В.С. Дунин,
Дальневосточный юридический институт МВД России

О.И. Бокова,
доктор технических наук, профессор

Н.С. Хохлов,
доктор технических наук, профессор

ПОСТРОЕНИЕ МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОВД НА ОСНОВЕ НЕЧЕТКОЙ НЕЙРОННОЙ ПРОДУКЦИОННОЙ СЕТИ

CONSTRUCTION OF THE MODEL OF INTELLIGENT SYSTEM OF SECURITY MANAGEMENT OF THE FACILITY INFORMATION MINISTRY OF THE INTERIOR BASED ON FUZZY NEURAL NETWORK PRODUCTION

Рассматривается построение модели интеллектуальной системы управления безопасностью объекта информатизации ОВД, основанной на интеграции механизмов нечеткого логического вывода и нейронных сетей для формализации сложных процессов управления.

The article discusses the construction of model of intellectual security management system of the object informatization of the Ministry of the Interior, based on integration of the mechanisms of fuzzy logical inference with neural networks for formalization of complex management processes.

Для обеспечения эффективного функционирования систем безопасности объектов информатизации используются системы управления безопасностью (СУБ). В таких системах реализуются функции планирования, управления, анализа, координации и прогнозирования, а также осуществляется оперативное обеспечение информацией лица, принимающего решения [1].

Управление системой безопасности понимается как процесс изменения структуры, алгоритмов и параметров системы безопасности с целью достижения оптимального состояния системы при изменении условий работы системы: появлении несанкционированных или непреднамеренных воздействий, каналов утечки информации.

Создание СУБ требует наличия информации об объекте управления, задания входных и выходных переменных. Объект защиты — объект информатизации, представляющей собой совокупность средств вычислительной техники, информационных ресурсов, технологий и исполнителей.

К одному из таких объектов, состоящих из множества подсистем функционирования, предоставляющих лицам, принимающим решения, эффективный инструмент управления, можно отнести комплексную автоматизированную интеллектуальную систему (КАИС) «Безопасный город», которая внедряется в органах внутренних дел в соответствии с программами построения правоохранительного сегмента системы обеспечения общественной безопасности городов Российской Федерации.

Существующий проект типовой модели КАИС «Безопасный город» представляет собой сложноорганизованную интеллектуальную территориально-распределенную систему безопасности, построение которой основывается на универсальной программ-

но-аппаратной платформе в соответствии с нормативно-техническими требованиями к программно-техническому комплексу системы. Так, развернутый на базе дежурной части УВД по городу Хабаровску центр управления нарядами, а также локальные центры управления — дежурные части отделов милиции города являются объектами информатизации и концентрации информационных ресурсов ограниченного распространения, циркулирующих на уровне сетевого взаимодействия подсистем КАИС «Безопасный город», доступ к которым осуществляется через удаленные рабочие места (хосты) дежурной смены. Состав данных подсистем различен, некоторые из них имеют свою внутреннюю инфраструктуру, свой синтаксис, свои СУБД, свои интеллектуальные средства поддержки.

При управлении в условиях информационного противоборства субъектов (программа, процесс, злоумышленник), реализующих или пытающихся реализовать угрозы от вторжения атак (Dos и DDos-атаки, атаки типа «Анализ сетевого трафика», «Перехват парольной информации», инсайдерские атаки и т.д.) и объектов (информационно-телекоммуникационная инфраструктура КАИС «Безопасный город»), имеет место отклонение состояния системы защиты информации относительно заданного состояния, при этом управляющая система не обладает полной информацией о состоянии информационной среды и состоянии объекта управления. Это связано с тем, что для формирования командной информации, реализующей управление в реальном времени, необходим регулярный контроль и оперативный анализ данных о подозрительной активности, которую можно идентифицировать как атаку.

Перед подразделениями, обеспечивающими информационную безопасность единого информационного пространства (ЕИП) ОВД, ставится задача эффективного управления защитой информации во все более усложняющейся сетевой среде. Требуются динамические методы, позволяющие оперативно контролировать изменения условий среды функционирования и предотвращать нарушения информационной безопасности, управляя сетевым оборудованием и средствами защиты.

Одним из таких инструментов, обеспечивающих эффективное, динамическое функционирование системы управления безопасностью информационной среды, является интеллектуальное управление.

