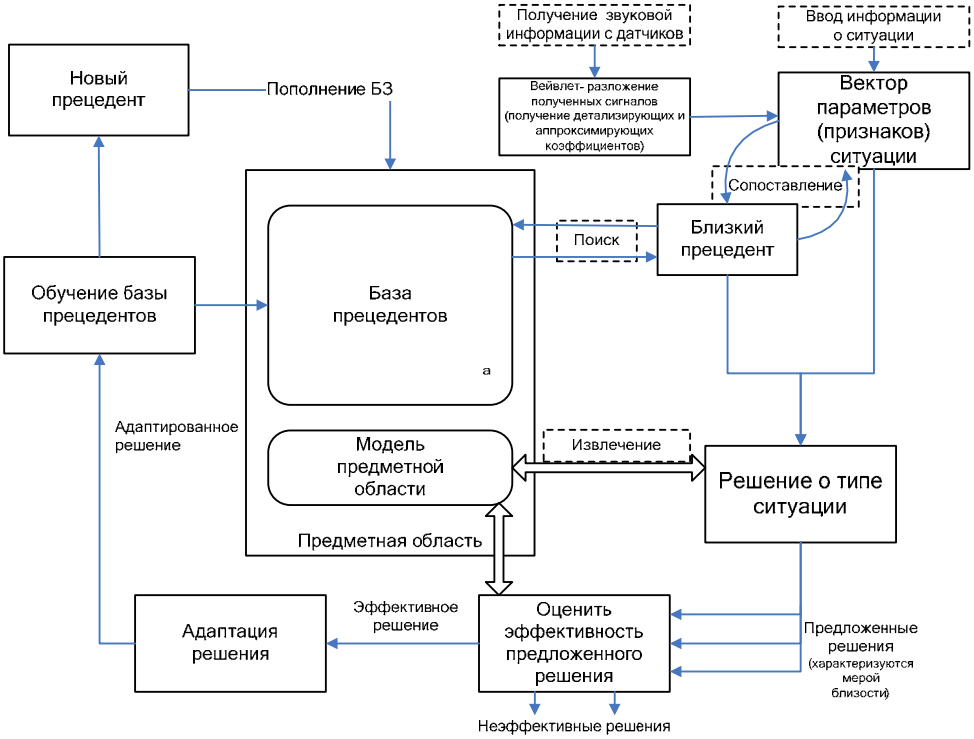

Рис. 4. Схема принятия решений на основе прецедентов

В качестве меры близости (расстояния до прецедента) можно использовать, например, Евклидову метрику:

$$l_{pj} = \sqrt{\sum_{i=1}^{n} \left(x_{\text{pi}} - x_{ji} \right)^2} ,$$

где x_{ji}, x_{pi} – соответственно значения i-го параметра (признака ситуации) для вектора состояния объекта контроля $\overline{X}_j$ и эталонного вектора состояния $\overline{X}_p$ (предполагается, что $\overline{X}_j$ и $\overline{X}_p$ нормированы, т.е. из компоненты принадлежат интервалу [0,1]); n – размерность векторов параметров $\overline{X}_j$ и $\overline{X}_p$.

Ближайший прецедент $\overline{X}_s$ при этом выбирается по правилу:

$$\overline{x}_s = \overline{x}_p \mid l_{si} = \min_p l_{pj},$$

где k – количество прецедентов.

Исследовательский прототип СППР создается на базе Delphi 7 с использованием MS Access в качестве базы знаний для хранения запросов и базы прецедентов. В данном программном продукте производится ввод параметров (признаков) ситуации. После ввода данных происходит поиск ближайших прецедентов, вывод информации о принятых решениях (с указанием расстояния до прецедентов) и пополнение базы прецедентов (рис.5).

