Раздел I. Компьютерная безопасность

УДК 005.2

В.В. Сагитова, В.И. Васильев

ИНТЕЛЛЕКТУАЛЬНАЯ ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО АУДИТУ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОСНОВЕ ПОСТРОЕНИЯ ОНТОЛОГИЙ

Рассматривается проблема аудита информационных систем персональных данных с учетом специфики персональных данных как объекта защиты. Приводится обзор основных требований к безопасности персональных данных, установленных законодательством и нормативными документами Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности. На основании обзора возможных подходов к аудиту информационной безопасности с учетом перечисленных документов, а также существующих международных и национальных стандартов в области информационной безопасности, предложен подход к решению задачи автоматизации аудита информационных систем персональных данных на основе интеллектуальной поддержки принятия решений с использованием онтологического анализа и нечеткого логического вывода. Онтологический подход позволяет систематизировать предметную область, выделить подмножество понятий и отношений между ними, которые используются для решения задач аудита информационных систем персональных данных. Онтология поддержки принятия решений по аудиту информационных систем персональных данных построена в программной системе Protégé и включает в себя метаонтологию и онтологию предметной области, содержащую понятия области информационной безопасности, понятия, характерные для предметной области защиты персональных данных, понятия из области аудита информационных систем персональных данных. Разработана встроенная в онтологию база знаний, содержащая возможные альтернативы решений по обеспечению безопасности персональных данных, составленные на основе анализа предметной области и знаний, накопленных экспертами. Предложена архитектура интеллектуальной системы поддержки принятия решений, реализуемая на базе нейронечеткой сети, применение которой позволит повысить эффективность принимаемых решений при обеспечении защиты персональных данных.

Система поддержки принятия решений; онтология; аудит; информационная система персональных данных; нечеткая логика; уровень защищенности персональных данных; оценка риска информационной системы персональных данных.

V.V. Sagitova, V.I. Vasilyev

INTELLIGENT DECISION MAKING SUPPORT FOR PERSONAL DATA INFORMATION SYSTEM AUDIT BASED ON CONSTRUCTING ONTOLOGIES

The problem of personal data information system audit taking into account the particularity personal data as a protection object is considered. The overview of basic requirements to personal data security established by laws and regulations of the Federal Service for Technical and Export Control and the Federal Security Service is considered. The approach to solving the problem of audit automatization for personal data information system based on a review of possible approaches to information security audit based on these documents and existing international and national information security standards is offered. This approach is based on the intelligent decision making support with use of ontological analysis and fuzzy logic inference. The ontological

approach allows to systematize a subject domain, to select a subset of concepts and relations between them, which are used for solving the problems of personal data information system audit. The ontology of decision support for personal data information system audit is constructed in Protégé program module. The ontology includes metaontology and subject domain ontology containing information security concepts, personal data protection concepts, personal data information system audit concepts. The built-in ontology knowledge base includes solutions alternatives to personal data security, based on subject domain analysis and experts knowledge. The architecture of intelligent decision making support system based on fuzzy neural network, application of which will allow to increase the efficiency of decision making for personal data protection, is offered.

Decision making support system; ontology; audit; personal data information system; fuzzy logic; security level for personal data; risk assessment of personal data information system.

Введение. В соответствии с федеральным законом ФЗ-152 «О персональных данных», *персональными данными* (ПДн) является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн) [1]. ПДн как объект защиты имеют свою специфику. Такие данные являются разнородными, переходящими из одной категории в другую, привязанными к конкретному субъекту ПДн, которому в случае нарушения конфиденциальности, целостности или доступности ПДн может быть нанесен значительный ущерб. Кроме того, ущерб от неправомерных действий над ПДн трудноооценим и утеря ПДн может быть выявлена не сразу, а спустя некоторое время. Вместе с тем, нормативно-методическая база по защите ПДн недостаточно проработана и зачастую противоречива. Существуют и такие препятствия, как бюджетные ограничения на обеспечение безопасности ПДн и нехватка квалифицированного персонала.

Важным компонентом создания и эксплуатации системы защиты ПДн является *аудит информационных систем персональных данных* (ИСПДн) – процесс получения объективных (качественных и количественных) оценок о текущем состоянии безопасности ИСПДн в соответствии с определенными критериями и показателями безопасности [2]. Аудит ИСПДн позволяет руководству организации определить реальное состояние информационных активов, оценить их защищенность, провести анализ информационных рисков и, следовательно, повысить эффективность управления информационной безопасностью (ИБ) компании.