Интеллектуальное управление возникает там, где информация трактуется как количественно неопределяемая совокупность данных, знаков, утверждений (распознавание образов, информационно-аналитический анализ криминальной обстановки на территории города, вероятность идентификации (распознавание) атак, реализующих угрозы хостам ЕИТКС ОВД, события информационной безопасности на пути распространения атак) и отношений между ними в логически ясном контексте их изложения [2].

Структура системы интеллектуального управления связана с моделью системы, в которой должны быть определены как традиционные элементы системы управления, так и модели обработки знаний, реализуемые интеллектуальной системой. С учетом существующих структур интеллектуальных систем, взаимодействующих с внешней средой для формирования целей управления, предложим структурную модель системы управления информационной безопасностью КАИС «Безопасный город» как типового объекта информатизации (рис.1).

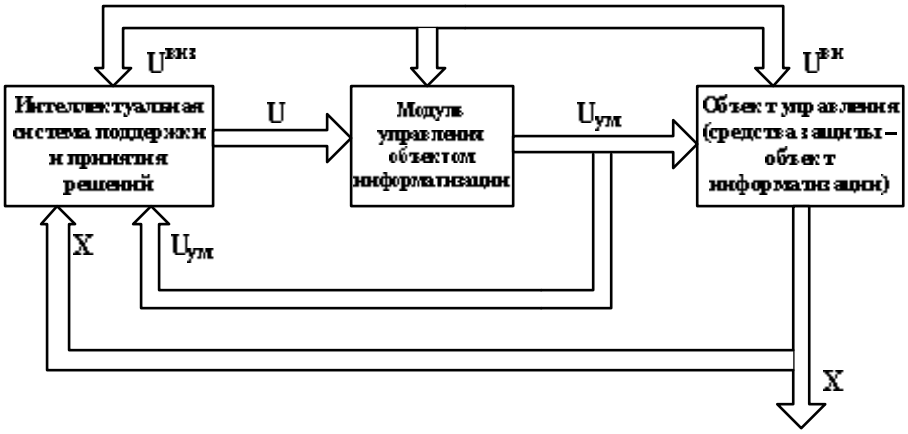

Рис.1. Структурная модель системы управления безопасностью объекта информатизации

Здесь: X – множество выходных управляемых переменных объекта управления; U — множество допустимых значений выходных переменных (заданные входные воздействия); $U_{ум}$ — множество управляющих воздействий; $U^{вн}$ — множество возмущающих воздействий, которое описывает возможные потенциальные действия злоумышленника (например, внешние угрозы информационной безопасности); $U^{вн3}$ — множество знаний о внешней среде воздействия на объект управления, заложенных в системе поддержки и принятия решений.

Главным элементом представленной модели, является интеллектуальная система поддержки и принятия решений по формированию управляющей командной информации в сложных, не всегда однозначных (не ясных, не четких) условиях функционирования объекта информатизации.

Интеллектуализация процессов управления имеет в виду использование математического, алгоритмического и программного обеспечения управляющих систем, способных решать задачи путем приобретения, хранения и целенаправленного преобразования знаний в процессе адаптации к разнообразным обстоятельствам (например, когда осуществляется информационно-технологический взаимообмен между разнородными информационными ресурсами КАИС «Безопасный город» или ЕИП ОВД).

Использование этого подхода в управляющей системе позволяет учитывать особенности обработки знаний различных типов, решать проблему неполноты, противоречивости и неопределенности знаний, присущих реальным системам защиты информации и системам поддержки принятия решений.

В последние годы наблюдается повышенный интерес к использованию нечетких интеллектуальных технологий и разработке нечетких прикладных систем и моделей.

Теория нечетких множеств, особенно те ее аспекты, которые связаны с лингвистической неопределенностью, часто возникающей при работе с экспертами на естественном языке, может быть использована как средство сбора и обработки нечеткой информации, представленной экспертом [3].

Одним из основных понятий, используемых в математических моделях для описания нечеткой величины, является понятие лингвистической переменной (ЛП), значениями которой являются не числа, а слова и предложения. Например, ЛП «число событий информационной безопасности на хосте конфиденциального контура ЕИТКС» может принимать значения: мало, средне, выше среднего, много, очень много, а ЛП «вероятность идентификации (распознавания) атаки по подозрительной активности» может принимать значения: малая, низкая, средняя, высокая.

