Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.04.04 – Программная инженерия
Направленность (профиль) образовательной программы Управление разработкой программного обеспечения

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2019 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему: Проектирование и реализация системы поддержки принятия решений по проведению аудита информационных систем персональных данных

Исполнитель студент группы 757ом	_____ (подпись, дата)	А.В. Дмитриева
Руководитель доцент, канд. техн. наук	_____ (подпись, дата)	С.Г. Самохвалова
Руководитель научного содержания программы магистратуры профессор, док. техн. наук	_____ (подпись, дата)	И.Е. Еремин
Нормоконтроль Инженер кафедры	_____ (подпись, дата)	В.Н. Адаменко
Рецензент Ген.директор Интернет-маркетинга Z-labs	_____ (подпись, дата)	И.С. Вирта
Рецензент Зам.директора по ИТ ГБУЗ АО АМИАЦ	_____ (подпись, дата)	Д.С. Щербань

Благовещенск 2019

Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав.кафедрой
_____А.В.Бушманов
«_____»_____2019 г.

З**АДАНИЕ**

К выпускной квалификационной работе студента Дмитриевой Анастасии Витальевны

1. Тема выпускной квалификационной работы: Проектирование и реализация системы поддержки принятия решений по проведению аудита информационных систем персональных данных (утверждено приказом от _____ № _____)

2. Срок сдачи студентом законченной работы _____г.

3. Исходные данные к выпускной квалификационной работе: предметная область, нормативно-правовая документация, перечень литературы

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов):

– анализ предметной области;

– проектирование системы поддержки принятия решений;

– описание реализации программного средства.

5. Перечень материалов приложения (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.):

– классификация информационных систем по уровням защищённости;

– требования к уровням защищённости;

– схема реализации программных модулей;

– база правил для нечёткой нейронной сети;

– обучающая выборка для нечёткой нейронной сети;

– техническое задание на проектирование.

6. Дата выдачи задания _____г.

Руководитель выпускной квалификационной работы: Самохвалова С.Г., доцент, канд. техн. наук

Задание принял к исполнению (_____г.): _____

(подпись студента)

РЕФЕРАТ

Выпускная квалификационная работа содержит 97 страниц, 34 рисунка, 3 таблицы, 59 источников.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ, УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ЖИЗНЕННЫЙ ЦИКЛ, СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ, НЕЧЁТКАЯ ЛОГИКА, НЕЧЁТКАЯ НЕЙРОННАЯ СЕТЬ

В выпускной квалификационной работе ставится задача исследования процесса аудита информационной безопасности, в частности анализ информационных систем персональных данных. Приводится и рассматривается понятие жизненного цикла программных средств, а также модели жизненного цикла, выбор и обоснование которой представлены в работе.

В работе также идёт рассмотрение процесса проектирования системы, которое описывается методологией UML и представляет собой функциональные модели, различные модели процессов, последовательностей, состояний и активностей.

В разделе описания реализации приводится описание интерфейса программного средства на языке C#, а также рассматривается процесс интеллектуального анализа данных, представленного нечёткой нейронной сетью, базирующейся на теории нечёткой логики.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

ТС – техническое средство;

ПЭМИН – побочные электромагнитные излучения и наводки; ИС – информационная система; ПДн – персональные данные;

ИСПДн – информационная система персональных данных;

АС – автоматизированная система;

АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;

ТКУИ – технические каналы утечки информации;

НСД – несанкционированный доступ;

ЭВМ – электронно-вычислительная машина;

ВС – вычислительная система;

ЗИ – защита информации;

ЖЦ – жизненный цикл;

UML – Unified Modeling Language (унифицированный язык моделирования);

СППР – система поддержки принятия решений;

ИИ – искусственный интеллект;

УЗ – уровень защищённости;

НДВ – недекларированные возможности;

ОС – операционная система;

ПО – программное обеспечение;

FIS – Fuzzy Inference System (система нечёткого вывода);

ANFIS – Adaptive Neuro-Fuzzy Inference System (адаптивная система нейро-нечёткого вывода).

ВВЕДЕНИЕ

Проблема обеспечения информационной безопасности является довольно актуальной в современном мире. Сейчас трудно себе представить жизнь без использования информационных технологий, информационных ресурсов и процессов их обработки. Их защита является наиболее важной задачей, к которой необходимо подходить разумно и рационально.

Существует множество различных механизмов обеспечения информационной безопасности. Одним из таких механизмов является процесс аудита информационной безопасности. Он создан для проведения анализа существующих уязвимостей, слабых мест в системе защиты, а также процесс аудита подразумевает определение возможных путей решений при возникающих проблемах.

Отдельной составляющей процесса проведения аудита информационной безопасности можно выделить аудит информационных систем персональных данных, представляющий собой анализ информационных систем в соответствии с нормативно-правовой документацией, регулирующей отношения в области обработки персональных данных. Не всегда данных о предметной области бывает достаточно, а нормативно-правовая документация не даёт полный перечень мероприятий по обеспечению состояния защищённости информационных систем. В таком случае в помощь аудитору при составлении экспертной оценки может помочь система поддержки принятия решений.

Целью выпускной квалификационной работы является создание системы поддержки принятия решений, предназначенной для осуществления функций аудита информационных систем персональных данных. В результате разработки системы должны разрешаться следующие поставленные задачи:

– возможность описания информационной системы персональных данных и определение уровня её защищённости по исследуемым входным показателям;

– оценка уровня защищённости информационной системы персональных данных в зависимости от предъявляемых к ней требований, в соответствии с нормативной документацией;
– помощь аудитору в формировании рекомендаций о состоянии защищённости информационной системы.

Научная новизна основных результатов работы состоит в применении механизма нечётких нейронных сетей, базирующихся на теории нечёткой логики, при составлении оценки уровня защищённости информационной системы персональных данных.

Практическая значимость проводимого научного исследования определяется возможностью осуществлять анализ любой информационной системы персональных данных в зависимости от её уровня защищённости.

Результаты научных исследований для написания магистерской диссертации были представлены в качестве публикаций в научных журналах и тезисах для выступления на конференции [17–19].

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Данный раздел рассматривает предметную область выпускной квалификационной работы. Здесь приведены основные понятия процесса аудита информационной безопасности, модели угроз и рисков. Пункт нормативно-правовой документации разбирает основные законы, постановления, приказы в области обработки персональных данных. Помимо этого в данном разделе рассматриваются, анализируются и сравниваются программные средства, решающие основные задачи информационной безопасности. Далее в разделе приводится понятие нечётких нейросетей и особенностей их применения в процессе аудита информационной безопасности. Важным пунктом также следует отметить понятие жизненного цикла и обоснование конкретной модели жизненного цикла. Последний пункт данного раздела рассматривает обоснование и выбор инструментальных и программных средств для построения системы поддержки принятия решений.

1.1 Процесс аудита информационной безопасности

В настоящее время проблема сохранности информационных ресурсов является одной из наиболее актуальных задач. Информационные ресурсы всегда являлись наиболее ценными среди прочих, а обеспечение их защиты предполагало применение серьёзных и эффективных с точки зрения качества и целесообразности контрмер. Комплекс мероприятий, технологий и методического обеспечения лёг в основу понятия информационной безопасности. С каждым годом информационные системы, осуществляющие основные процессы обработки, передачи и хранения информационных ресурсов, совершенствуются. А это значит, что проблема совершенствования обеспечения защиты данных ресурсов остро встаёт перед пользователями. Помимо этого информационная безопасность конкретной организации, предприятия должна быть строго регламентирована в соответствии с нормативно-правовой документацией. Нередко возникают ситуации, когда нормативно-правовых документов оказывается не-

достаточно, чтобы обеспечить полную защиту. Тогда речь идёт о возможности принятия экспертных решений, чтобы по возможности минимизировать возникающие проблемы, связанные с нехваткой данных о проблемной области.

Одним из методов обеспечения информационной безопасности выделают аудит ИБ. Аудит предполагает процесс получения количественных и качественных оценок о состоянии информационных ресурсов для конкретной организации, предприятия или компании в соответствии с приведёнными показателями безопасности, отражёнными в нормативно-правовых актах [38, 39]. Также аудит информационной безопасности служит для выявления оценки состояния защищённости информационных ресурсов, хранящихся в информационной системе, и соответственной выработки рекомендаций по применению организационных мер, а также программных и технических средств, направленных на обеспечение информационной безопасности и защиту от возникающих угроз ИБ [1].

Таким образом, выявляются следующие цели и задачи процесса проведения аудита информационной безопасности:

– обнаружение вероятных рисков, а вместе с тем и связанных с ними источников угроз по отношению к хранящимся в информационных системах ценным информационным ресурсам;

– определение оценки уровня защищённости информационной системы, по которому исследуемая ИС классифицируется;

– выявление оценки соответствия состояния защищённости системы требованиям к ИБ, рассматриваемым в нормативно-правовых актах;

– поиск и обнаружение возможных уязвимостей в системе обеспечения информационной безопасности;

– создание на основании полученных результатов рекомендаций по совершенствованию состояния защищённости исследуемой ИС.

В соответствии с вышеприведёнными задачами предлагается спроектировать и реализовать СППР, оказывающую помощь эксперту в проведении аудита информационной безопасности.

Помимо вышеперечисленных целей аудита ИБ, можно выделить разработку политик безопасности и прочей организационно-распорядительной документации по ЗИ, также формирование и постановку задач для персонала организации по обеспечению защиты информации, проведение обучения пользователей, обслуживающего персонала информационных систем в вопросах ИБ, принятие участия в разрешении конфликтов и инцидентов, связанных с нарушением ИБ.

Информационная безопасность представляет собой состояние сохранности информационных ресурсов, а также защищённости прав личности и общества в сфере информации [58].

Можно выделить следующие основные направления аудита информационной безопасности:

– аттестация объектов информатизации в соответствии с текущими требованиями ИБ;

– обеспечение контроля защищённости информации, имеющей ограниченный доступ;

– специализированные исследования ТС на наличие в них ПЭМИН;

– проектирование и создание объектов в защищённом исполнении.

Направление аттестации объектов информатизации подразумевает выполнение следующих задач:

– проведение аттестации АС, средств связи, а также передачи и обработки информации;

– аттестация помещений, где могут проводиться переговоры и озвучиваться конфиденциальная информация;

– аттестация ТС в выделенных помещениях.

Направление обеспечения контроля защищённости информации ограниченного доступа имеет следующие задачи:

– выявление ТКУИ и способы НСД к ней;

– контроль эффективности используемых средств защиты информации;

Направление специализированных исследований технических средств подразумевает выполнение следующих задач:

– анализ персональных ЭВМ, а также средств связи, обработки и передачи информации;

– локальные ВС;

– оформление результатов исследований в соответствии с нормативно-правовой документацией;

Направление проектирования и создания объектов в защищённом исполнении решает следующие задачи:

– разработка концепции ИБ;

– проектирование и создание АС, средств связи, обработки и передачи информации;

– проектирование помещений, где распространяется конфиденциальная информация.

Различают внешний и внутренний аудит. Первый подразумевает разовое мероприятие, инициатором которого, как правило, выступают руководители предприятия. Данный вид аудита требуется проводить регулярно.

Внутренний аудит, как правило, непрерывное мероприятие. Инициируется также руководством предприятия, но в соответствии с внутренним документом организации – «Положение о внутреннем аудите».

Процесс аудита информационной безопасности проходит по следующим этапам:

– 1-й этап – осуществление инициирования процесса аудита;

– 2-й этап – сбор первичной информации для аудита;

– 3-й этап – анализирование данных процесса аудита;

– 4-й этап – выработка рекомендаций;

– 5-й этап – составление аудиторского отчёта.

Первый этап начинается с решения следующих организаторских вопросов:

– все права и обязанности аудитора чётко определяются в его должностных инструкциях и положении о внутреннем аудите;

– аудитор инициирует составление подробного и согласованного с руководством плана по проведению аудита;

– сотрудники организации обязаны содействовать процессу проведения аудита и предоставлять для него всю необходимую информацию.

На данном этапе определяются и обосновываются границы проводимого обследования. Всё должно быть согласовано и обсуждено между аудиторами, руководством самой организации, а также её структурных подразделений.

Следующий этап сбора информации является наиболее трудоёмким и длительным. На данном этапе аудитору необходимо плотно взаимодействовать с сотрудниками организации, чтобы пополнить базу входных данных для будущего обследования. Необходимо проанализировать организационную структуру предприятия, а также всех её обслуживающих подразделений. Далее изучается общий функционал информационной системы, основные принципы её работы, определяются возможные риски и требования к её безопасности.

После сбора информации осуществляется её анализ. Методы анализа данных подразделяются на следующие:

– первый основывается на анализе рисков. Он является самым сложным, так как предполагает составление индивидуального и специфического набора требований безопасности. Здесь берутся в учёт особенности конкретной, среды функционирования ИС и существующие для неё угрозы;

– второй базируется на стандартах информационной безопасности. Они предполагают первичный, базовый набор требований к безопасности в соответствии уровнем защищённости ИС.

– третий является комбинацией первых двух подходов. За основу берутся существующие стандарты, которые по возможности дополняются другими требованиями, индивидуальными для каждой исследуемой ИС, на основе анализа рисков.

Следующий этап проведения процесса аудита – формирование рекомендаций. Рекомендации должны быть исчерпывающими, полными, экономически обоснованными, с разумной степенью детализации, применимыми к конкретной информационной системе.

Последний этап – аудиторский отчёт. Это результат проведения процесса аудита. В нём должны быть отражены такие пункты как: характеристика исследуемой информационной системы, описание используемого метода анализа информации, результаты проведённого анализа, выявленные недостатки в системе защиты, а также конкретные рекомендации аудитора по их устранению и усовершенствованию показателей защищённости ИС [5, 46].

1.2 Модель угроз информационной безопасности

Под угрозой безопасности понимается такая возможность воздействия на ИС, которая прямо или косвенно может нанести ущерб её состоянию безопасности. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты [54, 24].

Существует три основных типа угроз: угрозы, обусловленные действиями субъекта (антропогенные); угрозы, реализуемые техническими средствами (техногенные); угрозы, вызванные стихийными, погодными источниками [8].

Чтобы выбрать те или иные средства защиты, необходимо проанализировать как источники угроз, так и условия их реализации.

К антропогенным источникам угроз можно отнести следующие угрозы:

а) внешние:

1) криминальные структуры и группировки;

2) представители надзорных организаций и аварийных служб;

3) лица, заинтересованные в получении конфиденциальных сведений, но не имеющие прямого отношения к объекту защиты;

б) внутренние:

1) основной персонал организации;

2) представители службы безопасности;

3) вспомогательный персонал (уборщики).