Известно множество подходов к аудиту ИБ и оценке рисков, основанных на выполнении требований стандартов ИБ [3–10], но данные методы в значительной мере не учитывают собственной специфики ПДн, обуславливающей особенность проведения аудита ИСПДн, связанную с оценкой ущерба от реализации угроз и требованиями нормативной базы в области защиты ПДн. Существующие инструментальные средства проведения аудита ИСПДн либо носят исследовательский характер и их нет в открытом доступе [11–13], либо являются коммерческими, дорогостоящими и непрозрачными, т.е. непонятно, соответствуют ли они требованиям нормативных документов по защите ПДн [14]. Поэтому возникает необходимость разработки таких методик, моделей, интеллектуальных средств поддержки принятия решений, применение которых позволило бы повысить оперативность и эффективность принимаемых решений в процессе аудита ИСПДн не только с учетом специфики конкретной ИСПДн, но и с учетом появляющихся изменений в нормативно-законодательной базе, что определяет актуальность темы исследовательской работы.

В данной статье предлагается подход к построению системы поддержки принятия решений (СППР) по аудиту ИСПДн на основе построения онтологий и использования технологии интеллектуального анализа данных. Предлагаемый подход базируется на анализе рисков нарушения безопасности ИСПДн, использовании стандартов ИБ и проверке соответствия требованиям нормативных документов по защите ПДн.

Онтологический подход к построению интеллектуальной СППР по аудиту ИСПДн. *Интеллектуальная СППР* – автоматизированная система, предназначенная для оказания помощи в принятии решений на основе технологии интеллектуального анализа данных. Интеллектуальная СППР представляет собой комплекс программных инструментальных средств для анализа данных, моделирования, прогнозирования и принятия управленческих решений.

Принятие правильных и своевременных решений по защите ПДн зависит от корректности построения базы знаний СППР, содержащей возможные альтернативы решений по обеспечению защиты ПДн, составленные на основе анализа предметной области и знаний, накопленных экспертами. Поэтому задача формирования базы знаний является важнейшей задачей при разработке СППР, общая структура которой приведена на рис. 1.

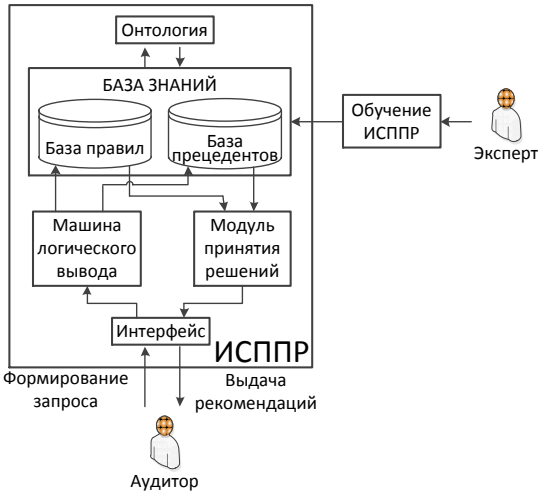

Рис. 1. Схема интеллектуальной поддержки принятия решений в процессе аудита ИСПДн

При разработке интеллектуальной СППР в процессе проведения аудита ИСПДн используются следующие модели представления знаний:

- онтологическая модель;
- продукционная модель – логический вывод решения определяется по системе правил;
- модель представления знаний о предыдущих ситуациях (база прецедентов), позволяющая учесть опыт предыдущих решений, повысить производительность работы системы.

Интеграция указанных моделей представления знаний осуществляется в рамках онтологического анализа. *Онтология* – это спецификация предметной области в виде частично упорядоченного множества понятий, отношений между ними и механизмов управления, необходимых для описания процессов решения задач в рассматриваемой предметной области. Использование онтологии позволяет систематизировать предметную область, выделить подмножество понятий, которые используются для решения поставленных задач, повысить достоверность принимаемых решений.

Поддержка решений осуществляется следующим образом. Аудитор анализирует сведения об ИСПДн и с использованием интерфейса формирует запрос к интеллектуальной СППР. Поиск решений осуществляется с использованием базы знаний, содержащей базу правил и базу прецедентов. В результате работы интеллектуальной СППР

предоставляются оценки по критериям аудита ИСПДн и выдаются рекомендации по улучшению системы защиты ПДн. Обучение интеллектуальной СППР подразумевает формирование правил на основе знаний экспертов и прецедентов принятия решений в процессе экспертного аудита ИСПДн. Таким образом, достигается необходимая степень объективности знаний интеллектуальной СППР.

Формальная онтология может быть представлена в виде кортежа

$$O = < X, R, F >, \quad (1)$$

где X – множество концептов предметной области, которую представляет онтология O; R – множество отношений между концептами заданной предметной области; F – множество функций интерпретации, заданных на концептах и отношениях онтологии. Указанные множества должны быть конечными и множество X не должно быть пустым [15].