Множество допустимых значений лингвистической переменной является терм-множеством. Формально ЛП описывается следующей пятеркой компонентов [4]:

$$ЛП = \langle X, T, U, G, M \rangle, \quad (1)$$

где X — имя ЛП («вероятность идентификации атаки»);

T — множество термов (значений) ЛП, которое представляет собой наименования нечеткой переменной;

U — область, на которой определены значения ЛП, определяется экспертом на основе анализа путей распространения атак;

G — описывает операции по порождению произвольных значений ЛП на основе тех, что входят в терм-множество; с помощью правил из G можно расширить терм-множество.

Компонент M образует набор семантических правил, с помощью которых происходит отображение значения лингвистической переменной в нечеткие множества U и выполняются обратные преобразования. Эти правила обеспечивают формализацию качественных утверждений экспертов при формировании проблемной области в памяти интеллектуального средства.

Построение модели реальной системы нечеткого вывода включает в себя ряд этапов (покажем на примере ЛП = «вероятность идентификации (распознавания) атаки по подозрительной активности») [5]:

1. Определение способа (схемы) нечеткого вывода заключений.

Способ вывода представляет собой конкретизацию методов прямого и обратного вывода заключений в системах нечетких продукций, в которых условия и заключения записаны в форме нечетких лингвистических переменных. Информацией, которая поступает на вход системы нечеткого вывода, являются измеренные некоторым образом входные переменные − число признаков аномальных событий. Эти переменные соответствуют реальным процессам в сети. Информация, которая формируется на выходе системы нечеткого вывода, соответствует выходной переменной, которая является коэффициентом уверенности в том, что аномальные события в сети являются атакой.

2. Формирование базы нечетких продукционных правил.

Система нечеткого вывода предназначена для преобразования значений входных переменных − информации о числе индикаторов – в выходную переменную на основе использования нечетких правил продукций (см. рис.2). Для этого система нечеткого вывода должна содержать базу правил нечетких продукций и реализовывать нечеткий вывод заключений на основе посылок или условий, представленных в форме нечетких логических высказываний, типа «ЕСЛИ X есть A, ТО Y есть D», «ЕСЛИ X_1 есть A и X_2 есть B, ТО Y есть D_1» и «ЕСЛИ X_1 есть A или X_3 есть B, ТО Y есть D_2» и др.

В зависимости от количества нечетких высказываний в предпосылках и заключениях база правил нечеткой продукционной модели может быть представлена структурой одного из следующих типов:

SISO-структура (SingleInput — SingleOutput, один вход — один выход);

MISO-структура (MultiInputs — SingleOutput, много входов — один выход);

MIMO-структура (MultiInputs — MultiOutputs, много входов — много выходов).

3. Процедура введения нечеткости (фаззификация). Следующий этап нечеткого вывода — фаззификация, под которой понимается процедура нахождения значений функций принадлежности нечетких множеств (термов) на основе обычных (не нечетких) исходных данных. Целью этапа фаззификации является установление соответствия между числовыми значениями отдельной входной переменной системы

нечеткого вывода и значением функций принадлежности соответствующего ей терма входной лингвистической переменной. После завершения этого этапа для всех входных переменных должны быть определены конкретные значения функций принадлежности по каждому из лингвистических термов, которые используются в подусловиях базы правил.

4. Процедура агрегирования степени истинности предпосылок по каждому из нечетких продукционных правил.

На этапе агрегирования определяется степень истинности условий по каждому из правил системы нечеткого вывода. Если условие правила состоит из нескольких подусловий, то определяется степень истинности сложного высказывания на основе расчетных формул нечеткой конъюнкции или нечеткой дизъюнкции. Этап агрегирования считается законченным, когда найдены все значения истинности для каждого из правил, входящих в рассматриваемую базу правил системы нечеткого вывода. Те правила, степень истинности условий которых отлична от нуля, считаются активными и используются для дальнейших расчетов, при этом для сокращения времени вывода учитываются только активные правила нечетких продукций.

5. Процедура аккумулирования активизированных заключений всех нечетких продукционных правил для каждой выходной переменной.

Аккумуляция значений нечетких правил продукций осуществляется для объединения нечетких множеств, соответствующих термам подзаключений, относящихся к одним и тем же выходным лингвистическим переменным.

6. Процедура приведения к четкости (дефаззификация) для каждой аккумулированной выходной переменной.