К техногенным источникам угроз относятся следующие:

– некачественные основные ТС;

– некачественное периферийное оборудование;

– некачественная поддерживающая инфраструктура.

Естественные источники угроз следующие:

– землетрясения;

– пожары;

– наводнения;

– радиоактивное излучение;

– стихийные явления;

– различного рода форс-мажорные обстоятельства.

Условия реализации угроз, как правило, составляют возможные каналы утечки информации:

– оптико-визуальный;

– акустический;

– вибро-акустический;

– побочные электромагнитные излучения и наводки (ПЭМИН);

– иные каналы утечки информации.

А также различные устройства съёма и перехвата защищённой информации по техническим каналам.

Кроме того, невозможно точно спрогнозировать поведение системы в момент осуществления воздействия на неё источника угроз.

Из этого следует, что безопасное состояние системы обуславливается только при осуществлении мер по устранению всевозможных реализаций угроз [12, 31].

1.3 Нормативно-правовые документы, регулирующие отношения в области обработки персональных данных

Самым первым основополагающим документом принято выделять Федеральный закон №152 «О персональных данных». Данный закон регулирует взаимоотношения в области обработки персональных данных между различными государственными органами власти (федеральными, субъектов Российской Федерации, иными), а также физическими и юридическими лицами при использовании информационных технологий, средств автоматизации или же без их использования. Данный закон приводит и описывает основные определения, связанные с процессами обработки персональных данных, вводит в рассмотрение понятия специализированных и биометрических персональных данных. Даёт пояснения касательно прав и обязанностей субъектов персональных данных, а также операторов персональных данных в процессе осуществления их обработки.

Следующим важным документом является Постановление правительства Российской Федерации №1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее – информационные системы) и уровни защищенности таких данных [40]. Данный документ рассматривает типы актуальных угроз, характерные для определённой ИСПДн:

– угрозы 1-го типа являются актуальными для информационной системы, если в системном программном обеспечении, используемом в ИС, присутствуют недекларированные (недокументированные) возможности;

– угрозы 2-го типа являются актуальными для информационной системы, если в прикладном программном обеспечении, используемом в ИС, присутствуют недекларированные возможности;

– угрозы 3-го типа актуальны для информационной системы, если в системном и программном обеспечении наличие недекларированных возможностей отсутствует.

Постановление также устанавливает четыре уровня защищённости для ИСПДн, в соответствии с категорией обрабатываемых ПДн, актуальных угроз и количества субъектов ПДн (отмечается наличие или же отсутствие в системе данных сотрудников оператора). Определяются следующие категории обрабатываемых в системе персональных данных:

– биометрические персональные данные – сведения, описывающие конкретные физиологические и биологические характеристики человека, в соответствии с которыми может быть установлена его личность и которые используются оператором для идентификации личности субъекта персональных данных;

– специальные категории персональных данных – персональные данные, описывающие расовую, национальную принадлежность человека, религиозные взгляды, политические, философские убеждения, а также детали состояния здоровья, либо его интимной жизни;

– общедоступные персональные данные – персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, сформированных в соответствии со статьёй 8 Федерального закона «О персональных данных»;

– иные категории персональных данных – все остальные персональные данные, не относящиеся к первым трём пунктам.

ИСПДн разделяются по количеству субъектов персональных данных:

– количество субъектов превышает 100 000;

– количество субъектов не превышает 100 000.

Классификация ИСПДн по уровням защищённости в зависимости от категорий обрабатываемых ПДн, типов актуальных угроз, количества субъектов ПДн и соответствующих данным показателям уровней защищённости отражена в таблице Приложения А.

В данном постановлении также рассматриваются требования для обеспечения того или иного уровня защищённости. Взаимосвязь требований к обеспечению информационной безопасности ИСПДн с уровнями защищённости показана в таблице Приложения Б.

Следует отметить приказ ФСТЭК от 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных». Данные меры по обеспечению состояния защищённости персональных данных применяются для защиты их от случайного или преднамеренного к ним доступа, уничтожения, видоизменения, распространения, а также помимо этого от иных неправомерных воздействий [41]. Данный документ характеризует такие меры обеспечения безопасности персональных данных, как: механизмы управления доступом и его разграничения, механизмы идентификации и аутентификации, способы антивирусной защиты, контроль обеспечения целостности персональных данных и другие. Данный документ приводит таблицу, показывающую взаимосвязь используемых мер по обеспечению состояния защищённости информационных ресурсов для каждого уровня защищённости персональных данных. Помимо этого в документе приведена таблица, которая рассматривает содержание мер по обеспечению безопасности персональных данных для каждого из уровней защищённости ПДн.

Необходимо отметить два методических документа ФСТЭК, которые описывают методику определения актуальных угроз и их тип.

Первый из них имеет название «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных сис-

темах персональных данных». Данный документ даёт основные понятия, связанные с угрозами персональных данных, характеризует порядок определения актуальных угроз, а также приводятся правила отнесения угрозы безопасности ПДн к актуальной [33]. Таким образом, чтобы оценить возможность осуществления конкретной угрозы, необходимо, в соответствии с данным документом, проанализировать такие показатели, как степень защищённости информационной системы персональных данных, а также вероятность реализации рассматриваемой угрозы. С помощью приведённой в методическом указании таблицы исследуются технические и эксплуатационные характеристики ИСПДн. Рассматриваются: территориальное размещение информационной системы, наличие соединения с сетями общего пользования, встроенные операции с записями баз ПДн, разграничение доступа к ПДн, наличие соединения с другими ПДн иных информационных систем персональных данных, уровень обезличивания персональных данных, объем ПДн, предоставляющиеся сторонним пользователям ИСПДн без предварительной обработки. На основании обследованных показателей определяется степень защищённости ИСПДн. Вероятность реализации рассматриваемых угроз определяется экспертным путём. Для этого показателя существуют четыре градации. Перечень актуальных угроз составляется при помощи выявления соотношения между полученными показателями степени защищённости ИСПДн и вероятности реализации угроз.

Второй документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». В данном документе идут в рассмотрение угрозы утечки информации по ТК, угрозы несанкционированного доступа к информационным ресурсам (описание уязвимостей ИСПДн, описание угроз прямого доступа в операционную среду ИСПДн, характеристика угроз безопасности ПДн, реализуемых с использованием протоколов межсетевого взаимодействия, характеристика угроз программно-математических воздействий и т.д.), а также приведены типовые модели угроз для различных видов ИСПДн. К примеру, таких как:

локальных ИСПДн, не имеющих подключения к сетям связи общего пользования, а также международного обмена; локальных ИСПДн, имеющих подключения к данным сетям; в АРМ, не подключённым к сетям связи общего пользования и АРМ, подключённым, а также в распределённых ИСПДн, имеющих подключение к сетям связи общего пользования и не имеющих [4].

Процесс проведения аудита, а также принципы и обязанности аудиторов регулирует Федеральный закон №307 от 2008-го года «Об аудиторской деятельности» [52]. В данном документе приведены основные понятия, касающиеся процесса проведения аудита, стандарты, принципы аудиторской этики, а также права и обязанности аудиторской организации и её членов.

За нарушение законов следует ответственность. В частности такая ответственность наступает при разглашении персональных данных. К ответственности может быть привлечено любое лицо (физическое, юридическое), нарушившее федеральный закон [32].

1.4 Сравнительный анализ существующих программных средств

Ведя речь об основной цели проведения аудита информационной безопасности, можно охарактеризовать её как осуществление процесса выявления оценки состояния защищённости информационной системы организации для управления им в целом, учитывая перспективы его дальнейшего развития и усовершенствования [2]. Таким образом, возможность оценивая уровня информационной безопасности исследуемой информационной системы организации является основной задачей процесса проведения аудита.

В данном пункте рассматриваются методы и инструментальные средства для проведения активного аудита информационной безопасности, а также программные средства анализа и управления рисками.

Данные программные средства решают основные задачи процесса проведения аудита ИБ:

– Internet Scanner – обеспечивает автоматизированное, своевременное обнаружение и анализирование уязвимостей, а также инвентаризацию программно-

аппаратного обеспечения в корпоративных сетях. Данная программа проводит анализ изменений уровня защищённости. Она позволяет генерировать отчетные ведомости, в которых сравниваются состояния защищенности выделенных участков сети в определённые промежутки времени – данная методика позволяет оценить изменения уровня защищённости корпоративных сетей после осуществления реализации защитных мер;

– System Security Scanner – предназначен для решения одного из наиболее важных аспектов управления информационной безопасностью – обнаружения уязвимостей. Данная система анализирует уязвимости на уровне операционной системы, в отличие от предыдущего программного продукта, который осуществляет анализ на уровне сетевых сервисов;

– Cisco Secure Scanner – осуществляет полный анализ и локализацию уязвимостей системы защиты от несанкционированного доступа к информационным ресурсам с составлением подробного описания самой сети, а также работающих в ней устройств;

– RiskWatch – группа программных продуктов для проведения различных видов аудита безопасности: анализ физической защиты ИС, анализ информационных рисков, оценка соответствия ИС требованиям стандарта международного стандарта ISO 17799;

– программное обеспечение CRAMM – реализует метод анализа и контроля рисков: определение возможных рисков, уязвимости информационных ресурсов и соответствующая оценка их уровней, идентификация угроз и соответствующая оценка их уровней, определение эффективности и целесообразности обратных мер, подтверждение оправданности расходов на обеспечение информационной безопасности;

– комплексная экспертная система управления информационной безопасностью «РискМенеджер» – позволяет построить модели угроз, модели событий рисков, провести оценки рискообразующих потенциалов угроз, построить модели защиты, модели влияния средств защиты на изменение состояния безопасности

системы, осуществить выбор наиболее эффективных комплексов защитных мер, чтобы те оказывались экономически целесообразными и эффективными.

Сравнительная таблица показывает основные характеристики исследуемых программных средств. Как видно из приведённой ниже таблицы, данные программные средства решают основные задачи процесса проведения аудита ИБ, однако в них отсутствует возможность оценки уровня защищённости обследуемой информационной системы.

Таблица 1 – Сравнительный анализ программных средств

Название программного средства	Специализация	Возможность оценки уровня защищённости ИС
Internet Scanner	Анализ уязвимостей, инвентаризация ПО	Отсутствует, однако возможно отслеживание его изменения
System Security Scanner	Анализ уязвимостей на уровне ОС	Отсутствует
Cisco Secure Scanner	Анализ уязвимостей	Отсутствует
RiskWatch	Анализ физической защиты ИС, анализ информационных рисков, оценка соответствия ИС требованиям стандарта международного стандарта ISO 17799	Отсутствует
CRAMM	Анализ рисков, определение эффективности контрмер	Отсутствует
РискМенеджер	Построение моделей угроз, моделей защиты, определение эффективности контрмер	Отсутствует

Данные программные продукты реализуют основные цели проведения аудита информационной безопасности. Как альтернатива подобным средствам будет создана система поддержки принятия решений, основанная на модульной нейронной сети, позволяющая проводить анализ в условиях недостаточности

исходных данных и построение в связи с этим прогнозов в соответствии с текущей нормативно-правовой документацией.

1.4 Особенности применения нечётких нейросетей в процессе аудита информационной безопасности

В общем случае нейронные сети представляют собой устройства параллельных вычислений, которые состоят из совокупности более простых и меньших по размеру процессоров. Каждый процессор такой нейронной сети имеет дело только с сигналами, которые он время от времени получает, и сигналами, которые он время от времени отправляет иным процессорам [47]. Искусственные нейронные сети представляют собой математические модели, а также их аппаратно-программную реализацию, схожие по принципам работы биологических нейронов. Это можно считать попыткой смоделировать и описать механизмы работы мозга. Первые разработки нейросетей принадлежали У. Маккалоку и У. Питтсу [30]. Когда были разработаны алгоритмы обучения нейросетей, те стали широко применяться в решении различных задач: в прогнозировании, распознавании образов, в задачах управления и т.д. С разных точек зрения сети могут иметь различное обозначение. Так, например, с точки зрения машинного обучения нейросеть является частным случаем методов распознавания образов, кластеризации и т.п. А с математической точки зрения это будет многопараметрическая задача нелинейной оптимизации.

Так, например, в задачах распознавания образов основными объектами могут выступать: изображения, примеры звуков, символы и т.п. Объекты характеризуются совокупностью значений признаков. Данная совокупность должна однозначно определять класс объекта. Здесь количество выходных показателей равно количеству определённых классов. При работе сети на вход поступает некоторый образ. Далее на одном из выходов должен оказаться признак принадлежности образа тому или иному классу. Другие же выходы должны показывать признаки непринадлежности.

Основным достоинством нейронных сетей является то, что генерируемую новую информацию об исследуемой проблемной области можно получить на основании прогнозов. При этом они могут обучаться с помощью уже имеющейся доступной информации. Процесс обучения – одно из основных преимуществ нейросетей перед традиционными алгоритмами. Во время процесса обучения нейросеть обнаруживает сложные зависимости между входными и выходными показателями, а затем осуществляет обобщение [13, 53, 59].

Построение нейросети сводится к следующим этапам:

– 1-й этап – конфигурирование и настройка структуры, а также основных составляющих нейронной сети;

– 2-й этап – обучение нейросети на основании уже существующих данных о предметной области;

– 3-й этап – проверка нейронной сети с использованием некоторой тестирующей выборки;

– 4-й этап – использование нейронной сети для разрешения задач о предметной области [34].

Частным случаем нейронных сетей являются так называемые нечёткие нейронные сети или гибридные сети. Они объединили в себе как достоинства нейронных сетей, так и систем нечёткого вывода. Поэтому они являются наиболее удобным и менее трудоёмким механизмом для решения поставленных задач об исследуемой предметной области.

Нечёткие нейронные сети основываются на теории нечёткой логики, в частности системе нечёткого вывода. Нечёткая логика предназначена для представления в формальном виде человеческих способностей к неточным, нечётким, приближенным суждениям, которые позволяют составлять более адекватное описание ситуаций, связанных с неопределённостью [27]. Математический раздел нечёткой логики является в своём роде обобщением раздела классической логики и теории множеств. Нечёткая логика основывается на понятии нечёткого множества, основоположником которого стал Лютфи Заде в 1965 году.

Нечёткая нейросеть, входящая в состав системы поддержки принятия решений в качестве одного из функциональных модулей, позволит проанализировать исследуемую информационную систему персональных данных с точки зрения оценки выполнимости и невыполнимости предъявляемых к ней требований. По степени выполнения тех или иных требований будет осуществляться общее оценивание состояния защищённости системы, а также выдаваться рекомендации по улучшению текущих показателей.