Онтологическая модель системы позволяет описывать необходимые для ее функционирования онтологии разных уровней. Онтология поддержки принятия решений по аудиту ИСПДн включает в себя онтологию верхнего уровня (метаонтологию) O^{meta}, онтологию предметной области $O^{ПрО}$ и онтологию задач предметной области O^{Z}:

$$O = < O^{meta}, O^{ПрО}, O^{Z}, MB >, \quad (2)$$

где MB – машина вывода, ассоциированная с онтологической системой.

Метаонтология O^{meta} оперирует общими концептами и отношениями, которые не зависят от конкретной предметной области. Концептами метауровня являются такие понятия, как объект, свойство, значение, процесс, событие, алгоритм и др.

Онтология предметной области $O^{ПрО}$ определяет набор понятий, используемых при решении конкретных задач, независимых от самого метода решения. Онтология предметной области содержит знания в области обработки и защиты ПДн, необходимые для принятия решений. Концептами этого уровня являются такие понятия, как информация, ПДн, ИСПДн, уровень защищенности, угроза, уязвимость, риск и др.

Онтология задач O^{Z} имеет дело с понятиями, описывающими методы преобразования объектов предметной области в процессе решения задач. Они ориентированы на решение конкретных проблем и включают понятия, необходимые для описания процесса логического вывода.

Для программной реализации онтологии была выбрана программная система Protégé, разработанная в Стэнфордском университете (США, Калифорния). На основе нормативных документов и методик, относящихся к области защиты ПДн, построена таксономия объектов, которые были объединены в иерархию классов и занесены в создаваемую онтологию (рис. 2).

В онтологию включены базовые понятия, характерные для области ИБ, защиты ПДн, аудита ИСПДн. Фрагмент графического представления отношений между классами объектов процесса аудита ИСПДн представлен на рис. 3.

Построение системы нечеткого логического вывода. В разрабатываемой СППР используется модель представления знаний в форме продукций, т.е. нечеткий логический вывод определяется по системе правил. При проектировании базы знаний необходимо обеспечить ее полноту и непротиворечивость. Поэтому важной задачей исследования является отображение множества задач принятия решений по аудиту ИСПДн на множество правил принятия решений.

В [16] предложен метод управления знаниями, включающий совокупность операций по формированию иерархической структуры правил принятия решений в онтологии, преобразованию детерминированных правил в нечеткие, а также контролю соответствия базы нечетких правил требуемым свойствам. Данный метод был применен к задаче управления знаниями при аудите ИСПДн.