Дефаззификация в системах нечеткого вывода представляет собой процедуру или процесс нахождения обычного (не нечеткого) значения выходных лингвистических переменных. Дефаззификацию называют приведением к четкости. Действительно, применяемые в системах управления модули способны воспринимать команды в форме количественных значений соответствующих переменных. При дефаззификации в соответствии с методом центра тяжести обычное (не нечеткое) значение выходной переменной равно абсциссе центра тяжести площади, ограниченной графиком кривой функций принадлежности выходной переменной.

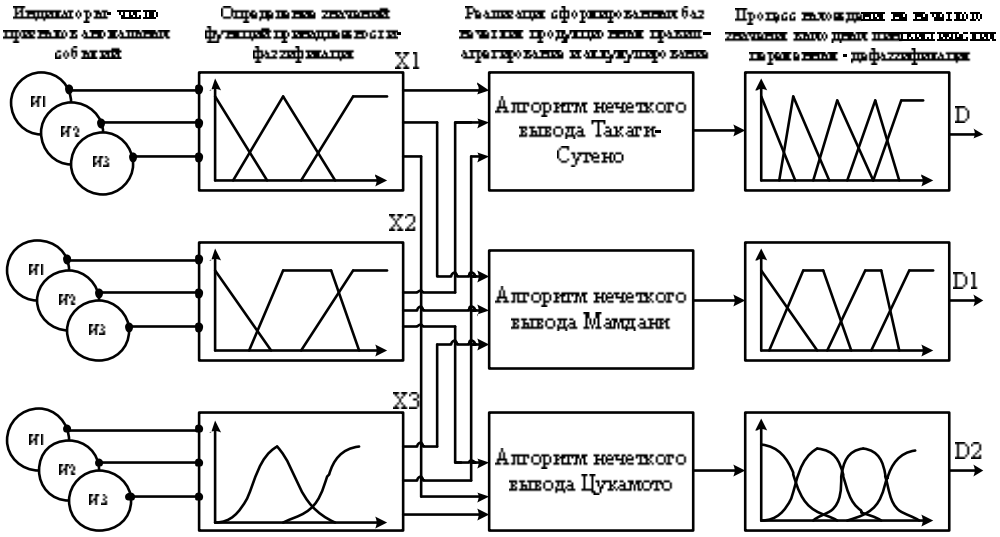

Рис. 2. Общая схема механизма одного из алгоритмов нечеткого логического вывода

Важными преимуществами моделей реальных систем, построенных на основе нечеткой математики, являются большая гибкость и адекватность реальному миру, а также более быстрое, по сравнению с традиционными моделями, получение окончательного результата через специфическое построение и простоту используемых нечетких операций.

Несмотря на несомненные достоинства нечетких продукционных моделей при решении целого ряда задач, в которых информация о системе, ее параметрах, а также о входах, выходах и состояниях системы является ненадежной и слабоформализованной, и заключающиеся, прежде всего, в описании модели на языке, близком к естественному, вместе с тем для нечетких продукционных моделей характерны и определены недостатки [5]:

исходный набор нечетких правил формируется экспертом и может оказаться неполным или противоречивым;

субъективность в выборе вида и параметров функций принадлежности в нечетких высказываниях;

отсутствует возможность автоматического приобретения знаний.

Формально нечеткие продукционные модели и алгоритмы нечеткого вывода на их основе могут быть представлены в виде нечетких продукционных сетей, по структуре идентичных многослойным нейронным сетям с прямым распространением сигнала (feedforward), элементы каждого слоя которой реализуют отдельный этап нечеткого вывода в нечеткой продукционной модели:

первый слой нейронов выполняет функцию введения нечеткости (фаззификация);

скрытые слои отображают совокупность нечетких правил и реализуют алгоритм нечеткого вывода;

последний слой выполняет функцию приведения к четкости (дефаззификация) выходной переменной.

Для устранения указанных выше недостатков в ряде работ [6] предложено создавать нечеткие продукционные модели адаптивными (с коррекцией в процессе и по результатам их функционирования как состава правил в базе, так и параметров функций принадлежности), а также реализовывать различные компоненты этих моделей на основе нейросетевой технологии.

Представление различных компонентов нечеткой продукционной модели с использованием нейронных сетей предполагает, прежде всего, использование формализмов, принятых при описании и функционировании нейронов и искусственных нейронных сетей. Объединение обоих подходов (нечеткой логики и нейронных сетей) позволяет, с одной стороны, привнести способность к обучению и вычислительную мощность нейронных сетей в системы с нечеткой логикой, а с другой — усилить интеллектуальные возможности нейронных сетей свойственными «человеческому» способу мышления нечеткими правилами выработки решений.

