ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2014. Т. 18, № 3 (64). С. 261–269 http://journal.ugatu.ac.ru

УДК 005.92:004.056

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ПРОВЕДЕНИЮ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В. В. САЛОВА[1], **В. И. ВАСИЛЬЕВ**[2]

[1] salovavv@mail.ru, [2] vasilyev@ugatu.ac.ru

ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 23 февраля 2014 г.

Аннотация. Рассмотрен подход к решению задачи автоматизации аудита информационных систем персональных данных на основе системы поддержки принятия решений с использованием технологии интеллектуального анализа данных. Предложена архитектура системы поддержки принятия решений, применение которой позволит повысить объективность принятия решений при обеспечении защиты персональных данных.

Ключевые слова: система поддержки принятия решений; аудит информационных систем персональных данных; нечеткая логика; уровень защищенности информационных систем персональных данных.

ВВЕДЕНИЕ

Персональные данные (ПДн) являются неотъемлемой частью информационных ресурсов во многих сферах деятельности общества и государства. В соответствии с требованиями федерального закона ФЗ-152 «О персональных данных», оператор обязан выполнить ряд организационных и технических мер, касающихся процессов обработки ПДн[1]. Причем обеспечение безопасности ПДн является непрерывным процессом и систему защиты необходимо поддерживать в актуальном состоянии.

Одним из важнейших компонентов непрерывного цикла процессов управления безопасностью информации является аудит. Под аудитом информационной безопасности (ИБ) понимается процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ организации в соответствии с определенными критериями и показателями безопасности[2] [1].

Выделяют три основных вида аудита ИБ: активный, экспертный и аудит на соответствие стандартам [2]. Экспертный аудит имеет ряд преимуществ над другими видами аудита: он позволяет произвести анализ организационно-распорядительной документации, учесть специфику ПДн, выполнить требования руководящих документов по защите ПДн, уменьшить стоимость и время проведения аудита.

Аудит информационных систем персональных данных (ИСПДн) позволяет руководству организации определить реальное состояние информационных активов, оценить их защищенность, провести анализ информационных рисков и, следовательно, повысить эффективность управления ИБ компании. Аудит ИСПДн имеет свою специфику. Современная нормативно-методическая база по защите ПДн недостаточно проработана и зачастую противоречива. Сложность обеспечения защиты ПДн объясняется и тем, что такие данные являются разнородными, привязанными к субъекту ПДн, их утеря может быть выявлена не сразу, а спустя некоторое время, сложно определить последствия утери ПДн. Влияние этих и многих других факторов определяет высокие требования к системе защиты ПДн. В связи с этим при аудите ИСПДн возникает неопределенность, неоднозначность принимаемых решений, связанная с оценкой защищенности ИСПДн и необходимостью учета нормативной базы.

Известны работы, посвященные защите ПДн, которые отражают основные этапы проведения аудита ИСПДн [3–5]. Вместе с тем за последнее время ФЗ-152 «О персональных данных» и связанная с ним нормативная база пре-

[1] О персональных данных: Федеральный Закон от 27 июля 2006 № 152-ФЗ.

[2] Об аудиторской деятельности: Федеральный закон от 30 декабря 2008 № 307-ФЗ.

терпели существенные изменения, которые отражены в Постановлении правительства РФ № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[3] и соответствующих документах Федеральной службы по техническому и экспортному контролю (ФСТЭК)[4]. Поэтому необходимо разработать новую методику, которая позволит оператору ПДн проводить аудит ПДн с учетом изменений в законодательстве.

В данной статье предлагается подход к построению системы поддержки принятия решений (СППР) по экспертному аудиту ПДн на предприятии, использование которой позволит автоматизировать основные этапы аудита ИСПДн с учетом их специфики, что, в свою очередь, ведет к повышению эффективности принимаемых решений по защите ПДн.

1. ТРЕБОВАНИЯ К УРОВНЮ ЗАЩИЩЕННОСТИ ИСПДн

Постановлением Правительства РФ № 1119 устанавливаются четыре уровня защищенности ИСПДн и соответствующие требования для каждого из них. Относить системы к тому или иному уровню защищенности, согласно этому документу, предлагается в зависимости от следующих критериев:

1. Категории обрабатываемых ПДн:

- специальные категории ПДн, к которым относятся ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;
- биометрические ПДн, к которым относятся сведения, характеризующие физиологические и биологические особенности субъекта, на основании которых можно установить его личность;
- общедоступные ПДн, к которым относятся ПДн, полученные только из общедоступных источников ПДн;
- иные категории ПДн, не представленные в трех предыдущих группах.

2. Форма отношений между организацией и субъектами:

- обработка ПДн сотрудников оператора;
- обработка ПДн субъектов, не являющихся сотрудниками оператора.