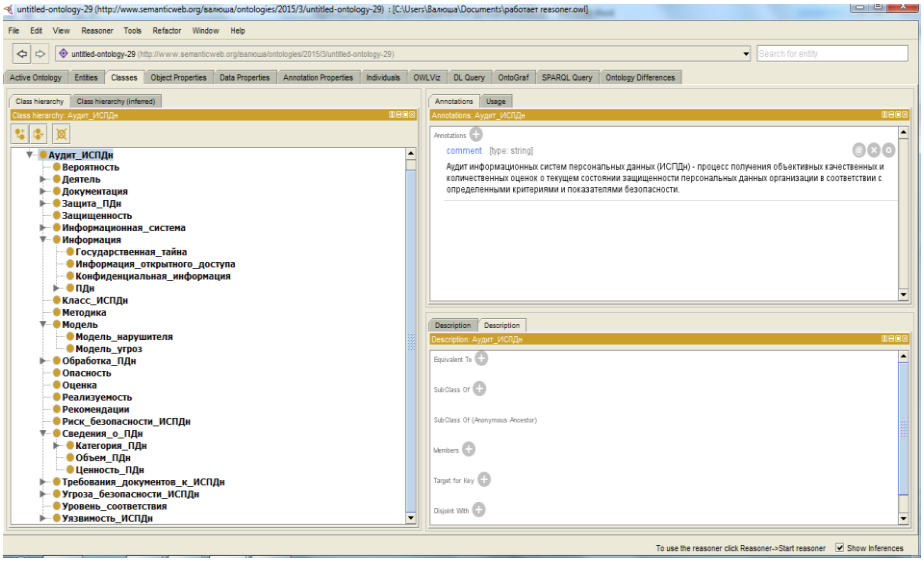

Рис. 2. Окно системы Protégé со сформированной таксономией объектов

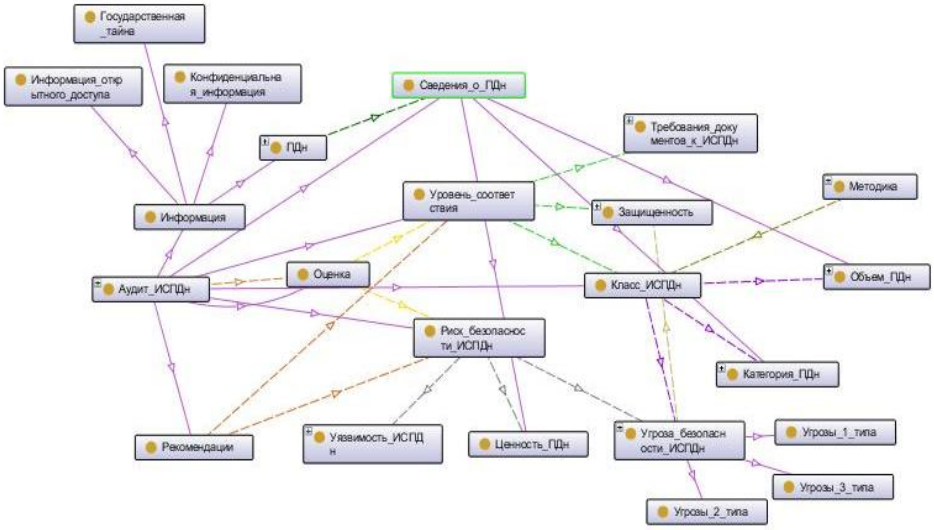

Рис. 3. Графическое представление отношений между классами объектов процесса аудита ИСПДн

На основе разработанной онтологии были сформированы правила поддержки принятия решений для отображения устойчивых причинно-следственных отношений между классами объектов, участвующих в процессе аудита ИСПДн. Разработанная база знаний является встроенной в онтологию, что позволяет накапливать и применять знания в дальнейшем.

Анализ основных задач обеспечения защиты ПДн показал, что при аудите ИСПДн часто возникает неопределенность принимаемых решений при оценке рисков безопасности ИСПДн и учете нормативной базы. В связи с этим правила принятия решений в онтологической базе знаний были расширены до нечетких правил в системе нечеткого вывода Мамдани:

$$R_j: Если\ X_1\ есть\ A_1^j\ и\ X_2\ есть\ A_2^j\ и\ ... \\ ...\ X_n\ есть\ A_n^j,\ то\ Y_j = B_k^j, \tag{3}$$

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.

В случае, когда использование базы знаний не позволяет получить решение либо правила еще не сформулированы ввиду отсутствия достаточных примеров принятия решений, применяется база прецедентов. База прецедентов представляет собой правила, описывающие специфические ситуации при принятии решений. При принятии решений по аудиту ИСПДн использование базы прецедентов позволяет адаптировать систему защиты ПДн к условиям обработки ПДн и используемым техническим средствам.

Требования к СППР по аудиту ИСПДн. В основе аудита ИСПДн лежит оценка соответствия защищенности ИСПДн базовым требованиям нормативных документов и анализ рисков безопасности ИСПДн. В результате анализа предметной области были сформулированы следующие основные функции, которые должна выполнять СППР при аудите ИСПДн:

- формирование подробного описания ИСПДн, их классификация по уровням защищенности, оценка ущерба, который понесет компания при нарушении конфиденциальности, целостности, доступности ПДн;
- формирование моделей угроз и уязвимостей;
- оценка эффективности применяемых мер по защите ПДн;
- оценка соответствия защищенности ИСПДн базовым требованиям нормативных документов;
- определение уровня риска безопасности ИСПДн;
- выработка рекомендаций по повышению безопасности ПДн.