1.5 Классы и характеристики пользователей

Данное программное средство сможет подходить пользователям, занимающимся непосредственным процессом аудита. Основным пользователем системы будет являться сам аудитор, участвующий в процессе проведения внутреннего аудита конкретной организации [25]. Это программное средство поможет ему осуществить процесс аудита информационной безопасности информационных систем персональных данных. Здесь в его распоряжении может стать не только определение уровня защищённости системы, но и его оценка, а также вывод рекомендаций.

Также помимо аудитора анализом систем могут заниматься непосредственно пользователи анализируемой информационной системы персональных данных. Это могут быть различные операторы, осуществляющие процессы ввода, обработки и получения информации, а также администратор информационной системы.

1.6 Выбор модели жизненного цикла

1.6.1 Описание процессов жизненного цикла

Жизненным циклом программного средства или системы является совокупность процессов, а также работ и задач, которая подразумевает собой разработку, эксплуатацию, а также сопровождение программного средства или системы и охватывающая их жизнь от формирования основной концепции до полного прекращения их использования [6]. Также жизненный цикл программного обеспечения представляет собой объединение множества процессов, начинаю-

щихся от момента принятия решения о создании ПО, его основной идеи, до полного вывода ПО из эксплуатации [16]. Концепция жизненного цикла берёт своё начало с конца XIX века, как комплекс идей развития, наследственности, адаптации отдельных видов живых организмов, а также целых популяций [56].

Все процессы жизненного цикла можно разделить на:

– основные;

– вспомогательные;

– организационные.

Основные процессы жизненного цикла представляют собой процессы, которые осуществляются под управлением и надзором основных сторон, участвующих в жизненном цикле программных средств. К данному подразделению можно отнести следующие процессы:

а) заказ – здесь происходит формирование работ заказчика, состоит из определения потребностей заказчика к системе, подготовки заявки на подряд;

б) поставка – данный процесс инициируется с подписания договора на создание и последующее внедрение разрабатываемой системы в предприятие. Здесь идут в рассмотрение и оговариваются все процедуры и ресурсы, которые необходимо будет задействовать и затратить на создание программного продукта;

в) разработка – состоит из работ и задач, инициируемых непосредственно разработчиком:

1) подготовка процесса разработки – выбор модели жизненного цикла, инструментальных средств разработки, языков программирования;

2) анализ требований к системе – анализ предметной области, определение требований на основании данной области;

3) проектирование системной архитектуры – определение общей архитектуры системы, а также дальнейшее уточнение требований;

4) анализ требований к программным средствам – на данном этапе анализируется назначение разрабатываемого программного средства;

5) проектирование программной архитектуры – создание эскизного проекта для создаваемого продукта;

6) техническое проектирование программных средств – проводится процесс детальное проектирования, реализуется технический проект;

7) программирование и тестирование программных средств – осуществляется кодирование, а после тестирование программных модулей;

8) сборка программных средств – сборка программных модулей и сопутствующих компонентов в единое программное средство;

9) квалификационные испытания программных средств;

10) сборка системы – осуществляется сборка объектов программной и технической конфигурации, ручных операций, других подсистем в единую систему;

11) квалификационные испытания создаваемой системы;

12) ввод в действие программных продуктов;

13) осуществление приёма программных продуктов.

г) эксплуатация – состоит из работ и задач, инициируемых оператором;

д) сопровождение – реализация различных модификаций в процессе эксплуатации, изменение существующего программного продукта при сохранении его целостности.

Вспомогательные процессы жизненного цикла являются отдельными составляющими остальных процессов ЖЦ, которые предназначены для обеспечения успешного создания и качественного исполнения программного продукта. К вспомогательным процессам можно отнести следующие процессы:

– документирование – предполагает создание, редактирование и выпуск сопроводительной документации по каждому этапу жизненного цикла;

– управление конфигурацией – управление выпуском и изменениями программных объектов системы;

– обеспечение качества – обеспечение гарантий того, что ПС и процессы ЖЦ соответствуют требованиям качества;

– верификация – процесс определения соответствия функционирования программных продуктов требованиям и условиям, которые были рассмотрены на предыдущих работах;

– аттестация – определение полноты соответствия установленных требований их функциональному назначению;

– совместный анализ – оценка состояния и результатов работ по проектированию;

– аудит – определение соответствия требованиям, оговоренным в договоре, а также требованиям нормативно-правовой документации и т.п.;

– решение проблем – анализ и решение проблем, которые были обнаружены в процессе разработки.

Организационные процессы жизненного цикла представляют собой процессы, предназначенные для работы с организационными структурами, их формирования и совершенствования, охватывающие процессы жизненного цикла и соответствующий персонал. К ним относятся следующие процессы:

– управление – здесь осуществляется разработка планов выполнения процессов жизненного цикла программных средств, а также надзор и контроль хода их выполнения;

– создание инфраструктуры;

– усовершенствование – создание, оценка, измерение, контроль и улучшение любого процесса жизненного цикла программных средств;

– обучение – возможность инициирования процесса обучения персонала предприятия основным принципам работам.

1.6.2 Выбор и обоснование модели жизненного цикла для разрабатываемого программного средства

Модель жизненного цикла ПО – структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении жизненного цикла [11]. Существуют следующие модели жизненного цикла программных средств и систем:

– каскадная модель жизненного цикла ПО;

– инкрементная модель жизненного цикла ПО;

– спиральная модель жизненного цикла ПО.

Для разработки системы поддержки принятия решений целесообразно будет выбрать каскадную модель ЖЦ ПО.

Классическая каскадная модель жизненного цикла основывается на полном формулировании требований в начале ЖЦ. Возврата на предыдущие шаги в целях уточнения требований не происходит.

Процесс реализации осуществляется с помощью строго упорядоченной последовательности независимых этапов. Данная модель предполагает, что каждый последующий этап должен начаться после полного завершения предыдущего. Каскадная модель в некотором случае представляет собой процесс разработки с различной степенью детализации. В некоторых проектах те или иные этапы разработки могут быть опущены и наоборот. На всех шагах модели по мере необходимости выполняются вспомогательные и организационные процессы. К примеру, аттестация, верификация, аудит, управление, документирование и т.п.

Данная модель обладает следующими достоинствами:

– сформированные требования стабильны и неизменяемы в течение всего жизненного цикла;

– необходимо проходить только один этап разработки, тем самым обеспечивая простоту создания программного продукта;

– простота планирования, организации и управления проектом в целом;

– модель проста для понимания заказчика.

Но вместе с тем, модель имеет и недостатки:

– излишняя сложность формулирования требований в начале жизненного цикла ПО;

– линейность структуры процесса реализации программного средства. Данную модель тяжело применять для разработки больших и сложных систем. Это гро-

зит серьёзными нарушениями графиков планируемых и осуществляемых работ, а также экономической нецелесообразностью;

– невозможность использования промежуточных продуктов;

– пользователь не принимает должного участия в разработке. Лишь в самом начале (в момент определения требований) и в конце (во время приёмки).

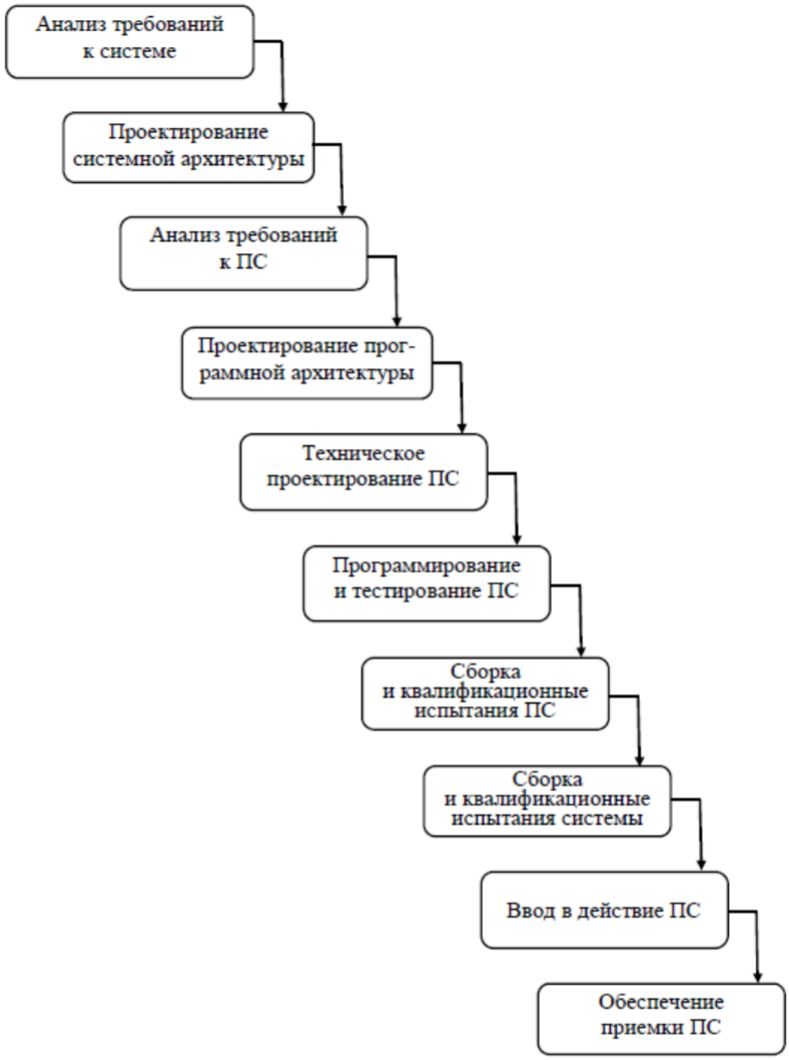

Рисунок 1 – Каскадная модель жизненного цикла программных средств

Данная модель будет хорошо применима в следующих случаях, когда разрабатывается проект с четкими, неизменяемыми в течение ЖЦ требованиями, реализация его понятна, и система в целом невысокой сложности. Таким образом, данная модель применима для реализуемой СППР, так как система имеет чётко определённые требования и невысокую сложность.

1.7 Обоснование и выбор инструментальных и программных средств для реализации системы поддержки принятия решений

Существуют различные инструментальные средства, позволяющие проводить научные исследования. Таким образом, создаются и совершенствуются различного рода средства познания: материальные, математические, логические, языковые, а также информационные. Все средства имеют одно общее свойство: всех их создают, формируют, обосновывают для определённых познавательных целей [36].

В процессе выполнения научной работы можно было использовать математические, информационные и языковые средства. Математические средства позволяют систематизировать и формализовать полученные опытным путём данные, а также находить и фиксировать количественные зависимости и закономерности. Математические средства используются помимо этого также как особые формы проведения аналогий (математическое моделирование). В качестве математического средства будет использована и применена на практике теория нечёткой логики, позволяющая смоделировать нечёткую нейронную сеть – один из модулей системы поддержки принятия решений.

Информационные средства позволяют упростить процессы проведения научных исследований и сократить время обработки данных. Существующие программные средства позволяют конструировать модули системы в соответствии с определёнными математическими алгоритмами для более правильной, корректной их работы.

Языковые средства в свою очередь дают понятийную базу. Важным языковым средством познания являются правила построения определений тех или иных понятий. При построении модуля интеллектуального анализа данных приходится прибегать к построению базы правил, которая содержит свои дефиниции, условия и заключения.

Пользовательский интерфейс реализуется с помощью языка C# на платформе .NET Framework. Данная платформа является многоязычной средой для

создания и выполнения приложений и имеет общеязыковую среду выполнения (CLR – Common Language Runtime) [23]. Данная среда имеет в своём распоряжении функции, значительно упрощающие трудоёмкость работ по проектированию приложений, а также уменьшающие объём программного кода.

Язык C# был разработан в 1998-2001-х годах инженерами компании Microsoft, где руководителями выступили Андерс Хейлсберг и Скотта Вильтаумота, как язык проектирования и создания приложений для платформы Microsoft .NET Framework [28]. Данный язык является полностью объектно-ориентированным языком, имеет возможности наследования и универсализации. Благодаря тому, что он является наследником C++, а именно: имеет схожий синтаксис и общие операторы, к нему проще перейти от его родителя. Усовершенствованный C# стал намного проще и надёжнее [7, 55].

Приложение для пользовательского интерфейса было создано с использованием Windows Forms. Интерфейс приложений такого типа строится в визуальном стиле на основании наиболее популярных форм Windows.

Для построения сети используется программное средство Matlab. В программном средстве Matlab механизм нечётких сетей реализован в модуле ANFIS – Adaptive Neuro-Fuzzy Inference System (адаптивная система нейро-нечёткого вывода). Matlab является широко используемой программной средой, реализующей многие функции и решающей задачи любой сложности. Имеет интуитивно-понятный интерфейс и проста в освоении [20, 48].

2 ПРОЕКТИРОВАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕ-ШЕНИЙ

Архитектурный проект предполагает осуществление процесса проектирования с помощью диаграмм языка UML, а также построение диаграмм основных функциональных модулей.

Цель процесса проектирования архитектуры системы заключается в определении того, как системные требования следует распределить относительно элементов системы [14].

UML – это унифицированный язык моделирования, используемый для описания проекта будущего программного продукта. Язык UML обеспечивает поддержку всех этапов жизненного цикла ИС и предоставляет для этих целей ряд графических средств – диаграмм [45].

Все диаграммы построены с помощью объектно-ориентированного CASE-средства Rational Rose. Данное средство позволяет автоматизировать процессы анализа и проектирования программного обеспечения, генерировать коды на различных языках программирования, а также выпускать проектную документацию. В состав Rational Rose входят следующие компоненты: репозиторий данных, графический интерфейс пользователя, средства просмотра проекта, средства контроля проекта, средства сбора статистики и генератор документов [26, 9, 10].

2.1 Диаграмма вариантов использования

Целью диаграммы вариантов использования является описание функционального назначения системы. Данная диаграмма является статической, поэтому не отражает временные рамки работы проектируемого программного средства. Процесс архитектурного проектирования следует начинать с построения данной диаграммы, так как она относится к концептуальному этапу проектирования программного средства. Основными составляющими диаграммы являются: вариант использования и действующее лицо – актёр. Вариант использования

отражает основные функции, которые должна выполнять будущая система. Актёр или действующее лицо представляет собой внешнюю сущность, которая может быть выражена в виде конкретного человека, устройства, системы или программы, выполняющая те или иные функции и являющаяся источником взаимодействия.

Для разрабатываемой системы в качестве актёров были выбраны:

– аудитор – конкретное лицо, работающее с системой;

– СППР – система поддержки принятия решений, с которой взаимодействует аудитор.

А также варианты использования:

– внести данные об ИСПДн (Информационной системе персональных данных);

– внести данные о ПДн (персональных данных);

– выдать уровень защищённости ИСПДн;

– выдать оценку уровня защищённости;

– выдать рекомендации.