Учитывая имеющиеся механизмы по интеграции нечетких моделей с нейронными сетями, позволяющие более эффективно решать задачи формализации предлагаемых целей управления, предложим структурную модель интеллектуальной системы поддержки и принятия решений по управлению безопасностью объекта информатизации, построенную на основе нечеткой нейронной продукционной сети (рис. 3).

Как видно из рис.3, первый слой (***Слой 1***) нечеткой продукционной сети представляет собой множество нейронов, выполняющих функцию введения нечеткости — фаззификацию, скрытые слои (***Слой 2, Слой 3, Слой 4***) отображают совокупность нечетких правил и реализуют алгоритм нечеткого вывода (например, Такаги — Сугено), последний слой (***Слой 5***) выполняет функцию приведения к четкости — дефаззификацию выходной переменной.

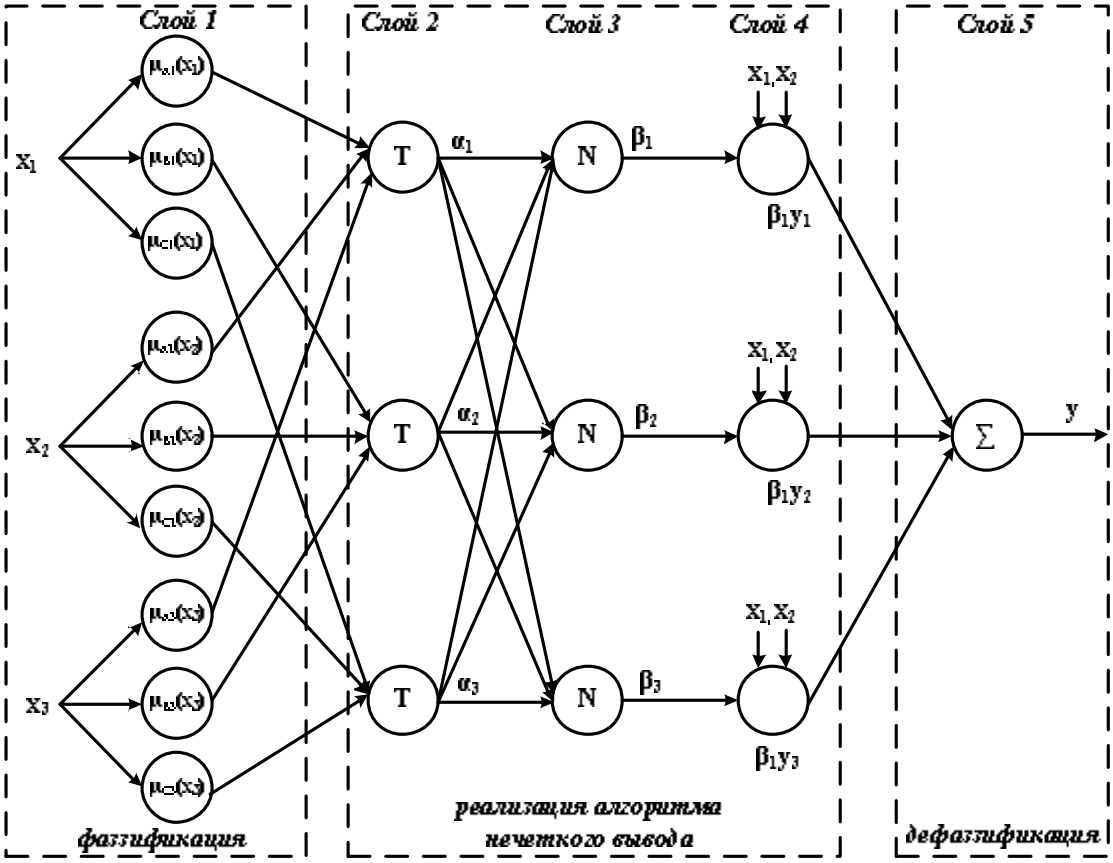

Рис. 3. Структура нечеткой продукционной сети ANFIS, реализующая алгоритм нечеткого вывода Такаги — Сугено

В отличие от «чистых» нейронных сетей каждый слой в целом и отдельные составляющие его элементы, так же как и конфигурация связей, все параметры и веса имеют физическую интерпретацию. Это свойство оказывается необычайно важным, поскольку знания не распределяются по сети и могут быть легко локализованы и при необходимости откорректированы экспертом.