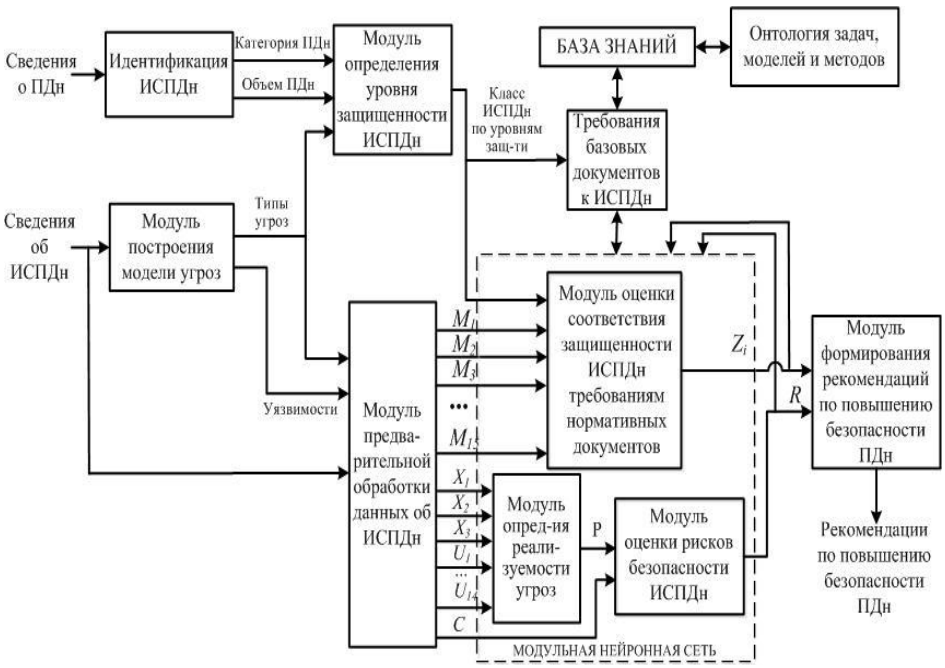

Рис. 4. Архитектура СППР по аудиту ИСПДн

Предложенная архитектура СППР по аудиту ИСПДн представлена на рис. 4. Она отражает последовательность выполнения основных функций аудита ИСПДн с учетом требований нормативных документов по защите ПДн и существующих международных и национальных стандартов в области ИБ.

Необходимые сведения о ПДн и ИСПДн определяются на основе опросных анкет. Модуль идентификации ИСПДн определяет категорию ПДн, обрабатываемых в ИСПДн, и их объем. Модуль построения модели угроз позволяет сформировать модель угроз по методике ФСТЭК [17, 18]. На данном этапе для каждого из трех типов угроз в соответствии с методическими документами ФСТЭК по защите ПДн определяются уязвимости, посредством которых возможна реализация этих угроз. Данный модуль позволяет определить исходную степень защищенности ИСПДн, уязвимости, тип угроз, их опасность и актуальность.

Модуль определения уровня защищенности ИСПДн позволяет классифицировать ИСПДн по уровням защищенности. Постановлением Правительства РФ № 1119 устанавливаются четыре уровня защищенности (УЗ) ИСПДн [19]. Относить системы к тому или иному уровню защищенности предлагается в зависимости от критериев, представленных в табл. 1.

Таблица 1

Критерии классификации ИСПДн

Категория ПДн	Тип угроз		
	1	2	3
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. *если больше 100 000 субъектов ПДн; ** если меньше 100 000 субъектов ПДн.*

На основании уровня защищенности конкретной ИСПДн, приказом ФСТЭК № 21 от 18.02.2013 г. [20] устанавливаются меры по обеспечению безопасности ПДн. В состав мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты ПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, входит 109 частных показателей M_{ij}, разбитых на 15 групповых показателей M_i, представленных в табл. 2.

Оценка частных показателей аудита ИСПДн M_{ij} основывается на свидетельствах, в качестве основных источников которых используются внутренние документы организации, относящиеся к обеспечению безопасности ПДн, опрос сотрудников, результаты наблюдений аудиторов за деятельностью сотрудников.

Для сравнения фактического состояния ИСПДн с требуемым и оценки риска безопасности ИСПДн предлагается использование технологии интеллектуального анализа данных с помощью модульной нейронечеткой сети (МНС).

Таблица 2

Групповые показатели обеспечения безопасности ИСПДн

Обозначение групповых показателей	Наименование групповых показателей безопасности ПДн
M_1	Обеспечение безопасности ПДн средствами идентификации и аутентификации субъектов и объектов доступа
M_2	Обеспечение безопасности ПДн средствами управления доступом субъектов доступа к объектам доступа
M_3	Обеспечение безопасности ПДн средствами ограничения программной среды
M_4	Обеспечение защиты машинных носителей ПДн
M_5	Обеспечение регистрации событий безопасности
M_6	Обеспечение безопасности ПДн средствами антивирусной защиты
M_7	Обеспечение безопасности ПДн средствами обнаружения вторжений
M_8	Обеспечение контроля (анализа) защищенности ПДн
M_9	Обеспечение целостности ИСПДн
M_{10}	Обеспечение доступности ПДн
M_{11}	Обеспечение защиты среды виртуализации
M_{12}	Обеспечение защиты технических средств
M_{13}	Обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных
M_{14}	Выявление инцидентов и реагирование на них
M_{15}	Управление конфигурацией ИСПДн и системы защиты ПДн

На входе МНС – показатели, характеризующие класс ИСПДн, угрозы безопасности ИСПДн $X_1 \div X_3$, уязвимости ИСПДн $U_1 \div U_{14}$, групповые показатели обеспечения безопасности ИСПДн M_i, ценность ПДн C, на выходе – показатели уровня соответствия защищенности ИСПДн требованиям нормативных документов Z_i и уровня риска безопасности ИСПДн R. В процессе оценки риска МНС сначала определяет вероятность реализации угроз каждого типа $P_1 \div P_3$, а затем уровень риска безопасности ИСПДн R. В качестве структуры нейронной сети была принята нечеткая нейронная сеть. Входные факторы МНС могут выражаться в количественных и качественных (полученных путем экспертной оценки) величинах. Модуль предварительной обработки данных об ИСПДн приводит входные величины к единому масштабу.