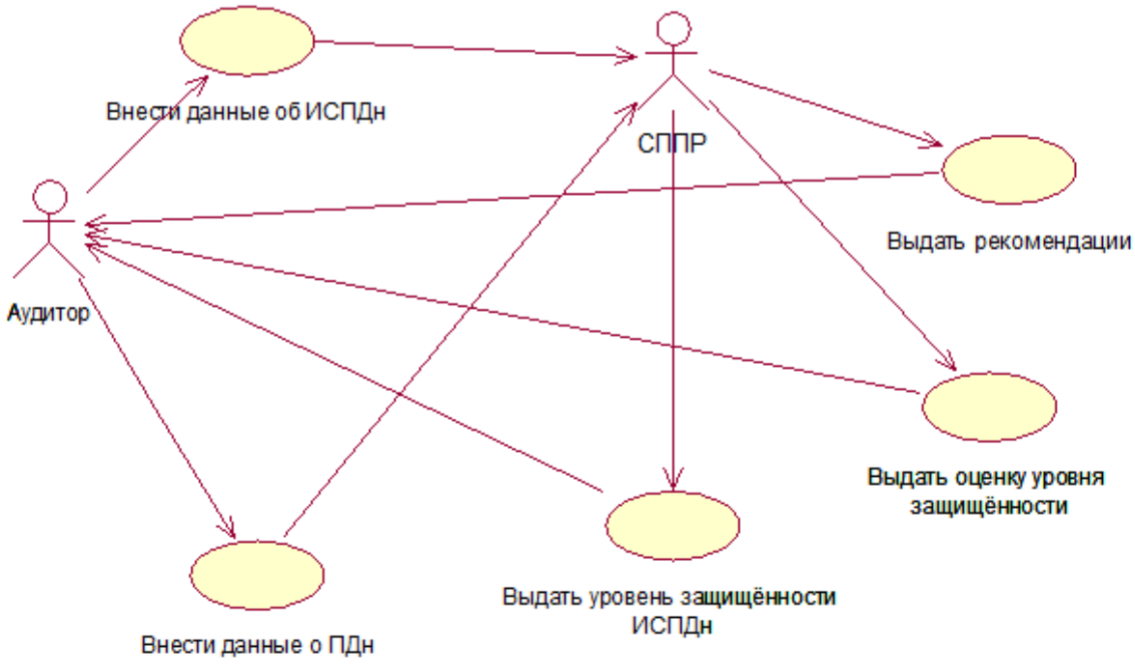

Рисунок 2 – Диаграмма вариантов использования

Между актёрами и вариантами использования возникает отношение ассоциации, что обозначает специфическую роль действующего лица при его взаимодействии с вариантами использования. Данная связь обозначается сплошной стрелкой.

2.2 Диаграмма последовательности

Диаграмма последовательности отражает взаимодействие объектов системы во времени, то есть является динамической. Основными составляющими данной диаграммы являются объекты, участвующие в работе системы, их линии жизни, показывающие динамику работы объектов и сообщения, передающиеся от одного объекта к другому.

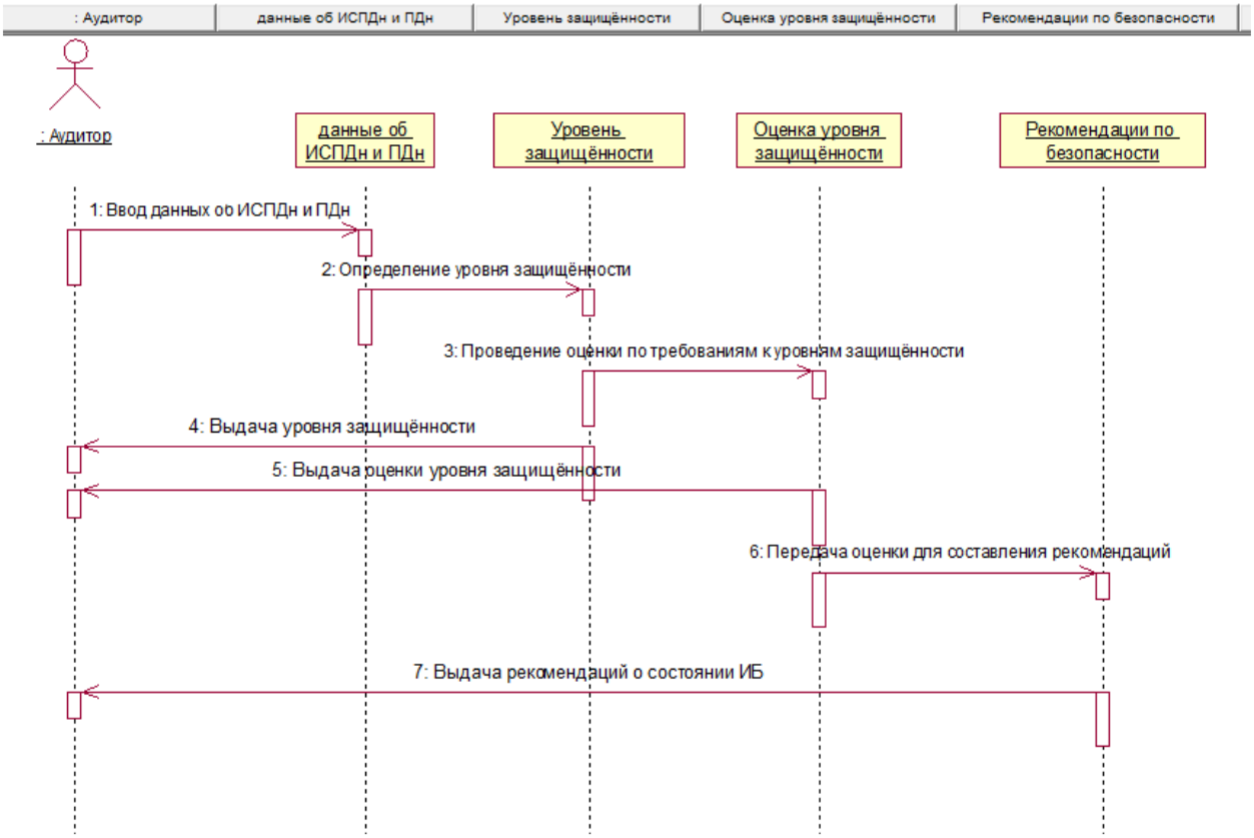

Рисунок 3 – Диаграмма последовательности

Объекты располагаются друг за другом в порядке выполнения той или иной работы. Каждое взаимодействие должно описываться совокупностью со-

общений, которые передаются между объектами. Сообщение представляет собой законченный фрагмент информации, который отправляется одним объектом другому. При этом приём сообщения инициирует выполнение определенных действий, направленных на решение отдельной задачи тем объектом, которому это сообщение отправлено.

Так объект «Аудитор» инициирует начало работы, передавая сообщение «Ввод данных об ИСПДн и ПДн» объекту «данные об ИСПДн и ПДн». Данный объект затем передаёт сообщение «Определение уровня защищённости» следующему объекту «Уровень защищённости». От этого объекта в свою очередь исходят два сообщения, одно из которых («проведение оценки по требованиям к уровням защищённости») переходит к последующему объекту – «Оценка уровня защищённости», а другое («Выдача уровня защищённости») передаётся Аудитору. От объекта «Оценка уровня защищённости» к конечному объекту «Рекомендации по безопасности» передаётся сообщение: «Передача оценки для составления рекомендаций». От него же также к Аудитору передаётся: «Выдача оценки уровня защищённости». Конечный объект «Рекомендации по безопасности» посылает окончательное сообщение Аудитору: «Выдача рекомендаций о состоянии ИБ».

2.3 Диаграмма состояний

Целью данной диаграммы служит описание последовательности возможных действий, происходящих с элементом рассматриваемой системы. Это своего рода граф специфического назначения, где в качестве вершин выступают состояния, а дуги в свою очередь изображают переход их одного состояния в другое.

Диаграмма состояний характеризуется начальным, конечным, а также промежуточными состояниями, а именно:

– инициализация, которая характеризуется вводом данных на входе об ИСПДн и ПДн;

– определение уровня защищённости, которое получает данные благодаря предыдущему состоянию, проводит их обработку в соответствии с нормативно-правовой документацией и выдаёт показатель уровня защищённости;

– оценка уровня защищённости, при котором производится процесс интеллектуального анализа данных в соответствии с предъявляемыми к исследуемой информационной системе персональных данных требований;

– формирование рекомендаций, которое анализирует полученную оценку и на выходе предоставляет сформированные рекомендации.

Рисунок 4 – Диаграмма состояний

2.4 Диаграмма активности

Для моделирования и проектирования процесса выполнения операций в языке UML используются диаграммы активности. Используемая в данных диаграммах графическая нотация во многом схожа с нотацией диаграммы состояний, так как на диаграммах активности аналогично присутствуют обозначения состояний и переходов. Каждое состояние на диаграмме активности соответствует осуществлению некоторой операции, а переход в следующее состояние срабатывает только в том случае, если завершилось предыдущее состояние.

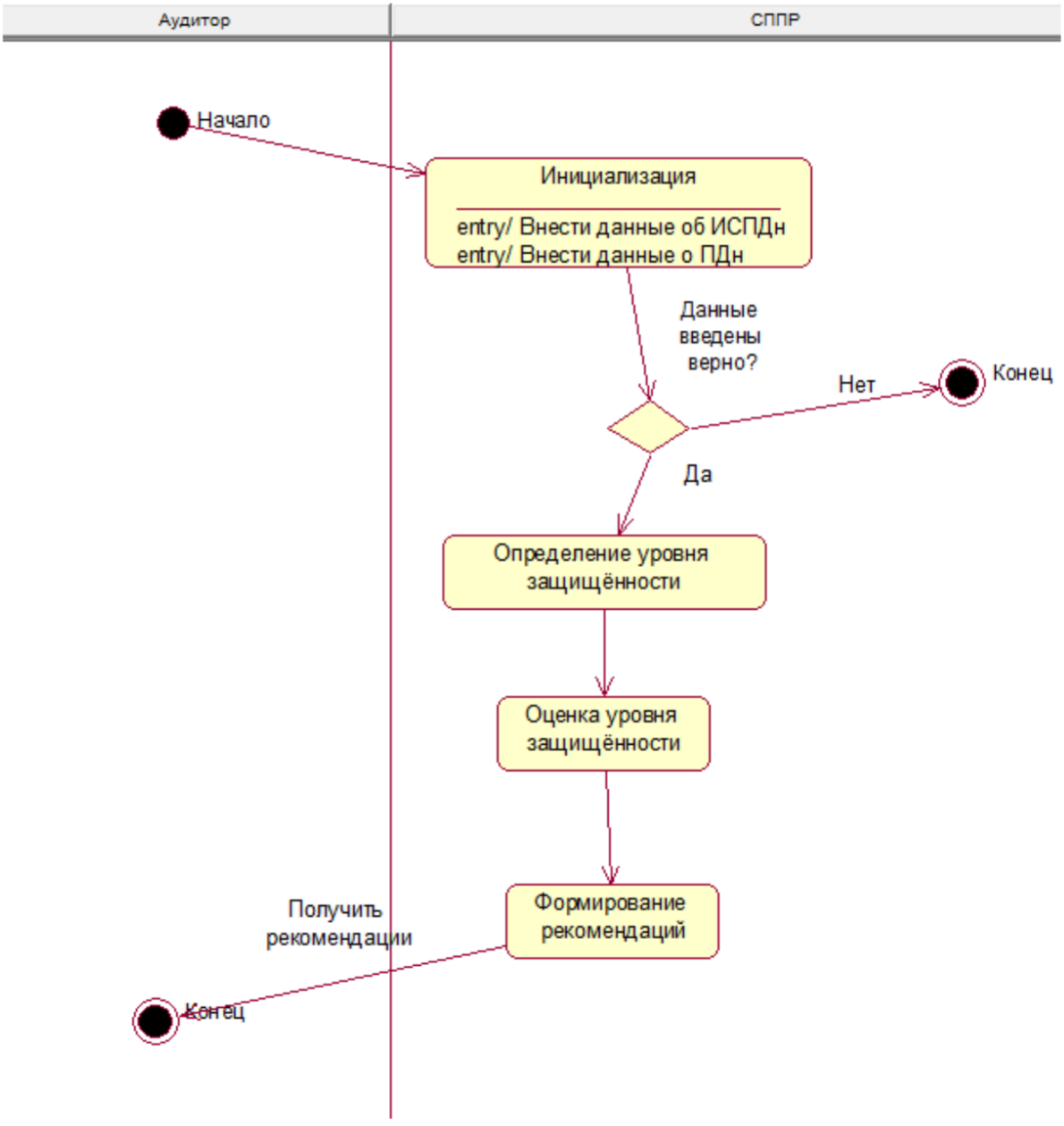

Рисунок 5 – Диаграмма активности

Так аудитор инициирует начало работы системы. Все остальные события приходятся на систему поддержки принятия решений. Возможно предварительное завершение работы системы, если данные, введённые в модуль инициализации, оказываются некорректными. Далее происходят события, аналогичные рассмотренным в диаграмме состояний:

– определение уровня защищённости;

– оценка уровня защищённости;

– формирование рекомендаций.

Конечное событие происходит на стороне аудитора, так как именно он получает всю информацию об исследуемой информационной системе персональных данных.

2.5 Диаграмма компонентов

Диаграмма компонентов отображает физические объекты (компоненты) и взаимоотношения между ними. Она является статической, поэтому временные рамки в ней не предусмотрены. Компонент – физическая часть системы, находящаяся в совместимости с набором интерфейсов, обеспечивает реализацию какого-либо иного интерфейса.