Представляемая нечеткая нейронная сеть сможет одновременно формировать нечеткие правила и адаптировать функции принадлежности путем модификации весов связей в процессе обучения и — что самое важное — для этого может применяться классический алгоритм обратного распространения ошибки.

Анализируя эффективность использования алгоритмов нечеткого вывода, базирующихся на нечетких продукционных моделях Мамдани, Цукамото, Такаги — Сугено при решении таких задач, как аппроксимация непрерывной функции, распознавание образов, классификация, оптимизация по различным критериям (обеспечение точности аппроксимации, вычислительные затраты на реализацию, оптимальность управления, минимизация времени для принятия решений), следует отметить, что алгоритм Такаги — Сугено является одним из оптимальных методов описания нечеткой нейронной продукционной сети.

Рассмотрим нечеткую сеть типа ANFIS, реализующую алгоритм нечеткого вывода Такаги — Сугено и основанную на следующих правилах:

П1: ЕСЛИ x_1 есть A_1 И x_2 есть A_2 И x_3 есть A_3, ТО $y_1 = D_1x_1 + D_2x_2 + D_3x_3$;

П2: ЕСЛИ x_1 есть B_1 И x_2 есть B_2 И x_3 есть B_3, ТО $y_2 = E_1x_1 + E_2x_2 + E_3x_3$;

ПЗ: ЕСЛИ x_1 есть C_1 И x_2 есть C_2 И x_3 есть C_3, ТО $y_3 = F_1 x_1 + F_2 x_2 + F_3 x_3$.

Здесь x_1, x_2, x_3 — это значения выходных управляемых переменных объекта управления (например, число признаков аномальных событий), значения индикаторов внешней среды, а y — допустимые значения выходных переменных, т.е. заданные входные воздействия на модуль управления, с целью выработки управляющего воздействия, направленного на объект управления (см. рис.1).

Допустим, нечеткие множества в этих правилах имеют следующие колоколообразные функции принадлежности типа:

$$\mu_{A_1}(x_1) = e^{-0,5\left(\frac{x_1 - d_1}{a_1}\right)^2}; \mu_{A_2}(x_2) = e^{-0,5\left(\frac{x_2 - d_2}{a_2}\right)^2}; \mu_{A_3}(x_3) = e^{-0,5\left(\frac{x_3 - d_3}{a_3}\right)^2}; \quad (2)$$

$$\mu_{B_1}(x_1) = e^{-0,5\left(\frac{x_1 - e_1}{b_1}\right)^2}; \mu_{B_2}(x_2) = e^{-0,5\left(\frac{x_2 - e_2}{b_2}\right)^2}; \mu_{A_3}(x_3) = e^{-0,5\left(\frac{x_3 - e_3}{b_3}\right)^2}; \quad (3)$$

$$\mu_{C_1}(x_1) = e^{-0,5\left(\frac{x_1 - f_1}{c_1}\right)^2}; \mu_{C_2}(x_2) = e^{-0,5\left(\frac{x_2 - f_2}{c_2}\right)^2}; \mu_{C_3}(x_3) = e^{-0,5\left(\frac{x_3 - f_3}{c_3}\right)^2}. \quad (4)$$

Данная сеть может быть описана следующим образом.

Слой 1. Выходы элементов этого слоя представляют собой значения функций принадлежности $\mu_{A_i}(x_i), \mu_{B_i}(x_i), \mu_{C_i}(x_i)$ при конкретных (заданных) значениях входных переменных.

Слой 2. Элементы второго слоя выполняют агрегирование степеней истинности предпосылок каждого правила базы в соответствии с операцией Т-нормы, в качестве которой здесь используется операция min-конъюнкции, по формулам:

$$\alpha_1 = min\{A_1(x_1), A_2(x_2), A_3(x_3)\}; \quad (5)$$

$$\alpha_2 = min\{B_1(x_1), B_2(x_2), B_3(x_3)\}; \quad (6)$$

$$\alpha_3 = min\{C_1(x_1), C_2(x_2), C_3(x_3)\}. \quad (7)$$

Слой 3. Элементы этого слоя выполняют нормализацию и вычисляют следующие значения:

$$\beta_1 = \frac{\alpha_1}{\alpha_1 + \alpha_2 + \alpha_3}; \quad \beta_2 = \frac{\alpha_2}{\alpha_1 + \alpha_2 + \alpha_3}; \quad \beta_3 = \frac{\alpha_3}{\alpha_1 + \alpha_2 + \alpha_3}. \quad (8)$$