После оценки риска безопасности ИСПДн необходимо выполнить обработку риска. Существует четыре варианта обработки риска: снижение риска, принятие риска, предотвращение риска и перенос риска. В том случае, если уровень защищенности ИСПДн или уровень риска безопасности ИСПДн не соответствует предъявляемым требованиям, СППР определяет по базе правил причину такого состояния системы и формирует рекомендации по выбору необходимых средств защиты с учетом того, что стоимость контрмер не должна превышать допустимых значений, иначе теряется суть оценивания и управления рисками безопасности ИСПДн.

На основе проведенного анализа была произведена реализация прототипа интеллектуальной СППР по аудиту ИСПДн. На основе нечетких правил построены нечеткие нейронные сети, позволяющие определить уровнь соответствия защищенности ИСПДн требованиям нормативных документов, вероятность реализации угроз 1-го, 2-го, 3-го типов и уровень риска безопасности ИСПДн. Риск безопасности ИСПДн R при этом зависит от входных факторов: вероятность реа-

лизации угроз *P* и ценность ПДн *C*. Значение выходной переменной *R* нейронной сети определяется по системе правил нечеткого логического вывода. Построение сети производится в системе MATLAB с помощью графического редактора адаптивных сетей ANFIS.

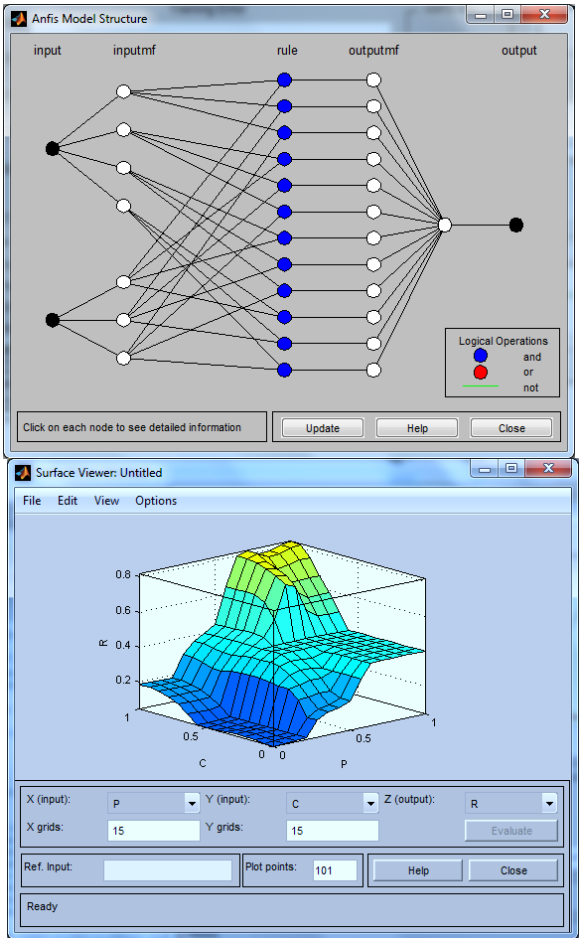

Рис. 5. Структура сети ANFIS и визуализация поверхности нечеткого вывода

На рис. 5 представлена структура нейронечеткой сети и визуализация поверхности нечеткого вывода, иллюстрирующая функциональную зависимость входных и выходной переменных $R = f(P, C)$ системы нечеткого логического вывода.

Заключение. Рассмотрен подход к решению задачи автоматизации аудита ИСПДн на основе построения СППР с использованием онтологического анализа и формированием нечеткого логического вывода. В ходе исследования решены следующие задачи:

- определена специфика ПДн как объекта защиты;
- предложена модель представления знаний в области защиты ПДн на основе использования онтологий;
- предложен метод управления знаниями интеллектуальной СППР в процессе аудита ИСПДн с учетом требований базовых документов по защите ПДн;

- предложена архитектура СППР по проведению аудита ИСПДн и определены требования к ней;
- приведен пример реализации нечеткой нейронной сети для определения уровня риска безопасности ИСПДн.

Новизна предлагаемого подхода заключается:

- в разработке модели представления знаний в области защиты ПДн, отличающейся использованием онтологий, позволяющей формализовать процесс аудита ИСПДн;
- в построении СППР, включающей оценку уровня соответствия защищенности ИСПДн требованиям нормативных документов и оценку рисков безопасности ИСПДн и отличиющейся использованием интеллектуальных технологий обработки данных, что позволяет формировать и в значительной степени автоматизировать процесс аудита ИСПДн с учетом вляиния факторов неопределенности однозначности принятия решений.