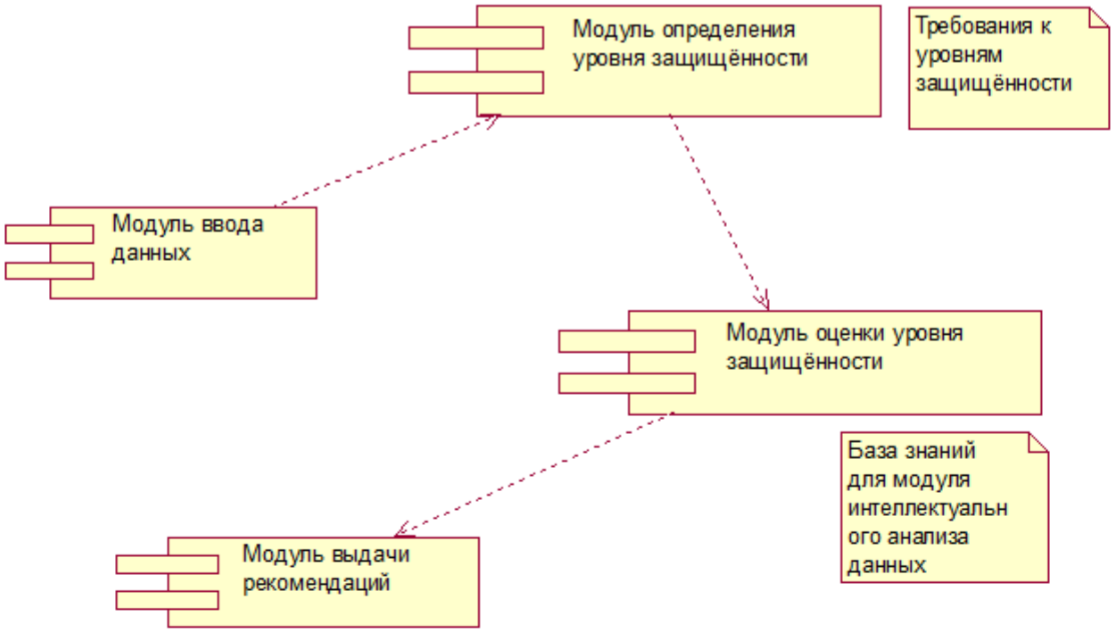

Рисунок 6 – Диаграмма компонентов

2.6 Проектирование архитектуры системы поддержки принятия решений

Модули системы должны выполнять следующие функции в соответствии с целями проведения аудита информационной безопасности.

Можно выделить следующие функции, которая должна выполнять система поддержки принятия решений:

– СППР должна подробно описывать информационную систему персональных данных, а также сами персональные данные в соответствии с нормативно-правовой документацией. В это входит определение категории обрабатываемых персональных данных, объём обрабатываемых персональных данных, тип ПДн (обрабатываются данные сотрудников оператора или же субъектов, не являющихся сотрудниками);

– составление модели угроз и злоумышленников. Данная операция должна осуществляться в соответствии с методическими документами ФСТЭК;

– определение уровня защищённости ИСПДн. Данная функция реализуется в соответствии с Постановлением Правительства №1119. С помощью полученных об ИСПДн и ПДн данных определяется текущий уровень защищённости и конкретные требования для него;

– оценка показателей защищённости. На основании показателей требований к уровню защищённости осуществляется оценка состояния защищённости ИСПДн. Данные требования анализируются с точки зрения соответствия реальных значений требуемым;

– формирование рекомендаций по совершенствованию состояния защищённости информационной системы персональных данных. На основании полученных данных о состоянии защищённости делается вывод о проделанной работе, и предлагаются возможные варианты по улучшению показателей защищённости.

В соответствии с вышеприведёнными функциями предлагается спроектировать следующие функциональные модули:

– модуль описания информационной системы персональных данных – определение категории обрабатываемых персональных данных, объём обрабатываемых персональных данных, тип ПДн;

– модуль определения уровня защищённости системы – в соответствии с Постановлением Правительства №1119 определяется текущий уровень защищённости и требования для него;

– модуль интеллектуального анализа данных – производит оценку показателей защищённости;

– модуль формирования рекомендаций по совершенствованию состояния защищённости информационной системы персональных данных.

Диаграмма архитектуры системы поддержки принятия решений, отображающая основные функциональные модули, представлена на рисунке 7.

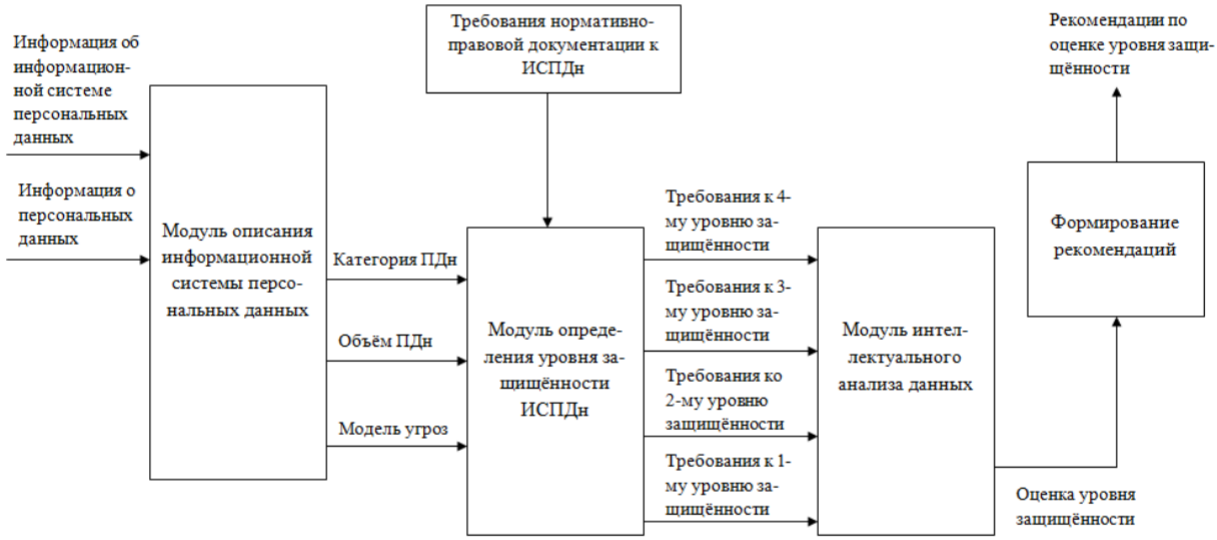

Рисунок 7 – Архитектура системы поддержки принятия решений

Входами к данной системе можно обозначить следующие показатели:

– информация о персональных данных – их тип, категория;

– информация об информационной системе персональных данных – объём обрабатываемых персональных данных, угрозы, которые могут быть обнаружены в процессе работы информационной системы персональных данных.

Выходом данной системы являются сформированные рекомендации по работе информационной системы персональных данных, в частности оценка уровня защищённости.

Требования нормативно-правовой документации являются наиболее важной составляющей системы поддержки принятия решений, так как они влияют на работу основных её модулей.

На схеме отображена взаимосвязь модулей:

– описания информационной системы персональных данных;

– определения уровня защищённости;

– интеллектуального анализа данных;

– формирования рекомендаций.

Так, в модуль описания информационной системы персональных данных поступают входные показатели СППР: информация о ПДн, а также информация об ИСПДн. Следующим шагом работы системы является определение уровня защищённости исследуемой информационной системы персональных данных.

Исходными данными для данного модуля являются:

– категория персональных данных;

– объём персональных данных;

– модель угроз.

На основании полученных показателей, а также в соответствии с Постановлением Правительства №1119 определяется уровень защищённости исследуемой информационной системы персональных данных.

В соответствии с одним из определённых уровней защищённости к исследуемой системе поддержки принятия решений должны предъявляться требования к уровням защищённости. Чем выше уровень защищённости, тем больше требований ему должно быть предъявлено.

Требования к уровням защищённости должны быть оценены аудитором, а их оценка будет введена в модуль интеллектуального анализа данных, который

выведет показатель итоговой оценки уровня защищённости исследуемой информационной системы персональных данных.

По итоговой оценке составляется рекомендация по повышению показателей уровня защищённости. Система поддержки принятия решений не гарантирует стопроцентный результат анализа. Она лишь может осуществить помощь в процессе принятия того или иного решения.

Система поддержки принятия решений предназначена для осуществления помощи эксперту или аудитору в процессе принятии решений на основании использования различных, существующих данных, нормативно-правовой документации, обычных документов, а также знаний и моделей предметных областей для определения и разрешения проблем [44].

Более подробно рассматривается модуль интеллектуального анализа данных, который представлен на рисунке 8, где X1-X2 представляют собой требования к уровням защищённости, а Y1-Y4, соответственно, выходную оценку по каждому из уровней:

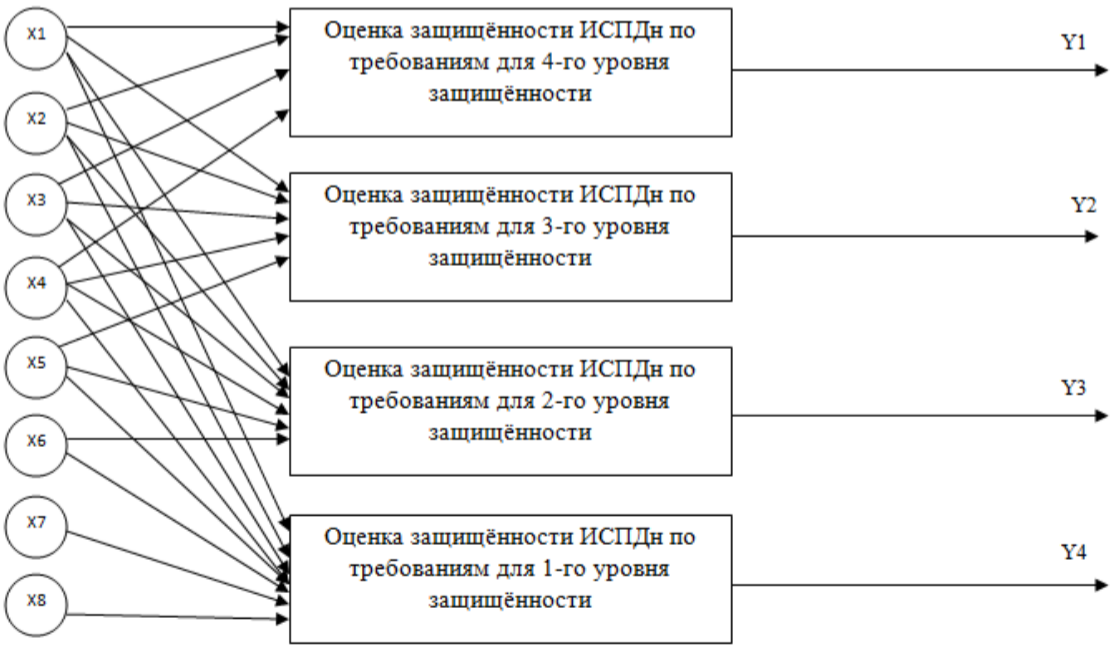

Рисунок 8 – Схема модуля интеллектуального анализа данных

Как видно из вышеприведённой схемы, всего уровней защищённости, предусмотренных Постановлением Правительства, выделяется четыре. В зависимости от того или иного уровня, количество требований будет различаться:

– 4-й уровень защищённости – самый низкий уровень защищённости. К нему предъявляются четыре требования, рассмотренные в Постановлении Правительства;

– 3-й уровень защищённости – средний уровень защищённости. К данному уровню предъявлено пять требований к уровням защищённости;

– 2-й уровень защищённости – уровень защищённости выше среднего. К данному уровню предъявляется шесть требований;

– 1-й уровень защищённости – самый высокий уровень защищённости. К нему предъявляется восемь требований к уровням защищённости.

Третья глава подробно рассматривает модуль интеллектуального анализа данных, который основывается на теории нечёткой логики и представляет собой нечёткую нейронную сеть.

3 ОПИСАНИЕ РЕАЛИЗАЦИИ ПРОГРАММНОГО СРЕДСТВА

В данном разделе приводится полное описание реализации системы поддержки принятия решений, состоящее из описания интерфейса, а также описания модуля интеллектуального анализа данных, представленного нечёткой ней-ронной сетью.

3.1 Определение входных и выходных показателей для системы

В зависимости от классификации информационной системы по четырём уровням, к ней предъявляются определённые требования. Классификация и требования к информационным системам персональных данных представлены в Постановлении правительства Российской Федерации №1119. Будущая система поддержки принятия решений должна оперировать основными сведениями об информационной системе персональных данных. Для классификации системы необходимо определить категорию обрабатываемых персональных данных. Постановление Правительства предполагает 4 категории:

– биометрические персональные данные;

– специальные категории персональных;

– общедоступные персональные;

– иные категории персональных данных.

Далее необходимо определить количество субъектов обрабатываемых персональных данных. Различают:

– количество субъектов не превышает 100 000;

– количество субъектов превышает 100 000.

Необходимо также составить модель угроз для информационной системы. Постановление Правительства определяет следующие типы актуальных угроз:

– угрозы 1-го типа являются актуальными для информационной системы, если в системном программном обеспечении, используемом в ИС, присутствуют недекларированные (недокументированные) возможности;

– угрозы 2-го типа являются актуальными для информационной системы, если в прикладном программном обеспечении, используемом в ИС, присутствуют недекларированные возможности;

– угрозы 3-го типа актуальны для информационной системы, если в системном и программном обеспечении наличие недекларированных возможностей отсутствует.

В результате анализа информационной системы персональных данных осуществляется классификация системы по четырём уровням защищённости. Каждый уровень должен гарантировать выполнения определённых требований, предъявляемых к системе. Существуют следующие требования:

– организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

– обеспечение сохранности носителей персональных данных;

– утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

– назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИСПДн;

– ограничение доступа к содержанию электронного журнала сообщений;

– автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

– создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Классификация информационных систем по уровням защищённости отражена в приложении А. Взаимосвязь требований с уровнями защищённости приведена в приложении Б.

3.2 Реализация пользовательского интерфейса

Схема программной реализации модулей отражена в Приложении В. Модель выполнена в методологии UML и представляет собой диаграмму компонентов. В качестве компонентов выступают основные физические элементы или файлы программного средства.

Пользовательский интерфейс был реализован при помощи языка C# на платформе Microsoft .NET Framework в программной среде Microsoft Visual Studio. MS Visual Studio – линейка программных продуктов компании Microsoft, в которые входят интегрированная среда разработки ПО, а также ряд других инструментальных средств. Данные продукты позволяют создавать как консольные приложения, так и приложения с графическим интерфейсом, в том числе с поддержкой технологии Windows Forms [42, 29, 49].

Для данного программного средства были реализованы основные окна работы с программой: вход в программу, окно непосредственной работы с программой, где необходимо было осуществить ввод данных об ИСПДн и ПДн, а также окно определения уровня защищённости.

При входе в программу осуществляется процесс ввода логина и пароля администратора, которые уже определены в системе.

Для основного окна работы с системой необходимо определить условия считывания входных данных: при каких показателях будет выдаваться тот или иной уровень защищённости.