3. Количество обрабатываемых ПДн:

- менее 100 000 субъектов;
- более 100 000 субъектов;

4. Тип актуальных угроз:

- угрозы 1-го типа связаны с наличием недекларированных возможностей в системном программном обеспечении (ПО), используемом в ИСПДн;
- угрозы 2-го типа связаны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;
- угрозы 3-го типа не связаны с наличием недекларированных возможностей в ПО, используемом в ИСПДн.

Класс ИСПДн по уровням защищенности определяется в соответствии с табл. 1.

Таблица 1

Критерии классификации ИСПДн

Категория ПДн	Угрозы 1-го типа	Угрозы 2-го типа	Угрозы 3-го типа
Специальные ПДн	1 УЗ	1 УЗ* 2 УЗ**	2 УЗ* 3 УЗ**
Биометрические ПДн	1УЗ	2 УЗ	3 УЗ
Общедоступные ПДн	2 УЗ	2 УЗ* 3 УЗ**	4 УЗ
Иные ПДн	1 УЗ	2 УЗ* 3 УЗ**	3 УЗ* 4 УЗ**
Специальные ПДн сотрудников оператора	–	2 УЗ	3 УЗ
Общедоступные ПДн сотрудников оператора	–	3 УЗ	–
Иные ПДн сотрудников оператора	–	3 УЗ	4 УЗ

Примечание. УЗ – уровень защищенности; *если больше 100000 субъектов ПДн; ** если меньше 100000 субъектов ПДн.

В основе аудита ИБ лежит оценка факторов, определяющих уровень защищенности информации. Эти факторы отражаются в требованиях нормативной документации к уровням защищенности ИСПДн, представленных в табл. 2.

[3] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства [утверждено 2012 г.].

[4] Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных: Приказ [утвержден ФСТЭК России 2013 г.].

Таблица 2

Требования к уровням защищенности ИСПДн

Обозначение	Требования	Уровни защищенности ИСПДн			
		1	2	3	4
X_1	Режим обеспечения безопасности помещений, где обрабатываются ПДн	+	+	+	+
X_2	Сохранность носителей ПДн	+	+	+	+
X_3	Перечень лиц, допущенных к ПДн	+	+	+	+
X_4	Средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ	+	+	+	+
X_5	Должностное лицо, ответственное за обеспечение безопасности ПДн	+	+	+	-
X_6	Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
X_7	Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн	+	-	-	-
X_8	Структурное подразделение, ответственное за обеспечение безопасности ПДн	+	-	-	-

2. ТРЕБОВАНИЯ К СИСТЕМЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

СППР предназначена для оказания помощи в принятии решений на основе использования данных, документов, знаний и моделей для идентификации и решения проблем [6, 7]. В результате анализа предметной области были сформулированы следующие основные функции, которые должна выполнять СППР при аудите ПДн:

- формирование подробного описания ИСПДн, их классификация по уровням защищенности;
- формирование моделей угроз и моделей злоумышленников;
- оценка эффективности применяемых мер по защите ПДн;
- выработка рекомендаций по улучшению системы защиты ПДн.

Для определения показателей защищенности ИСПДн предлагается использование технологии интеллектуального анализа данных с помощью модульной нейронной сети (МНС). Архитектура СППР представлена на рис. 1.

Данная СППР отражает основные функции аудита ИСПДн: она позволяет построить модель угроз, классифицировать ИСПДн по уровням защищенности, определить требования к ИСПДн согласно нормативной базе и уровень соответствия защищенности ИСПДн этим требованиям. В зависимости от показателя уровня защищенности ИСПДн формируются рекомендации по повышению безопасности ПДн.

Сведения о ПДн и ИСПДн определяются на основе опросных анкет. Модуль идентификации ИСПДн определяет класс ПДн и их объем. Модуль построения модели угроз позволяет сформировать модель угроз по методике ФСТЭК[5] и определить типы угроз[6]. Модуль определения уровня защищенности ИСПДн позволяет классифицировать ИСПДн по уровням защищенности в соответствии с требованиями законодательства.

МНС представлена на рис. 2, с ее помощью производится сравнение фактического состояния ИСПДн с требуемым. На входе МНС – показатели, характеризующие класс ИСПДн и факторы $X_1 \div X_8$ для оценки уровня защищенности ИСПДн, на выходе – показатель уровня защищенности ИСПДн Y_i по требованиям i-го уровня. Данные факторы могут выражаться в количественных и качественных величинах. Модуль предварительной обработки данных об ИСПДн приводит входные величины МНС к единому масштабу.

[5] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Метод. документ [утв. ФСТЭК России 2008 г.].

[6] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Метод. документ [утв. ФСТЭК России 2008 г.].