Использование предложенной СППР позволит повысить эффективность принятия решений по защите ПДн.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. О персональных данных: Федер. закон: принят Гос. Думой 8 июля 2006 г. – М.: Российская газета, 2006. – 21 с.
2. *Лихоносов А., Денисов Д.* Основы аудита информационной безопасности: учебное пособие. – М.: МФПА, 2010. – 305 с.
3. *Салова В.В.* Анализ методов оценки риска в информационных системах персональных данных // Материалы Восьмой Всероссийской зимней школы-семинара аспирантов и молодых ученых «Информационные и инфокоммуникационные технологии». – Уфа, 2013. – С. 289-292.
4. *Sheela S., Rajasundari T.* Information Flow Analysis Based On Security Metrics // International Journal of Innovative Research in Science, Engineering and Technology. – March 2014. – Vol. 3, Special Issue 3. – P. 2264-2269.
5. CMS Information Security Risk Assessment (is RA) Procedure (Centers for Medicare & Medicaid Services), March 19, 2009.
6. Security Risk Assessment & Audit Guidelines [G51] (The Government of the Hong Kong Special Administrative Region), Version 5.0, September, 2012.
7. Practical Methods for Information Security Risk Management // Informatica Economică. – 2011. – Vol. 15, No. 1. – P. 151-159.
8. Risk Assessment Process: Information Security (New Zealand Government), February, 2014.
9. *Behnia A, Rashid R.A., Chaudhry J.A.* A Survey of Information Security Risk Analysis Methods // Smart Computing Review. – February, 2012. – Vol. 2, No. 1.
10. *Breier J., Hudec L.* Risk analysis supported by information security metrics // Proc. of the 12th International Conference on Computer Systems and Technologies, 2011.
11. *Голембиовская О.М.* Автоматизация выбора средств защиты персональных данных на основе анализа их защищенности: автореф. дисс. … канд. техн. наук. – СПб., 2013. – 19 с.
12. *Куракин А.С.* Методы и алгоритмы построения информационных систем персональных данных в защищенном исполнении: Автореф. дисс. … канд. техн. наук. – СПб., 2013. – 33 с.
13. *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.
14. Б-152. URL: http://b-152.ru (дата обращения 17.02.2015).
15. *Болотова Л.С.* Системы искусственного интеллекта: модели и технологии, основанные на знаниях. – М.: Финансы и статистика, 2012. – 664 с.
16. *Черняховская Л.Р., Старцева Е.Б., Муксимов П.В. и др.* Поддержка принятия решений при стратегическом управлении предприятием на основе инженерии знаний. – Уфа: АН РБ, Гилем, 2010. – 128 с.

17. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Метод. документ: утвержден ФСТЭК России 14 февр. 2008 г. – URL: http://fstec.ru/ component/attachments (дата обращения 17.02.2015).
18. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Метод. документ: утвержден ФСТЭК России 15 февр. 2008 г. – URL: http://www.zki.infosec.ru (дата обращения 17.02.2015).
19. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ: утверждено 1 нояб. 2012 г. – М.: Российская газета, 2012. – 7 с.
20. 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 18 февр. 2013 г. – М.: Российская газета, 2013. – 8 с.