На рисунке 9 изображен фрагмент данных условий:

```
private void button1_Click(object sender, EventArgs e)
{
    obj = int.Parse(textBox1.Text);

    if ((obj>100000) && checkBox2.Checked && checkBox3.Checked && (textBox2.Text =="Специальные"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
    if ((obj > 100000) && checkBox2.Checked && checkBox4.Checked && (textBox2.Text == "Специальные"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
    if ((obj < 100000) && checkBox2.Checked && checkBox3.Checked && (textBox2.Text == "Специальные"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
    if (checkBox1.Checked && checkBox3.Checked && (textBox2.Text == "Специальные"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
    if (checkBox3.Checked && (textBox2.Text == "Биометрические"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
    if ((obj > 100000) && checkBox2.Checked && checkBox3.Checked && (textBox2.Text == "Иные"))
    {
        this.Hide();
        Form3 Frm3 = new Form3();
        Frm3.Show();
    }
```

Рисунок 9 – Условия считывания входных показателей при работе системы поддержки принятия решений

Окно вывода информации об уровне защищённости содержит основную информацию, характерную для того или иного уровня защищённости. В данном случае такой информацией являются требования, предъявляемые к уровню защищённости.

3.3 Реализация модуля интеллектуального анализа данных

3.3.1 Основные понятия теории нечёткой логики

Модуль интеллектуального анализа данных базируется на теории нечёткой логики.

Теория нечёткой логики вводит в рассмотрение привычного высказывания степень неопределённости, тем самым позволяя отойти от привычных оп-

ределений классической теории логики. Таким образом, все высказывания в теории нечёткой логики могут принимать значения не только «Истина» или «Ложь» («0» или «1»), но и любые параметры в интервале [0, 1].

Нечёткое множество – это множество, которое характеризуется степенью неопределённости принадлежащих ему элементов, когда в некоторых случаях невозможно с полной уверенностью утверждать, что тот или иной элемент принадлежит данному множеству [35, 50, 37].

Математическое определение нечёткого множества имеет следующий вид. Множество *A* есть множество пар чисел вида:

,

где *x* – элемент некоторого множества *X*;

– функция принадлежности, отражающая степень принадлежности (соответствия) *x* заданному множеству *A*.

Данная функция также задаётся в форме отображения:

.

Данное отображение говорит о том, что каждому ставится в соответствие определённое действительное число, принадлежащее множеству [0, 1].

При этом если , то элемент абсолютно точно принадлежит множеству *A*. И наоборот. Если , то элемент абсолютно точно не принадлежит множеству *A*.

В общем случае запись нечёткого множества имеет вид:

. (1)

Чаще всего функции принадлежности, как правило, задаются графически и имеют различные формы и виды. Все точки, отложенные по оси *x,* задают множество. Точки по оси *y* – соответствующие им функции принадлежности.

Например, на рисунке 10 показана треугольная форма функции принадлежности:

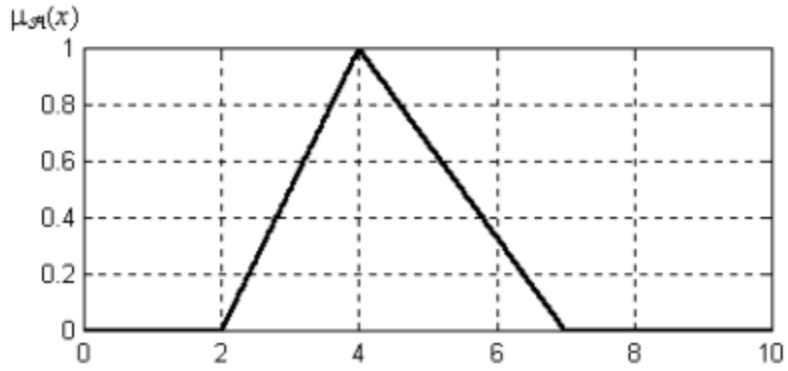

Рисунок 10 – Функция принадлежности треугольной формы

В общем случае аналитически её можно описать следующим образом:

$$f_{\Delta}(x;a,b,c) = \begin{cases} 0, x \le a \\ \dfrac{x-a}{b-a}, a \le x \le b \\ \dfrac{c-x}{c-b}, b \le x \le c \\ 0, c \le x \end{cases} \quad (2)$$

где *a, b* и *c* принимают свободные действительные значения.

Конкретно для данного примера *a=2, b=4, c=7*. Следовательно, для значения *a* функция принадлежности будет иметь вид , для значения пе-ременной *b* функция принадлежности имеет вид , а для значения *c* функция принадлежности соответственно будет равна .

Помимо этого существуют трапециевидные функции принадлежности. А также Z-образные и S-образные функции принадлежности, описываемые математическими моделями, имеющие иной вид.

В теории нечёткой логики принято использовать понятия нечёткой переменной и лингвистической переменной [22].

Определение нечёткой переменной имеет следующий вид. Нечёткая переменная – это набор чисел вида:

,

где α – имя нечёткой переменной;

X – множество нечёткой переменной;

– нечёткое множество на множестве нечёткой переменной X.

Лингвистическая переменная представляет собой обобщение нечёткой переменной и имеет вид:

,

где β – имя лингвистической переменной;

T – множество значений лингвистической переменной (так называемых термов) или терм-множество. Каждое из них является наименованием отдельной нечёткой переменной α;

X – множество нечётких переменных, относящихся к определению лингвистической переменной β;

G – синтаксическая процедура, реализующая процесс создания из множества T новых термов. В данной синтаксической процедуре могут быть применены логические связки «ИЛИ», «И», а также модификаторы типа «немного», «очень», «НЕ»;

M – семантическая процедура, ставящая в соответствие терму, созданному с использованием синтаксической процедуры G, некоторое осмысленное содержание при помощи формирования соответствующего нечёткого множества.

Нечётким множествам свойственны точно такие же логические операции, какие применимы в теории классической логики. Для них используются такие логические операции, как например: конъюнкция, дизъюнкция, импликация, логическое отрицание, эквивалентность.

В теории нечёткой логики помимо вышеприведённых определений использовано определение правила нечётких продукций. Нечёткие продукции на-

ходят своё применение в системах искусственного интеллекта и широко в них используются. Нечёткие продукции применяют для представления знаний и вывода заключений определённой предметной области в экспертных системах, а также для исследования, описания, исследования и моделирования сложных систем и процессов [15].

Экспертным системам приходится иметь дело с задачами ИИ, относящимися к верхнему уровню. Помимо этого они генерируют решения для помощи в управлении с учётом сложившейся ситуации, накапливают знания для базы знаний и пытаются копировать экспертное поведение [3].

Правило нечёткой продукции представлено следующим образом:

,

где *(i)* – имя нечёткой продукции;

Q – область применения продукции. Предназначена для описания предметной области, к которой относится продукция;

P – условие выполнимости ядра нечёткой продукции. Логическое выражение (предикат), которое позволяет активизировать (выполнить) ядро нечёткой продукции в случае выполнения условия истинности этого выражения;

– ядро нечёткой продукции, где:

A – антецедент, посылка продукции или же условие ядра;

B – консеквент или заключение ядра;

«=>» – логическое следование (или секвенция);

S – данный метод определяет значение степени истинности заключения ядра. Его можно охарактеризовать как реализацию алгоритма нечёткого вывода в общем случае. Помимо этого данный метод носит названия метода композиции или же активизации;

F – его второе название – весовой коэффициент. Его задача состоит в определении количественной оценки степени истинности нечёткой продукции. Данный коэффициент может принимать значения, принадлежащие интервалу [0, 1];

N – постусловия продукции. Данный параметр характеризует различные действия при реализации ядра продукции.

Центральный элементом понятия нечёткой продукции является ядро продукции. Его роль состоит в определении посылки в форме:: «ЕСЛИ *A*, ТО *B*».

Совокупность множества нечётких продукций представляет собой продукционную систему.

3.3.2 Описание системы нечёткого вывода

В общем случае процесс нечёткого вывода представляет собой алгоритм образования нечётких заключений на основе нечётких посылок (или условий). Он является совокупностью вышеприведённых понятий, таких как нечётких и лингвистических переменных, а также нечётких композиций и импликаций. Систему нечёткого вывода можно считать частным случаем продукционной системы.

Центральным элементом систем нечёткого вывода являются нечёткие лингвистические высказывания. Различают следующие типы нечётких лингвистических высказываний:

– высказывание «β есть α», где β – наименование лингвистической переменной, α – значение лингвистической переменной, которому ставится в соответствие тот или иной лингвистический терм из терм-множества *T*;

– высказывание «β есть α», где – модификатор типа: «НЕМНОГО», «ОЧЕНЬ», «МНОГО»;

– составные высказывания, являющиеся объединением первых двух типов с использованием логических связок «ИЛИ», «И», «НЕ», «ЕСЛИ_ТО».

Нечёткие высказывания позволяют формировать правила нечётких продукций, а именно их условий и заключений. Однако в данном случае антецедент (условие) ядра *A* и консеквент (заключение) ядра *B* представлены в виде типов высказываний 1, 2 и 3, представленных выше.

В общем виде правило формулируется следующим образом:

ПРАВИЛО <#>: ЕСЛИ , ТО ,

где является условием правила нечёткой продукции, а , соответственно, заключением. При этом не должен быть равен .

Для получения заключений из условий традиционно применяются механизмы или алгоритмы нечёткого вывода.

Алгоритм нечёткого вывода в общем виде состоит из приведённых ниже этапов, схематически представленных на рисунке 11:

Рисунок 11 – Этапы алгоритма нечёткого вывода

Формирование базы правил. Этап подразумевает составление базы правил нечётких продукций. Необходимо соблюдать полноту, непротиворечивость и согласованность составленных правил, чтобы избежать неправильных и неадекватных результатов.

База правил в общем виде задаётся следующим образом:

ПРАВИЛО_№1: ЕСЛИ «Условие_1», ТО «Заключение_1»

ПРАВИЛО_№2: ЕСЛИ «Условие_2», ТО «Заключение_2»

ПРАВИЛО_№3: ЕСЛИ «Условие_3», ТО «Заключение_3»

…

ПРАВИЛО_№n: ЕСЛИ «Условие_n», ТО «Заключение_n»

– весовой коэффициент или коэффициент определённости нечёткой продукции, принимающий значение в интервале [0, 1]. При неявности весового коэффициента его значение по умолчанию должно принимать единицу.

При составлении базы правил должна быть определена совокупность правил нечётких продукций , совокупность входных лингвистических переменных , а также совокупность выходных лингвистических переменных .

Фаззификация входных переменных. По-другому этот этап называют введением нечёткости. На данном этапе осуществляется процесс локализации и определения функций принадлежности лингвистических термов по исходным данным – каждому исходному данному – численному значению каждой входящей в систему нечёткого вывода переменной ставится в соответствие значение функции принадлежности определённого терма лингвистической переменной. Итогом данного этапа будет являться совокупность функций принадлежности по всем термам лингвистических переменных.

Агрегирование подусловий. Этап подразумевает нахождение значений степеней истинности подусловий по каждому из совокупности правил системы нечёткого вывода. Подусловия, имеющие первый или второй тип лингвистических высказываний, рассмотренные в предыдущем пункте, принимают степени истинности в соответствии с их функциями принадлежности. При составных подусловиях (третий тип лингвистических высказываний) для определения степени истинности необходимо использовать операторы нечёткой конъюнкции или нечёткой дизъюнкции.

Активизация подзаключений. Этап подразумевает нахождение степеней истинности (выполнимости) подзаключений для каждого правила совокупности

нечётких продукций. Здесь идёт рассмотрение подзаключений каждого правила и их весовые коэффициенты. Степенью истинности каждого подзаключения будет являться алгебраическое произведение значения истинности подусловия, который был определён на предыдущем этапе, и весового коэффициента данного правила.

После этого следует найти функции принадлежности для каждого подзаключения выходных лингвистических переменных. Для этого применяется один из нижеприведённых методов:

– min-активизация:

; (3)

– prod-активизация:

; (4)

– average-активизация:

, (5)

где – функция принадлежности терма некоторой выходной переменной , определённой на множестве Y;

– степень истинности подзаключения, определённая на данном этапе.

Аккумулирование заключений. На данном этапе осуществляется процесс нахождения функций принадлежности для каждой выходной лингвистической переменной из множества . Этап подразумевает объедине-ние всех степеней истинности итоговых заключений для выявления функций принадлежности каждой выходной переменной. Это необходимо, так как за-

ключения, относимые к одной и той же лингвистической переменной, имеют принадлежность разным правилам системы нечёткого вывода.

Дефаззификация выходных переменных. Последний этап работы системы нечёткого вывода. Иначе данный этап называют введением чёткости. Введение чёткости подразумевает процесс выявления обычного (чёткого) значения для каждой выходной переменной. На данном этапе для введения чёткости используются методы дефаззификации: метод центра тяжести, метод центра площади, метод центра тяжести для одноточечных множеств, метод левого модального значения, метод правого модального значения. Один из них используется в алгоритме нечёткого вывода типа Сугено, приведённом ниже.

3.3.3 Описание системы нечёткого вывода типа Сугено

Существует несколько широко используемых алгоритмов нечёткого вывода, осуществляющие процесс нечёткого вывода. Данные алгоритмы различаются, как правило, только отдельными параметрами, определёнными и специфичными для каждого алгоритма. Одним из таких алгоритмов можно выделить алгоритм Сугено. Данный алгоритм помимо этого также используется при формировании модульных нейронных сетей в модуле ANFIS программного пакета Matlab.

Состоит алгоритм типа Сугено из следующих этапов:

– 1-й этап – формирование базы правил. Правила формируются в соответствии со следующей моделью:

ПРАВИЛО <#>: ЕСЛИ И , ТО

,

где и – весовые коэффициенты. Полученное значение *w* принимает вид некоторого действительного числа;

– 2-й этап – фаззификация входных переменных в общем случае соответствует этапу фаззификации стандартной системы нечёткого вывода;

– 3-й этап – агрегирование подусловий. Для нахождения степени истинности подусловий должна быть применена логическая операция min-конъюнкции;

– 4-й этап – активизация подзаключений. На данном этапе применяется метод min-активизации для нахождения степени истинности всех подзаключений, а затем осуществляется вычисление обычных (чётких) значений выходных переменных. Для этого применяется вид задания правил из 1-го этапа, где вместо
и – значения входных переменных до введения нечёткости;
– 5-й этап – аккумулирование заключений. Здесь расчёты проводятся с обычными действительными числами.
– 6-й этап – дефаззификация выходных переменных. Для данного этапа используется модификация метода центра тяжести для одноточечных множеств:

———— , (6)

где – степень истинности подзаключения, выявленная на четвёртом этапе;
– чёткое значение, определённое на четвёртом этапе.

3.3.4 Описание лингвистических переменных

Для создания модуля интеллектуального анализа данных, представленного нейронной сетью, необходимо выявить входные и выходные данные. Ими будут являться требования к уровням защищённости, отражённые в таблице приложения Г, а также итоговая оценка уровня защищённости ИСПДн.

Приведённые требования могут быть однозначно и неоднозначно определяемыми.