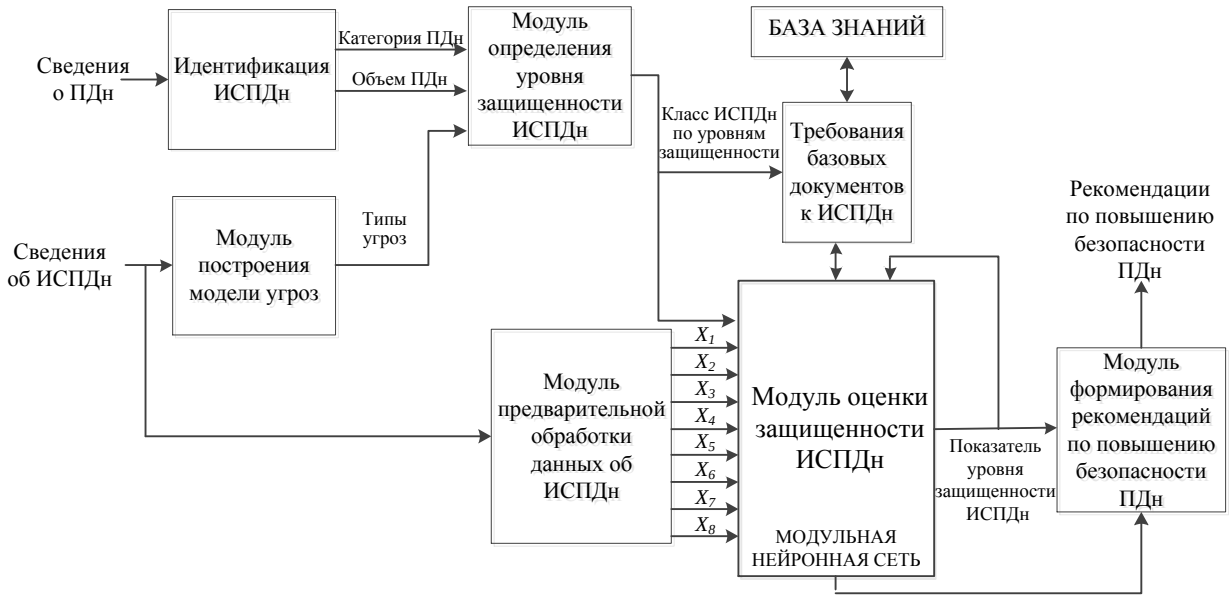

Рис. 1. Архитектура СППР

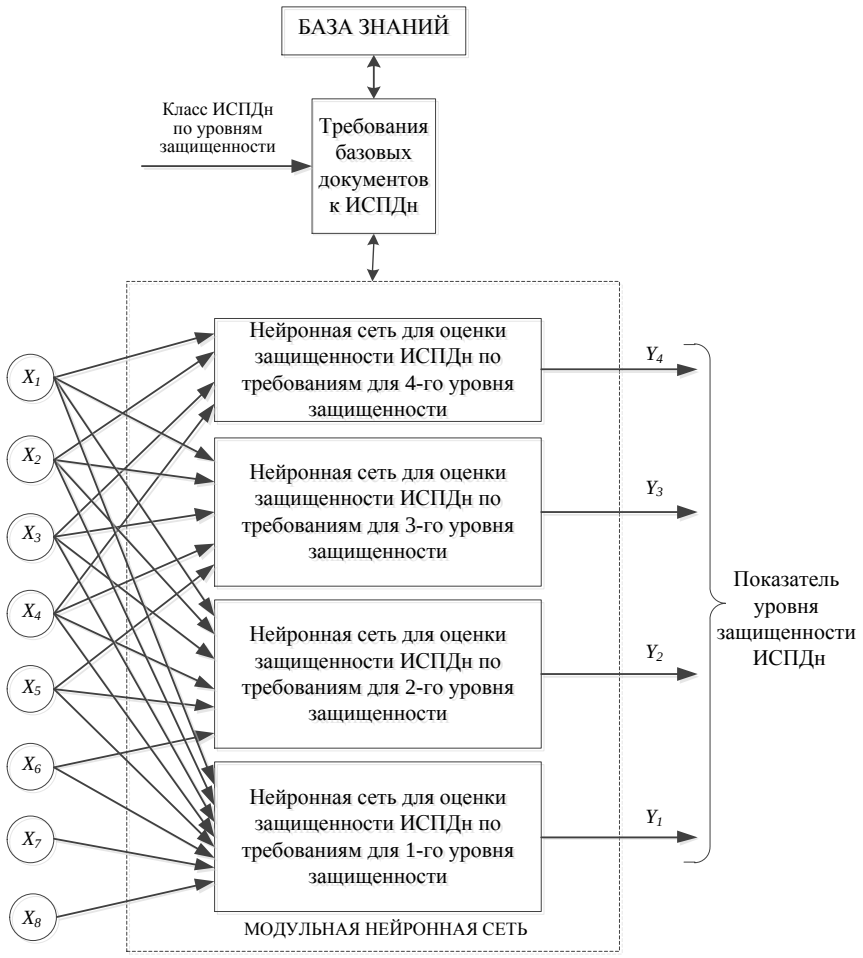

Рис. 2. Модульная структура нейронной сети

Входные факторы, в свою очередь, предлагается разделить на факторы, которые определяются однозначно и неоднозначно. Однозначно можно определить выполнение следующих факторов:

- перечень лиц, допущенных к ПДн (X_3);
- должностное лицо, ответственное за обеспечение безопасности ПДн (X_5);
- автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн (X_7);
- структурное подразделение, ответственное за обеспечение безопасности ПДн (X_8).