Слой 4. Данный слой вычисляет значения заключений по каждому правилу:

$$y_1 = D_1 x_1 + D_2 x_2 + D_3 x_3; \quad (9)$$

$$y_2 = E_1 x_1 + E_2 x_2 + E_3 x_3; \quad (10)$$

$$y_3 = F_1 x_1 + F_2 x_2 + F_3 x_3. \quad (11)$$

Слой 5. Элемент этого слоя определяет дефаззифицированное значение на выходе сети:

$$y = \frac{\alpha_1 y_1 + \alpha_2 y_2 + \alpha_3 y_3}{\alpha_1 + \alpha_2 + \alpha_3} = \beta_1 y_1 + \beta_2 y_2 + \beta_3 y_3. \quad (12)$$

Параметры элементов первого слоя нечеткой нейронной продукционной сети a_i и b_i, c_i и d_i, e_i и f_i функций принадлежности являются настраиваемыми в ходе обучения. Если задано четкое множество примеров обучающей выборки $\{(x^k, y^k), k = 1, \ldots, K\}$, то параметры сети a_i и b_i, c_i и d_i, e_i и f_i, которые определяют форму функций принадлежности, могут быть настроены с использованием алгоритмов

обучения, например на основе градиентных методов (алгоритм обратного распространения ошибки).

Обычно применяется комбинация градиентного спуска в виде алгоритма обратного распространения ошибки и метода наименьших квадратов [6]. Алгоритм обратного распространения ошибки настраивает параметры антецендентов правил, т.е. функций принадлежности. Методом наименьших квадратов оцениваются коэффициенты заключений правил, так как они линейно связаны с выходом сети. Каждая итерация процедуры настройки выполняется в два этапа. На первом этапе на входы подается обучающая выборка и по невязке между желаемым и действительным поведением сети методом наименьших квадратов находятся оптимальные параметры оптимальные параметры узлов первого слоя. На втором этапе остаточная невязка передается с выхода сети на входы и методом обратного распространения ошибки модифицируются параметры узлов первого слоя. При этом найденные на предыдущем этапе коэффициенты заключений правил не изменяются. Итерационная процедура настройки продолжается, пока невязка превышает заранее установленное значение.

Предложенная нечеткая нейронная продукционная сеть в качестве модели интеллектуальной системы поддержки и принятия решений по управлению безопасностью объекта информатизации ОВД, по-нашему мнению, является достаточно адекватной схемой реализации механизмов управления в среде функционирования объекта. В первую очередь это подтверждается наличием в структуре модели обучаемых слоев и настраиваемых параметров нечетких множеств, что, несомненно, повышает качество управления и принятия решений в трудно формализуемых сложных процессах информационного противоборства, характерного для КАИС «Безопасный город».

Таким образом, рассмотренные правила построения модели интеллектуального управления при обеспечении безопасности таких объектов информатизации ОВД, как подсистемы КАИС «Безопасный город», подсистемы единого информационного пространства, могут быть использованы при разработке алгоритмической, математической и программной поддержки создаваемых и внедряемых в оперативно-служебную деятельность ОВД единых информационных систем и телекоммуникационной инфраструктуры.

ЛИТЕРАТУРА

1. Машкина И.В., Рахимов Е.А. Модель системы управления безопасностью объекта информатизации // Информационное противодействие угрозам терроризма. — 2006. — №6. — С. 89—92.

2. Дунин В.С. Актуальность применения интеллектуальных технологий управления при реализации некоторых положений Концепции информатизации ОВД и ВВ МВД России // Сборник XIX Международной конференции «Информатизация и информационная безопасность правоохранительных органов», посвященной 65-летию Победы в Великой Отечественной войне. — М.: Академия управления МВД России, 2010. — С. 254—257.

3. Машкина И.В., Гузаиров М.Б. Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Приложение к журналу «Информационные технологии», 2008. — №7. — С.32.

4. Штовба С.Д. Проектирование нечетких систем средствами Matlab. — М.: Горячая линия — Телеком, 2007. — 288с., ил.

5. Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети. — М.: Горячая линия — Телеком, 2007. — 284 с., ил.

6. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / пер. с польск. И.Д. Рудинского. — М.: Горячая линия — Телеком, 2008. — 452 с., ил.