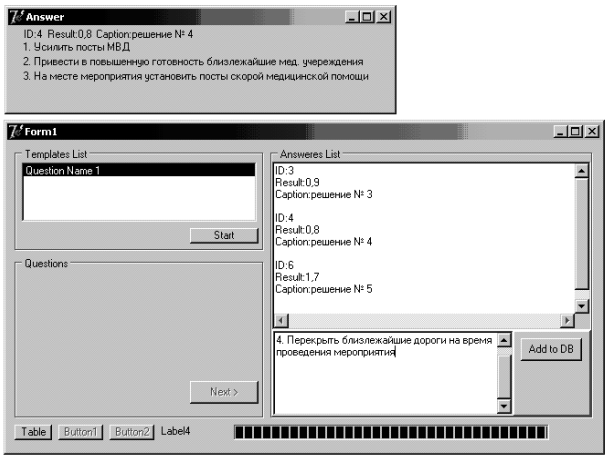

Рис. 5. Вывод данных и пополнение базы прецедентов

6. Выводы

Целью создания интеллектуальной системы поддержки принятия решений является повышение достоверности и оперативности действий по обеспечению безопасности в городе на основе принципов ситуационного управления и вывода по прецедентам. Систематизация данных, характеризующая уровень защищенности важных объектов на основе паспортов безопасности, устанавливает при этом основные требования к структуре, составу и характеру необходимых действий для обеспечения безопасности объекта в случае возникновения экстремальных ситуаций. Применение вейвлет-преобразования акустических сигналов позволяет распознать характер и положение источников угроз, что является предпосылкой к распознаванию экстремальной ситуации на объекте. На основе системы вывода по прецедентам определяется тип этой ситуации и осуществляется выбор типового

решения, которое должно использоваться при планировании действий силовых структур.

В целом, разработка и внедрение предлагаемой системы позволит повысить оперативность и объективность принимаемых решений по оценке оперативной обстановки, значительно сократить время реагирования на возникшие экстремальные ситуации, повысить уровень защищенности критически важных объектов территориальных объектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев В.И., Красько А.С., Матвеев П.В., Никитин А.А., Пестриков В.А.* О создании концепции безопасный город // Информационная безопасность: Материалы VIII Международной научно-практической конференции. Ч.1. – Таганрог: Изд-во ТРТУ, 2006. – С.28 – 30.

2. www.safetydynamics.net

3. *Андреев Н.Д., Дуленко В.А., Михайлов В.И., Пестриков В.А.* Методические рекомендации по разработке паспорта безопасности подразделения органов внутренних дел. – Уфа: Изд-во УЮИ МВД РФ, 2005. – 17 с.

4. *Дьяконов В.П.* Вейвлеты. От теории к практике – М.: Солон-Р, 2002. – 448 с.

5. *Бадамшин Р.А., Черняховская Л.Р., Ильясов Б.Г.* Проблемы управления сложными динамическими объектами в критических ситуациях на основе знаний. – М.: Машиностроение, 2003. – 240 с.

УДК 681.3

С.А. Радько, О.М. Лепешкин

РАЗВИТИЕ МЕТОДОЛОГИЧЕСКОГО ПОДХОДА РАЗРАБОТКИ ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННОЙ МОДЕЛИ ДОСТУПА СОЦИОТЕХНИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

В результате объединения сложных социальных и технико-технологических систем в социотехническую перед современными системами управления стоит проблема решения организационно-управленческих задач распределения и контроля использования информационных ресурсов в реальном масштабе времени. Ввиду того, что данная задача связана с ключевыми понятиями «функции» и «ресурсы», актуальна тема разработки функционально-дискреционной модели доступа (ФДМД).

Подход реализации данной модели направлен на безопасность функционирования критических информационных систем обработки информации в органах управления. Причем в качестве объекта в СТИС рассматривается не вычислительная система как такова, а информационно-управляющая система, которой свойственны следующие особенности:

- работа в реальном масштабе времени;
- специфические требования по надежности и безопасности функционирования;
- эксплуатационные и инструментальные особенности;
- непрерывный режим функционирования;
- оператор часто отсутствует;
- нештатные ситуации должны корректно разрешаться самой вычислительной системой;