Для каждого из однозначно определяемых входных факторов определены два лингвистических терма; оценка производится экспертом, который устанавливает значение 1 при выполнении фактора и значение 0 – при невыполнении:

- S – «невыполнение фактора X_i»;
- L – «выполнение фактора X_i».

Для факторов X_i, значения которых не определяются однозначно (X_1, X_2, X_4, X_6), определены три лингвистических терма, оценка которых производится с помощью опросной анкеты и определяется экспертом по шкале от 0 до 1, где:

- S – [0; 0,3) – «низкий уровень показателя X_i»;
- M – [0,3; 0,9) – «средний уровень показателя X_i»;
- L – [0,9; 1] – «высокий уровень показателя X_i».

Значение результирующего (интегрального) показателя уровня защищенности ИСПДн (Y_i) определяется исходя из значений входных факторов X_1–X_8 с использованием системы правил, установленных экспертом. Для выходного параметра Y_i определены пять лингвистических термов:

- низкий уровень защищенности (S);
- уровень защищенности ниже среднего (SM);
- средний уровень защищенности (M);
- уровень защищенности выше среднего (ML);
- высокий уровень защищенности (L).

В том случае, если уровень защищенности ИСПДн не соответствует предъявляемым требованиям, СППР определяет то правило (т.е. то требование), которое не выполняется и учитывает это при формировании рекомендаций по выбору необходимых средств защиты ПДн.

3. ПОСТРОЕНИЕ СИСТЕМЫ ПРАВИЛ

В разрабатываемой СППР используется модель представления знаний в форме продукций, т.е. выходные показатели нейронной сети определяются по системе правил. Правила – это способ представления знаний предметной области, на основе которых осуществляется принятие решений в той или иной ситуации, прогнозируется развитие ситуации с учетом состояния исследуемого объекта и внешней среды [6]. При проектировании базы знаний необходимо обеспечить ее полноту и непротиворечивость.

С целью поддержки принятия решений в области проведения аудита ИСПДн выделяются правила определения уровня защищенности ИСПДн. Каждое правило R_j записывается в виде:

$$R_j: \text{Если } X_1 \text{ есть } A_1^j \text{ и } X_2 \text{ есть } A_2^j \text{ и } \ldots \ldots \text{ и } X_n \text{ есть } A_n^j, \text{то } Y_j = B_k^j, \quad (1)$$

где R_j – j-е правило (j = 1, 2, …, m); X_i – входные переменные (i = 1, 2, …, n); Y_j – выход j-го правила; A_n^j, B_k^j – нечеткие подмножества.

Рассмотрим пример построения системы правил для определения показателя уровня защищенности ИСПДн по требованиям для 4-го уровня защищенности. В данном случае показатель уровня защищенности Y согласно требованиям базовых документов зависит от четырех входных факторов $X_1 \div X_4$.

Значение выходной переменной для каждого состояния системы определяется экспертом в соответствии с нормативной документацией. Так как на входе системы одна переменная X_3, определенная двумя термами (S и L) и три переменных X_1, X_2, X_4, каждая из которых определена тремя лингвистическими переменными (S, M и L), то таблица правил содержит всего $2 \times 3^3 = 54$ правила.

Оценка показателя уровня защищенности ИСПДн производится по шкале от 0 до 1, где [0,9; 1] – высокий уровень защищенности; [0,7; 0,9) – уровень защищенности выше среднего; (0,3; 0,7) – средний уровень защищенности, (0,1; 0,3] – уровень защищенности ниже среднего; [0; 0,1] – низкий уровень защищенности.

В табл. 3 приведен фрагмент системы правил для определения показателя уровня защищенности ИСПДн.

Для оценки качества построенной нейронной сети необходимо провести ее тестирование. При построении тестирующей выборки можно воспользоваться методом Монте-Карло, который позволяет случайным образом выбрать

в указанных интервалах значения входных переменных и при помощи экспертной оценки определить соответствующие им выходные значения. В табл. 4 приведен фрагмент тестирующей выборки.