REFERENCES

1. O personal'nykh dannykh [On personal data]: *Feder. Zakon: prinyat Gos. Dumoy 8 iyulya 2006 g.* [Federal law: passed by the State Duma on July 8, 2006]. Moscow: Rossiyskaya gazeta, 2006, 21 p.
2. *Likhonosov A., Denisov D.* Osnovy audita informatsionnoy bezopasnosti: Uchebnoe posobie [The fundamentals of auditing information security: a Training manual]. Moscow: MFPA, 2010, 305 p.
3. *Salova V.V.* Analiz metodov otsenki riska v informatsionnykh sistemakh personal'nykh dannykh [Analysis of methods of risk assessment in information systems of personal data], *Materialy Vos'moy Vserossiyskoy zimney shkoly-seminara aspirantov i molodykh uchenykh «Informatsionnye i infokommunikatsionnye tekhnologii»* [The materials of the Eighth all-Russia winter school-seminar of graduate students and young scientists "Information and communication technologies"]. Ufa, 2013, pp. 289-292.
4. *Sheela S., Rajasundari T.* Information Flow Analysis Based On Security Metrics, *International Journal of Innovative Research in Science, Engineering and Technology*, March 2014, Vol. 3, Special Issue 3, pp. 2264-2269.
5. CMS Information Security Risk Assessment (is RA) Procedure (Centers for Medicare & Medicaid Services), March 19, 2009.
6. Security Risk Assessment & Audit Guidelines [G51] (The Government of the Hong Kong Special Administrative Region), Version 5.0, September, 2012.
7. Practical Methods for Information Security Risk Management, *Informatica Economică,* 2011, Vol. 15, No. 1, pp. 151-159.
8. Risk Assessment Process: Information Security (New Zealand Government), February, 2014.
9. *Behnia A, Rashid R.A., Chaudhry J.A.* A Survey of Information Security Risk Analysis Methods, *Smart Computing Review*, February, 2012, Vol. 2, No. 1.
10. *Breier J., Hudec L.* Risk analysis supported by information security metrics, *Proc. of the 12th International Conference on Computer Systems and Technologies, 2011.*
11. *Golembiovskaya O.M.* Avtomatizatsiya vybora sredstv zashchity personal'nykh dannykh na osnove analiza ikh zashchishchennosti: Avtoref. diss. … kand. tekhn. nauk [Automating the choice of protection of personal data based on the analysis of their security: Autoabstract cand. eng. sc. diss]. St. Petersburg, 2013, 19 p.
12. *Kurakin A.S.* Metody i algoritmy postroeniya informatsionnykh sistem personal'nykh dannykh v zashchishchennom ispolnenii: Avtoref. diss. … kand. tekhn. nauk [Methods and algorithms of information systems of personal data in a secure execution: Autoabstract cand. eng. sc. diss.]. St. Petersburg, 2013, 33 p.
13. *Shelupanov A.A., Mironova V.G., Erokhin S.S., Mitsel' A.A.* Avtomatizirovannaya sistema predproektnogo obsledovaniya informatsionnoy sistemy personal'nykh dannykh «AIST-P» [Automated system of pre-survey information systems of personal data "STORK-P", *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk state University of control systems and Radioelectronics], 2010, No. 1 (21), pp. 14-22.
14. B-152. Available at: http://b-152.ru (accessed 17 February 2015).

15. *Bolotova L.S.* Sistemy iskusstvennogo intellekta: modeli i tekhnologii, osnovannye na znaniyakh [Artificial intelligence systems: models and technologies based on knowledge]. Moscow: Finansy i statistika, 2012, 664 p.
16. *Chernyakhovskaya L.R., Startseva E.B., Muksimov P.V. i dr.* Podderzhka prinyatiya resheniy pri strategicheskom upravlenii predpriyatiem na osnove inzhenerii znaniy [The decision support in strategic management of enterprise-based knowledge engineering]. Ufa: AN RB, Gilem, 2010, 128 p.
17. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Metod. dokument: utverzhden FSTEK Rossii 14 fevr. 2008 g. [The method of determining actual threats to the security of personal data during their processing in personal data information systems: a Methodological document: approved by the Russian FSTEC 14 Febr. 2008]. Available at: http://fstec.ru/component/attachments (accessed 17 February 2015).
18. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Metod. dokument: utverzhden FSTEK Rossii 15 fevr. 2008 g. [The basic model of threats to the security of personal data at their processing in information systems of personal data: Method. document: approved by the FSTEC of Russia 15 Feb. 2008]. Available at: http://www.zki.infosec.ru (accessed 17 February 2015).
19. Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh: Postanovlenie Pravitel'stva RF: utverzhdeno 1 noyab. 2012 g. [About approval of requirements to protection of personal data during their processing in personal data information systems: regulation of the Government of the Russian Federation: approved 1 Nov. 2012]. Moscow: Rossiyskaya gazeta, 2012, 7 p.
20. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnoy sisteme personal'nykh dannykh: Prikaz: utverzhden FSTEK Rossii 18 fevr. 2013 g [On approval of the composition and content of organizational and technical measures for personal data security at their processing within the information system of personal data: the Order: approved by the Russian FSTEC 18 Feb. 2013]. Moscow: Rossiyskaya gazeta, 2013, 8 p.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

Сагитова Валентина Владимировна – ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ); e-mail: sagitovavv@mail.ru; 450092, Республика Башкортостан, г. Уфа, ул. Батырская, 18, кв. 134; тел.: +79177603537; кафедра вычислительной техники и защиты информации; аспирант.

Васильев Владимир Иванович – e-mail: vasilyev@ugatu.ac.ru; 450000, Республика Башкортостан, г. Уфа, ул. Карла Маркса, 12; кафедра вычислительной техники и защиты информации; зав. кафедрой; д.т.н.; профессор.

Sagitova Valentina Vladimirovna – Ufa State Aviation Technical University (UGATU); e-mail: sagitovavv@mail.ru; 18, Butyrskaya street, ap. 134, Ufa, Republic of Bashkortostan, 450092, Russia; phone: +79177603537; the department of computer engineering and information security; postgraduate student.

Vasilyev Vladimir Ivanovich – e-mail: vasilyev@ugatu.ac.ru; 12, Karla Marksa street, Ufa, Republic of Bashkortostan, 450000, Russia; the department of computer engineering and information security; dr. of eng. sc.; professor.