Однозначно определяемые требования (требования, которые можно определить как однозначно выполняемые и невыполняемые):
– перечень лиц, допущенных к ПДн (Х3);
– должностное лицо, ответственное за обеспечение безопасности ПДн (Х5);
– автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн (Х7);

– структурное подразделение, ответственное за обеспечение безопасности ПДн (X8).

А также неоднозначно определяемые требования (их выполнение не может быть точно определено):

– режим обеспечения безопасности помещений, где обрабатываются ПДн (X1);

– сохранность носителей (X2);

– средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ (X4);

– ограничение доступа к содержанию электронного журнала сообщений (X6).

Вышеприведённый список говорит о том, что однозначно определяемые требования могут принимать только значения 0 либо 1. В то время как параметры неоднозначно определяемых требований могут варьироваться и принимать значения в интервале [0, 1].

Далее на основании полученных сведений определяются лингвистические переменные и их термы.

Для однозначно определяемых лингвистических переменных можно выделить только два лингвистических терма:

– S – однозначное выполнение требования;

– L – однозначное невыполнение требования.

Таким образом, числовые значения для вышеприведённых термов:

для терма S и для терма L.

Для неоднозначно определяемых переменных вводятся в рассмотрение три лингвистических терма:

– S – уровень выполнимости требования имеет низкое значение;

– M – уровень выполнимости требования имеет среднее значение;

– L – уровень выполнимости требования имеет высокое значение.

Таким образом, числовые значения для данных термов принадлежат интервалам: для терма S, для терма M и для терма L.

Для итоговой оценки, представленной одним выходом , определяются пять термов следующего вида:

– S – уровень защищённости оценивается низко;

– SM – уровень защищённости оценивается ниже среднего;

– M – оценка уровня защищённости принимает средние значения;

– ML – уровень защищённости оценивается выше среднего;

– L – оценка уровня защищённости принимает высокие значения.

Соответственно, числовые значения для данных термов принадлежат интервалам: для терма S для терма SM, , для терма M, , для терма ML и для терма L.

Данные параметры будут использованы при построении нечёткой нейронной сети, описываемой в последующем пункте.

3.3.5 Построение нейросети

Модуль интеллектуального анализа данных представляет собой модульную или гибридную, нечёткую нейронную сеть.

В среде Matlab механизм гибридных сетей реализован в модуле ANFIS – Adaptive Neuro-Fuzzy Inference System (адаптивная система нейро-нечёткого вывода). Созданная с помощью данного модуля гибридная нейронная сеть представляет собой нейронную сеть, имеющая несколько входов, которые являются лингвистическими переменными, и единственный выход [21, 57, 43].

Метод адаптивной системы нейро-нечёткого вывода был разработан в начале 1990-х годов. Выводу данной системы ставится в соответствие совокупность правил нечёткого вывода вида: «если-то». Данные правила обладают существенным достоинством, характеризующимся способностью обучаться аппроксимации нелинейных функций.

Термы входящих переменных подлежат описанию обычными функциями принадлежности, в то время как выходная перемена должна быть описана константой, либо линейной функцией принадлежности.

ANFIS предполагает работу с системой нечёткого вывода типа Сугено. Данный метод говорит о том, что все весовые коэффициенты должны быть равны единице.

Пакет Matlab с помощью отдельных редакторов позволяет пользователю настраивать элементы сети: возможность настройки функций принадлежности и базы правил, а также помимо этого вывод визуализированной трёхмерной поверхности итоговых показателей.

Чтобы построить нечёткую нейронную сеть, необходимо для начала составить базу правил.

В качестве примера исследуемая информационная система персональных данных классифицируется по четвёртому уровню защищённости. Таким образом, категория обрабатываемых данных – общедоступные, количество субъектов ПДн не должно превышать 100 000, тип актуальных угроз не предусматривает недекларированные возможности в ПО и ОС – третий тип. А значит, для данного уровня защищённости будут определены следующие требования:

– режим обеспечения безопасности помещений, где обрабатываются ПДн (X1);

– сохранность носителей (X2);

– перечень лиц, допущенных к ПДн (X3);

– средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ (X4);

Три требования, представляющие собой неоднозначно определяемые лингвистические переменные, определяются тремя лингвистическими термами (S, M, L). Однозначно определяемое требование определяется двумя термами (S, L). Таким образом, сумма правил будет равна: .

Правила описываются в форме:

где – j-е правило;

X1, X2, X3, X4 – входные показатели;

– значение выхода j-го правила;

, , , , – нечёткие подмножества.

Фрагмент правил показан на рисунке 12:

	A	B	C	D	E	F
1		Входные факторы				
2	№	X1	X2	X3	X4	Y
3	1	S	S	S	S	S
4						
5	2	S	S	L	M	M
6						
7	3	S	S	S	L	SM
8						
9	4	S	S	L	S	SM
10						
11	5	S	S	S	M	SM
12						
13	6	S	S	L	L	M
14						
15	7	S	M	S	S	SM
16						
17	8	S	M	L	M	M
18						
19	9	S	M	S	L	M
20						
21	10	S	M	L	S	M

Рисунок 12 – Фрагмент базы правил для нечёткой нейронной сети

Полная база правил отражена в приложении Г.

После построения базы правил осуществляется составление обучающей выборки на её основе. Для этого необходимо для каждого правила каждой входной переменной случайно выбрать значение, подходящее тому или иному лингвистическому терму. К примеру, для построения данной выборки был использован численный метод Монте-Карло. Фрагмент обучающей выборки отображён на рисунке 13:

№	X1	X2	X3	X4	Y
1	0.289	0.049	0	0.208	0.013
2	0.162	0.073	1	0.301	0.43
3	0.044	0.147	0	0.97	0.14
4	0.189	0.254	1	0.26	0.27
5	0.17	0.149	0	0.82	0.205
6	0.28	0.146	1	0.983	0.37
7	0.245	0.891	0	0.116	0.208
8	0.042	0.573	1	0.831	0.555
9	0.15	0.673	0	0.953	0.62
10	0.115	0.585	1	0.093	0.611

Рисунок 13 – Фрагмент обучающей выборки

Полная выборка отражена в приложении Д.

Чтобы начать работу с редактором ANFIS, следует ввести в командную строку программной среды Matlab команду anfisedit. Произойдёт открытие редактора нечёткого вывода.

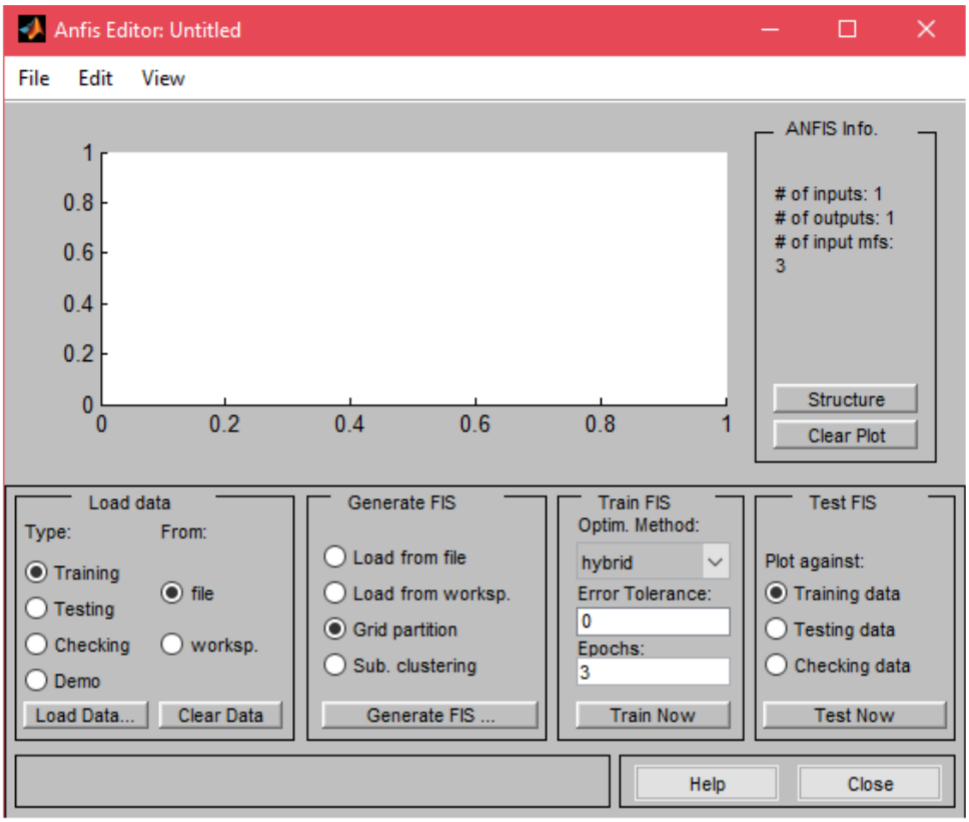

Рисунок 14 – Главное окно модуля ANFIS

Кнопка Load Data позволяет загрузить входные данные в будущую сеть. Входными данными будет являться созданная раннее обучающая выборка для нечёткой нейронной сети, сохранённая в текстовом редакторе в формате .dat. Для данной системы можно выделить следующие типы входных данных:

– обучающие данные – эти данные для обязательного использования, они созданы для непосредственного построения гибридной сети;

– тестовые данные – при помощи этих данных оценивается качество построенной сети;

– проверочные данные – с помощью проверочных данных определяется факт переобучения сети;

– демонстрационные данные – загрузка и работа с демонстрационными примерами.

Когда обучающая выборка была успешно загружена из файла, главное окно редактора ANFIS приняло вид:

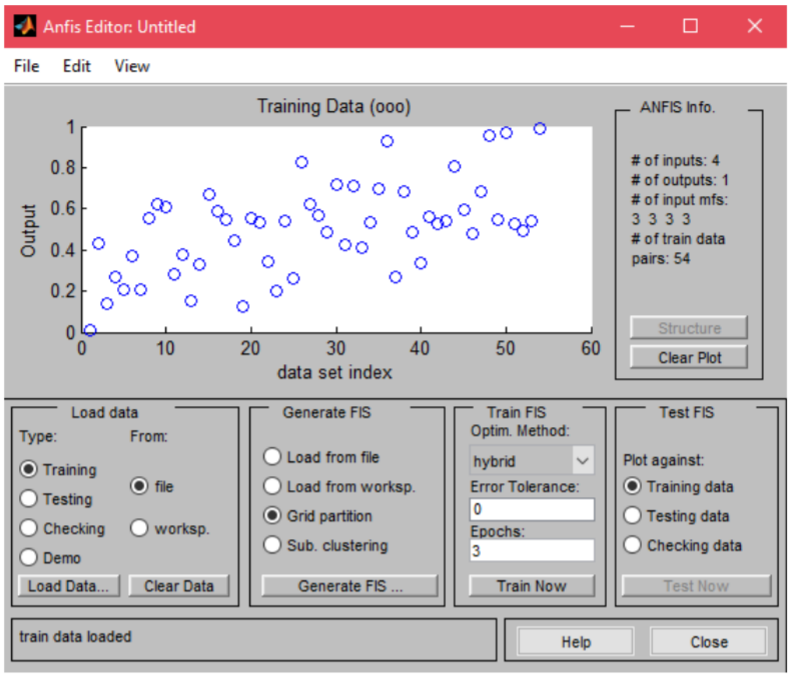

Рисунок 15 – Загрузка данных в модуль ANFIS

Далее необходимо создать структуру системы нечёткого вывода алгоритма типа Сугено, рассмотренного в предыдущих пунктах. Для этой цели существует кнопка Generate FIS.

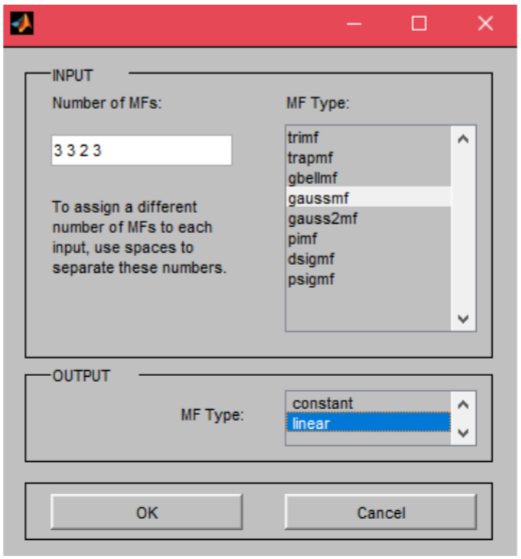

Рисунок 16 – Окно генерации структуры нечёткого вывода

В данном окне показаны основные параметры для настройки входных и выходной переменной. Для входных: количество функций принадлежности, а также их тип. Для выходной переменной настраивается только тип функции принадлежности: константа, либо линейная.

После нажатия на кнопку Structure главной рабочей области будет выведена структура полученной нечёткой нейронной сети:

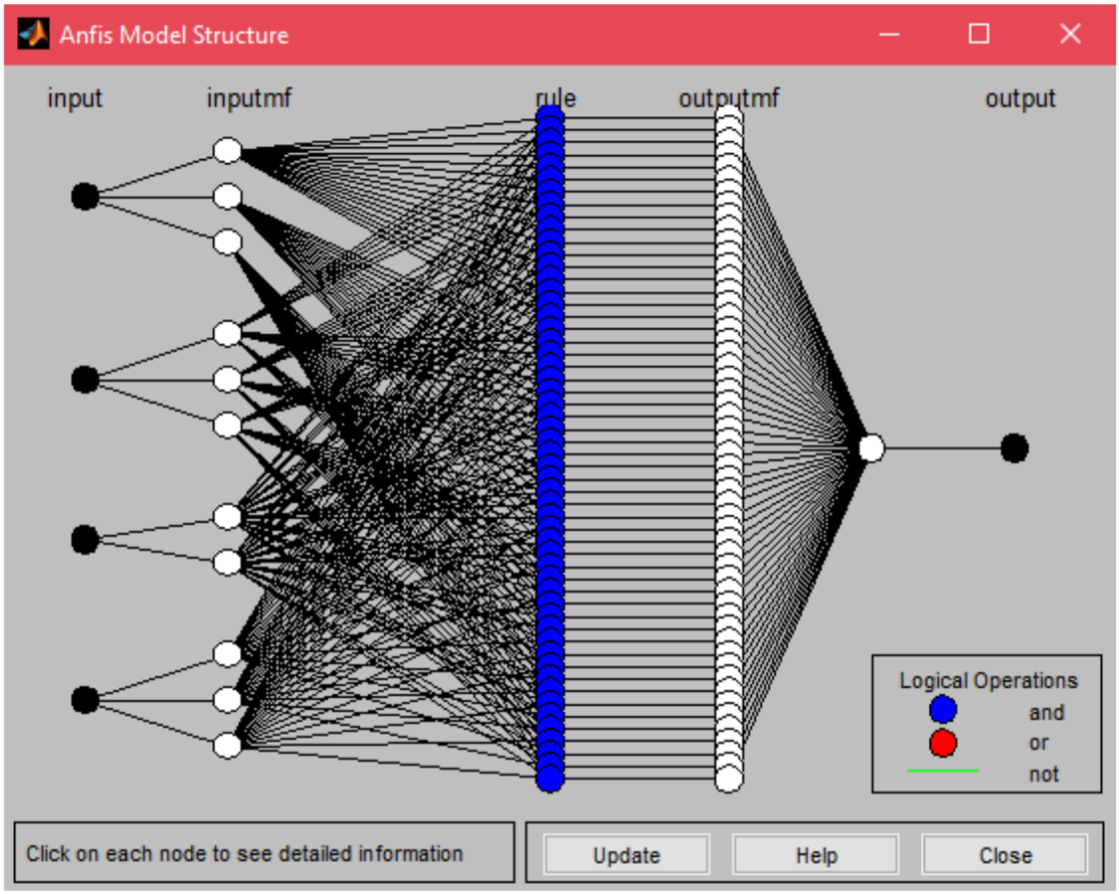

Рисунок 17 – Структура нечёткой нейронной сети

Для начала выбирается метод обучения. Это может быть либо гибридный: данный метод основывается на комбинации метода убывания обратного градиента и метода обратных квадратов, либо метод обратного распространения. После определения метода обучения устанавливается уровень ошибки обучения. По умолчанию данное значение равно 0. Затем устанавливается количество проводимых итераций обучения. Данное значение будет равно 40. Процесс обучения происходит после нажатия на кнопку Train now.