Таблица 3

Система правил для обучения нейронной сети

№	Входные факторы				Показатель уровня защищенности ИСПДн, *Y*
	X1	*X2*	*X3*	*X4*	
1.	*S*	*S*	*S*	*M*	*SM*
2.	*M*	*S*	*S*	*S*	*SM*
3.	*S*	*S*	*L*	*S*	*SM*
4.	*S*	*S*	*L*	*M*	*M*
5.	*S*	*S*	*L*	*L*	*M*
…	...	...	...	...	...
50.	*S*	*M*	*S*	*M*	*M*
51.	*S*	*M*	*S*	*L*	*M*
52.	*L*	*L*	*S*	*L*	*ML*
53.	*S*	*L*	*L*	*L*	*ML*
54.	*L*	*L*	*L*	*L*	*L*

Таблица 4

Выборка для тестирования

№	Входные факторы				Показатель уровня защищенности ИСПДн, *Y*
	X1	*X2*	*X3*	*X4*	
1	*S* *(0,15)*	*S* *(0,1)*	*S* *(0)*	*M* *(0,4)*	*SM* *(0,3)*
2	*M* *(0,3)*	*S* *(0,2)*	*S* *0)*	*S* *(0,1)*	*SM* *(0,3)*
3	*S* *(0,98)*	*M* *(0,67)*	*S* *(0)*	*M* *(0,89)*	*M* *(0,52)*
4	*L* *(1)*	*L* *(1)*	*S* *(0)*	*M* *(0,89)*	*M* *(0,63)*
5	*M* *(0,67)*	*S* *(0,17)*	*L* *(1)*	*L* *(0,99)*	*ML* *(0,73)*
…	...	...	...	...	...
14	*M* *(0.51)*	*M* *(0,67)*	*L* *(1)*	*L* *(1)*	*ML* *(0,76)*
15	*L* *(0,98)*	*L* *(1)*	*L* *(1)*	*M* *(0,87)*	*L* *(0,9)*

4. ПОСТРОЕНИЕ НЕЙРОННОЙ СЕТИ

В качестве структуры нейронной сети для вычисления показателя уровня защищенности ИСПДн по требованиям для 4-го уровня защищенности целесообразно принять нечеткую нейронную сеть, структура которой представлена на рис. 3.

Слой 1 – термы входных переменных $X_1 \div X_4$. В этом слое производится преобразование входных данных в нечеткие. На выходе узлов этого слоя – степень принадлежности значения входной переменной соответствующему нечеткому терму.

Слой 2 – антецеденты (посылки) нечетких правил. Каждый узел этого слоя соответствует одному нечеткому правилу. Данная система логического вывода имеет 54 нечетких правила. Выходом узлов этого слоя является степень выполнения правила $\mu_i(X)$, которая рассчитывается по формуле:

$$\mu_i(X) = \omega_I\left(\mu_i(x_1) \cup \mu_i(x_2) \cup \dots \mu_i(x_n)\right), \quad i = 1 \dots 54, \qquad (2)$$

где X – входной вектор; $x_1 \dots x_n$ – элементы входного вектора; ω_i – весовые коэффициенты правил.

Слой 3 – заключения правил. В этом слое узлы рассчитывают вклад соответствующего нечеткого правила в выход сети.

Слой 4 – агрегирование результата, полученного по различным правилам. Узел этого слоя суммирует вклады всех правил.

Построение нечеткой нейронной сети производится в системе MATLAB с помощью специального графического редактора адаптивных сетей ANFIS. Редактор ANFIS позволяет создавать конкретную модель адаптивной системы нейро-нечеткого вывода, выполнять ее обучение, визуализировать структуру, изменять и настраивать ее параметры, а также использовать настроенную сеть для получения результатов нечеткого вывода.

Этапы построения нечеткой нейронной сети:

- построение обучающей выборки;
- загрузка обучающих данных в редактор адаптивных сетей ANFIS;
- генерация системы нечеткого вывода [8].

На рис. 4 представлены функции принадлежности и правила, используемые для определения показателя уровня защищенности ИСПДн.

На рис. 5 представлена структура сгенерированной системы нечеткого вывода по схеме Мамдани и визуализация поверхности нечеткого вывода, которая показывает функциональную зависимость входов и выхода системы в системе координат (X_1,X_2,Y).

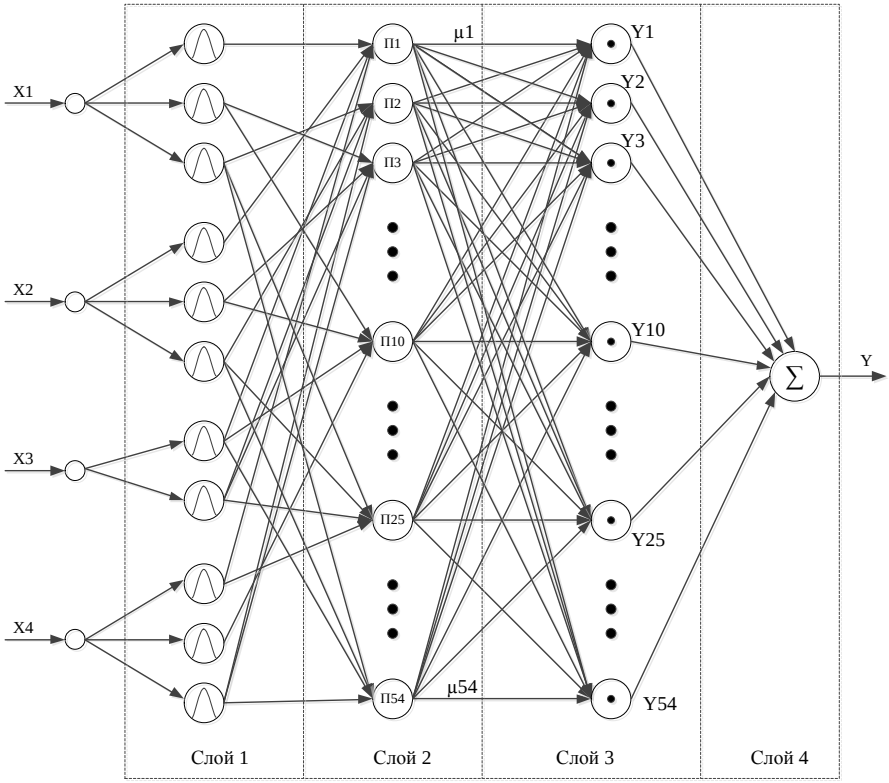

Рис. 3. Структура нечеткой нейронной сети

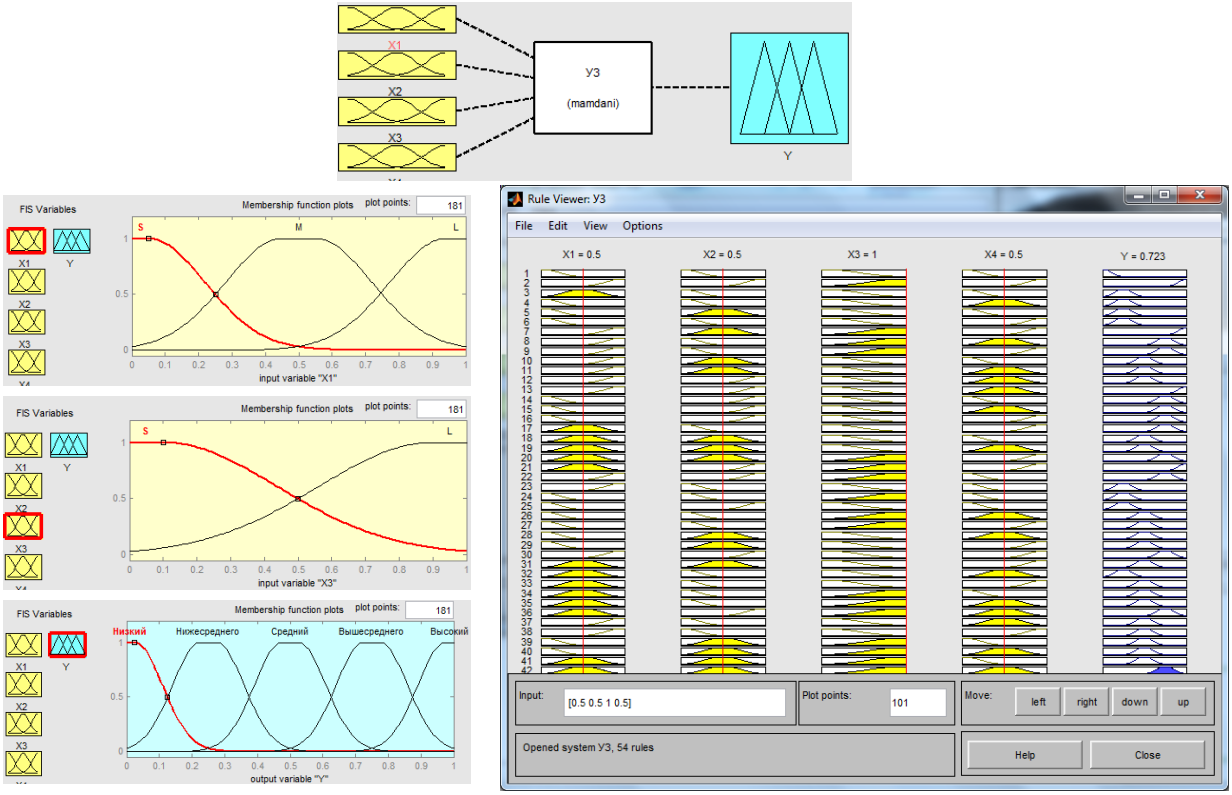

Рис. 4. Функции принадлежности и правила,
используемые для определения уровня защищенности ИСПДн

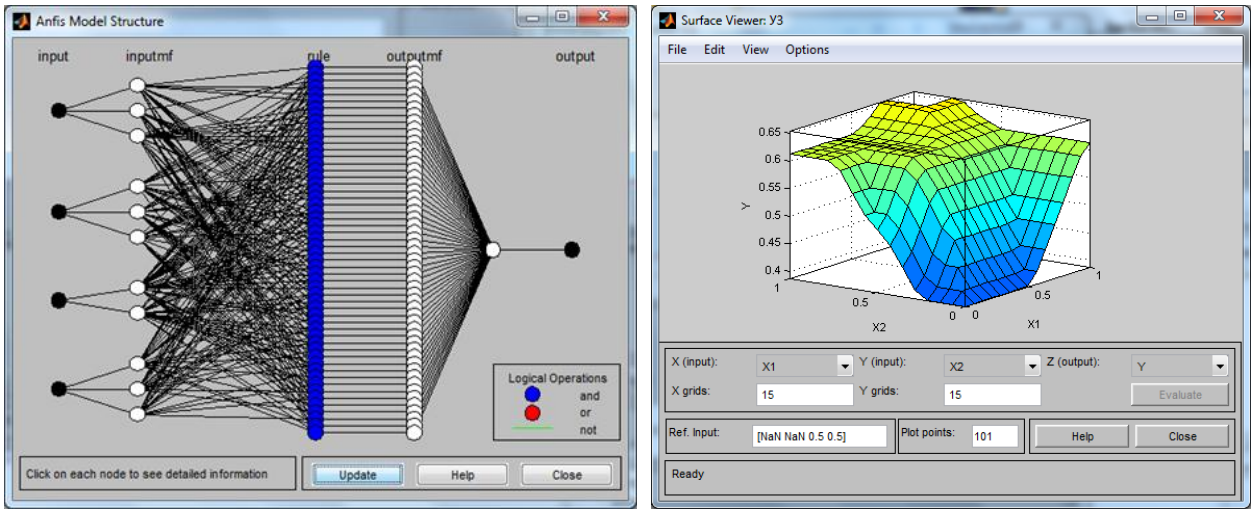

Рис. 5. Структура нейро-нечеткой сети ANFIS и визуализация поверхности нечеткого вывода

Для проверки результатов обучения используются тестовые данные. Для оценки качества построенной модели используется средняя ошибка аппроксимации $\bar{A}$, которая определяется как среднее значение относительных отклонений расчетных значений Y_i от фактических $\hat{Y}$:

$$\bar{A} = \frac{1}{n}\sum\left|\frac{Y_i - \hat{Y}}{Y_i}\right| \times 100\%. \qquad (3)$$

Для данной сети средняя ошибка аппроксимации составляет около 5%. Следовательно, качество построенной нейронной сети соответствует требованиям.

5. ПРИМЕР ПРИМЕНЕНИЯ СППР

Рассмотрим пример применения предложенной СППР по аудиту ИСПДн. Пусть ИСПДн классифицирована по 4-му уровню защищенности, входные факторы определяются экспертом на уровне следующих значений: X_1= *0,95 (L);* X_2= *1 (L);* X_3= *1 (L);* X_4= *0,7 (M).* Тогда на выходе МНС будет значение 0,8. Данное значение говорит о том, что ИСПДн на 80% соответствует требованиям базовых документов по защите ПДн и имеет уровень защищенности «выше среднего». Для формирования рекомендаций по повышению уровня защищенности ИСПДн в базе правил находится правило, которое сработало для данных входных значений, затем находится похожее правило, которое на выходе МНС выдаст высокий уровень защищенности, но с минимальным различием в позициях. В данном случае, для того чтобы МНС давала на выходе высокий уровень защищенности, необходимо увеличить значение показателя X_4 с *M* на *L*. В соответствии с этим на выходе СППР по аудиту ИСПДн выдаются рекомендации по улучшению системы защиты ПДн с указанием уделить особое внимание наиболее уязвимым направлениям по защите ИСПДн, а именно: средства защиты информации, соотвествующие требованиям законодательства по защите ПДн.

Использование предложенной интеллектуальной СППР по проведению аудита ИСПДн позволит организациям формировать модель угроз, проводить классификацию ИСПДн по уровням защищенности, определять требования нормативных документов к ИСПДн, рассчитывать показатель уровня защищенности ИСПДн, поддерживать систему защиты ПДн в актуальном состоянии, следуя рекомендациям по повышению безопасности ПДн. Повышение эффективности принимаемых решений и снижение затрат на создание и поддержание системы защиты ПДн достигается за счет автоматизации основных этапов аудита в интеллектуальной СППР.

ЗАКЛЮЧЕНИЕ

В статье рассмотрен подход к решению задачи автоматизации аудита ИСПДн на основе построения СППР с использованием технологии интеллектуального анализа данных. В ходе исследования решены следующие задачи:

- рассмотрены требования к уровню защищенности ИСПДн в соответствии с законодательством в области защиты ПДн;
- выделены основные факторы, характеризующие оценку уровня защищенности ИСПДн;
- предложена архитектура СППР по проведению аудита ИСПДн и определены требования к ней;

- рассмотрен алгоритм построения системы правил и обучающей выборки для нечеткой нейронной сети, осуществляющей вычисление показателя уровня защищенности ИСПДн с учетом требований нормативных документов к уровню защищенности ИСПДн;
- предложен алгоритм построения нечеткой нейронной сети для вычисления показателя уровня защищенности ИСПДн по требованиям для 4-го уровня защищенности;
- приведен пример применения СППР по аудиту ИСПДн.

Применение разработанной СППР по проведению аудита ИСПДн с использованием технологий интеллектуального анализа данных позволит повысить объективность принятия решений, снизить временные и материальные затраты на обеспечение защиты ПДн при их обработке в ИСПДн.

СПИСОК ЛИТЕРАТУРЫ

1. **Аудит** безопасности Intranet / С. А. Петренко, А. А. Петренко. М.: ДМК Пресс, 2002. 416 с. **[** S. A. Petrenko and A. A. Petrenko, *Audit of Intranet security*, (in Russian). Moscow: DMKPress, 2002. **]**

2. **Аудит** информационной безопасности [Электронный ресурс]. URL: http://www.sovit.net/articles/methodics/ (дата обращения 20.02.2014). **[** *Information security audit* [Online]. Available: http://www.sovit.net/articles/methodics **]**

3. **Голембиовская О. М.** Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности: автореф. дис. … канд. техн. наук. СПб., 2013. 19 с. **[** O. M. Golembiovskaya, *Automating of personal data protection means selection on the basis of their security level*, (in Russian). St. Petersburg, 2013 **]**

4. **Зеленский О. А.** Построение математической модели для анализа и оценки уровня безопасности персональных данных в информационных системах // Вестник Московского университета имени С. Ю. Витте. 2013. № 1 (2). С. 83–87. **[** O. A. Zelenskii, "Constructing of mathematical model to analyze and assess the security level for personal data in information systems," (in Russian), *Vestnik of Moscow University Named After S. Witte*, no. 1 (2), pp. 83-87, 2013. **]**

5. **Шелупанов А. А., Миронова В. Г., Ерохин С. С., Мицель А. А.** Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1 (21). С. 14–22. **[** A. A. Shelupanov, V. G. Mironova, S. S. Erohin, and A. A. Micel, "Automated system of personal data information systems survey AIST-P," (in Russian), *Reports of Tomsk State University of Control Systems and Radio Electronics*, no. 1 (21), pp. 14-22, 2010. **]**

6. **Поддержка** принятия решений при стратегическом управлении предприятием на основе инженерии знаний / Л. Р. Черняховская, Е. Б. Старцева, П. В. Муксимов, К. А. Макаров, А. И. Малахова. Уфа: АН РБ, Гилем, 2010. 128 с. **[** L. R. Chernyahovskaya, E. B. Starceva, P. V. Muksimov, K. A. Makarov, and A. I. Malahova, *Decision making support for strategic management of the company on the basis of knowledge engineering*, (in Russian), Ufa: ANRB, Gilem, 2010. **]**

7. **Васильев В. И.** Интеллектуальные системы защиты информации: учеб. пособие. 2-е изд. М.: Машиностроение, 2012. 199 с. **[** V. I. Vasilyev, *Intelligent information security systems*, (in Russian), Moscow: Mashinostroenie, 2012. **]**

8. **Ярушкина Н. Г.** Основы теории нечетких и гибридных систем: учеб. пособие. М.: Финансы и статистика, 2004. 320 с. **[** N. G. Yarushkina, *Fundamentals of the theory of fuzzy and hybrid systems*, (in Russian), Moscow: Financy i Statistika, 2004. **]**

ОБ АВТОРАХ

САЛОВА Валентина Владимировна, асп. каф. выч. техники и защ. информации. Дипл. спец. по защ. информации (УГАТУ, 2012). Готовит дис. о системах аудита информационных систем персональных данных.

ВАСИЛЬЕВ Владимир Иванович, зав. каф. выч. техники и защ. информации. Дипл. инж. по пром. электронике (УАИ, 1970). Д-р техн. наук по сист. анализу и автоматич. управлению (ЦИАМ, 1990). Иссл. в обл. многосвязн., многофункц. и интел. систем.

METADATA

Title: Intelligent decision making support system for personal data information system audit.

Authors: V. V. Salova[1], V. I. Vasilyev[2]

Affiliation: Ufa State Aviation Technical University (UGATU), Russia.

Email: vasilyev@ugatu.ac.ru.

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 18, no. 3 (64), pp. 261-269, 2014. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: A way to solve a problem of automatic audit for personal data information system based on decision making support system with intelligent data analysis technology being involved is considered. The architecture of decision making support system providing adequate decision making and personal data protection is introduced.

Key words: decision making support system; audit of personal data information system; fuzzy logic; security level for personal data information system.

About authors:

SALOVA, Valentina Vladimirovna, Postgrad. student, Dept. of Computer Engineering and Information Security. Information Security Specialist (USATU, 2012). Prepares diss. on personal data protection.

VASILYEV, Vladimir Ivanovich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer in Industrial Electronics. (USATU, 1970), Dr. of Tech. Sci. (CIAM, 1990). Invest. in multivariable, multifunctional and intelligent systems.