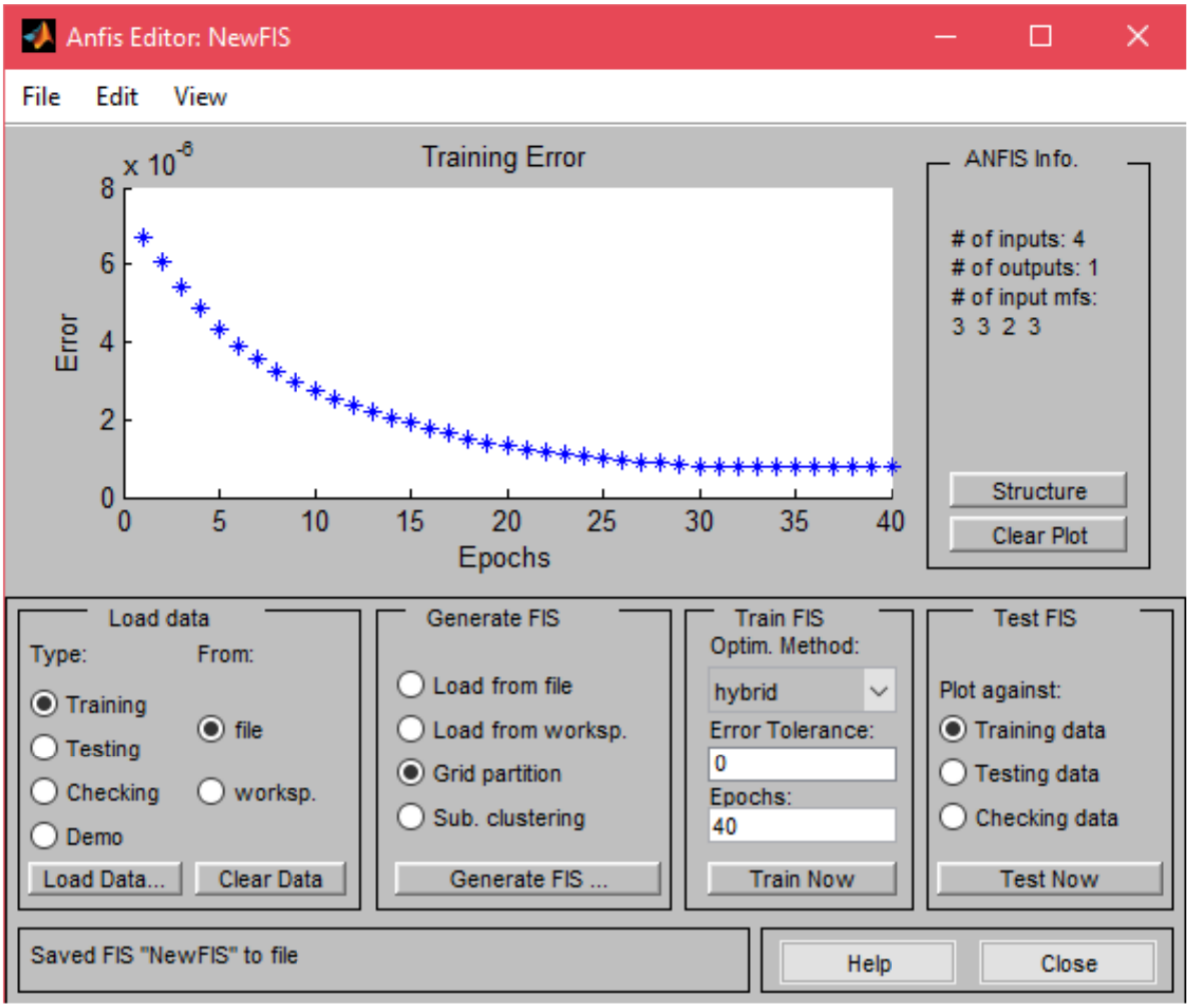

Рисунок 18 – Процесс обучения нечёткой нейронной сети

Полученный после обучения график будет отображать зависимость ошибки обучения от количества итераций обучения.

Matlab позволяет сохранить в файл сгенерированную структуру нечёткой сети с помощью последовательного нажатия на кнопки в верхнем меню редактора FIS File –> Export –> To file.

Созданную нечёткую нейронную сеть можно также настраивать в других специализированных редакторах, предусмотренных в пакете Matlab.

Редактор системы нечёткого вывода или же FIS editor является одним из таких редакторов. С его помощью можно настраивать функции принадлежности нейронной сети, задавать их параметры, давать имена входным и выходным переменным, а также добавлять новые переменные.

Чтобы открыть данный редактор, необходимо ввести в командную строку mfedit, либо в верхнем меню редактора ANFIS выбрать: Edit –> FIS Properties.

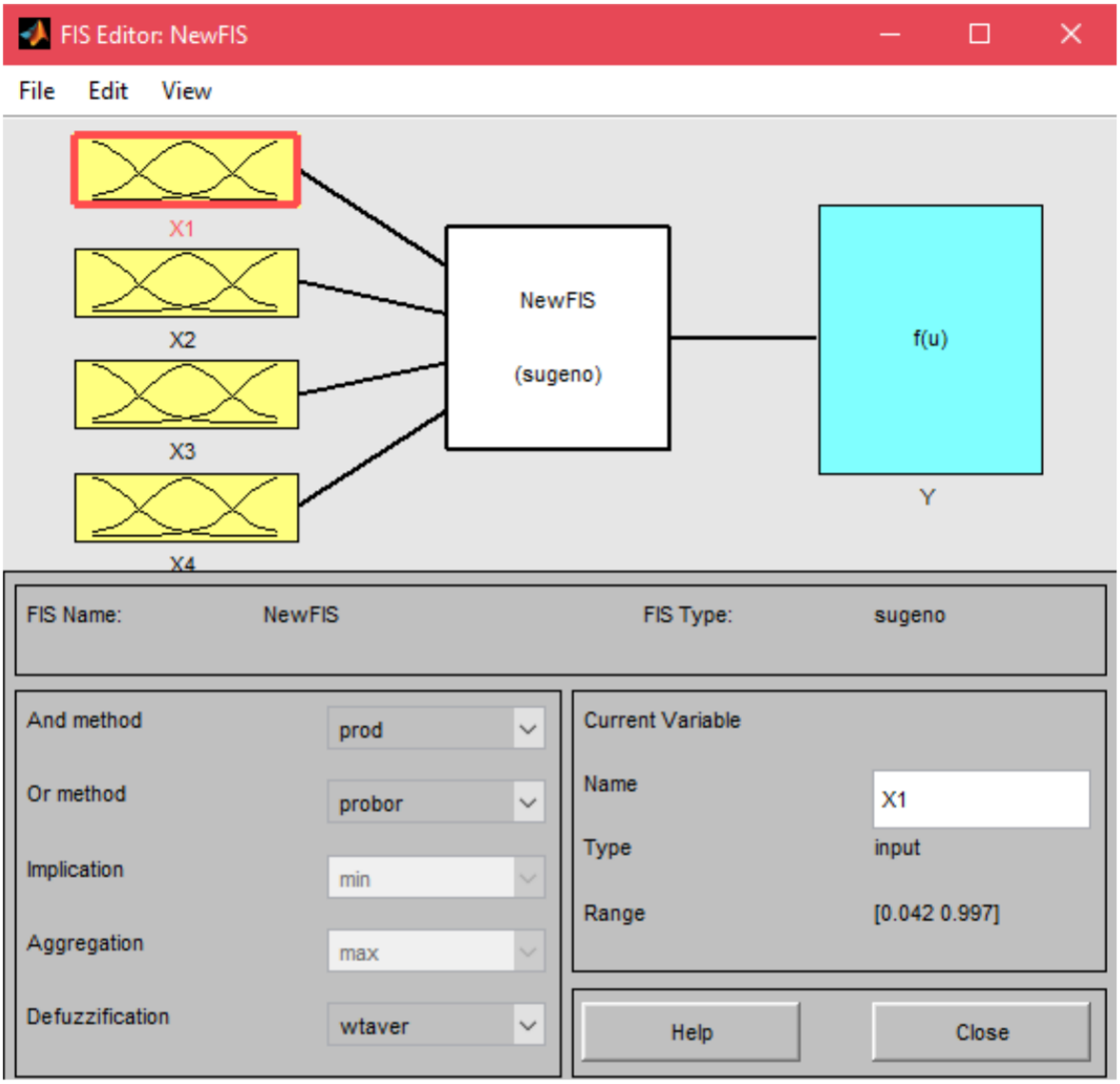

Рисунок 19 – Главное окно редактора системы нечёткого вывода

Данный редактор позволяет менять методы нечётких логических «ИЛИ» и «И» и способ дефаззификации, при этом методы импликации и агрегации оказываются неактивными.

Двойной щелчок по переменной позволяет открыть окно редактирования функций принадлежности для данной переменной.

Рисунок 20 – Окно редактирования функций принадлежности

Данное окно, отображённое на рисунке 20, позволяет редактировать функции принадлежности для определённых переменных. Аналогично можно задавать имена для функций принадлежности, определять их тип и задавать конкретные параметры.

Следующий редактор позволяет изменять и просматривать базу правил нечёткой нейронной сети.

Вызывается он из верхнего меню редакторов FIS или ANFIS: Edit –> Rules.

В данном редакторе можно выбирать способы связей между входными переменными, изменять описания правил, а также определять и выбирать их весовые коэффициенты, удалять старые и добавлять новые правила.

Окно редактирования базы правил изображено на рисунке 21:

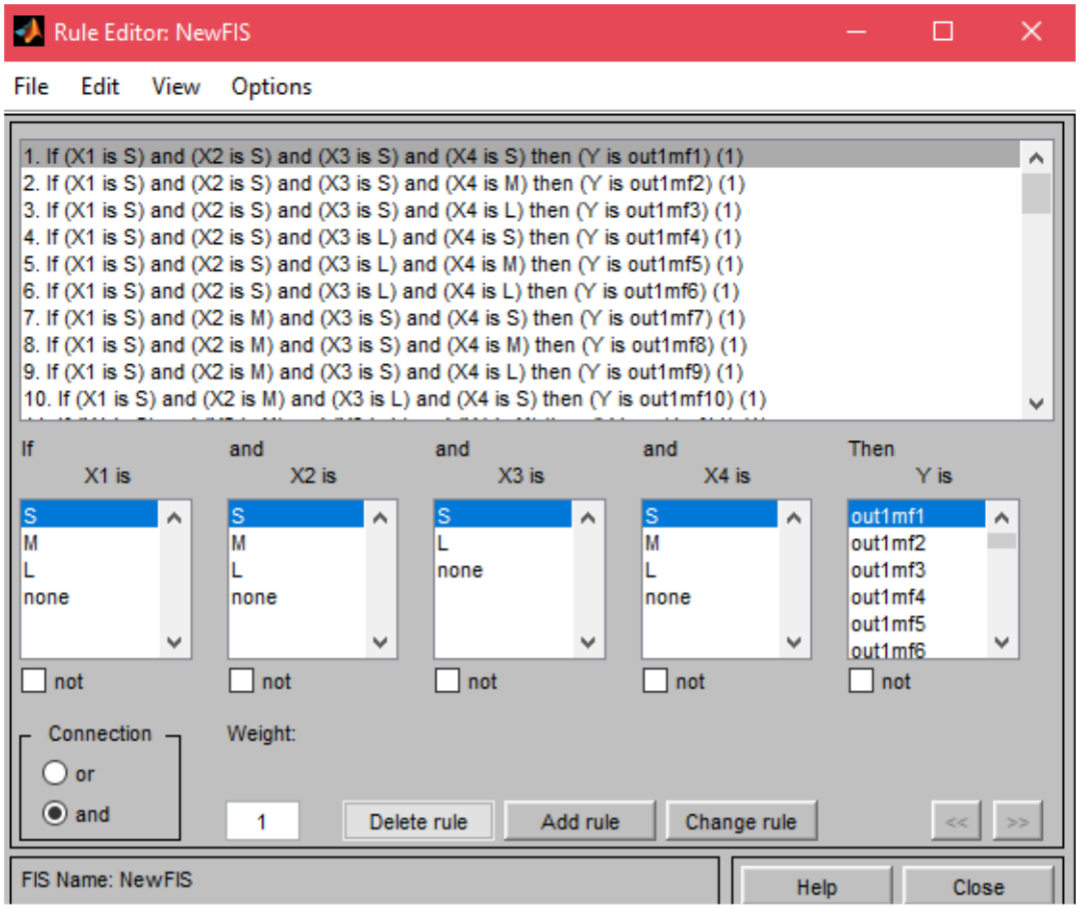

Рисунок 21 – Окно редактирования базы правил

3.4 Тестирование программных модулей

Для работы с системой поддержки принятия решений необходимо осуществить первичный вход в программу. Для этого необходимо ввести в поля логин и пароль для администратора. В данном случае логином и паролем будет являться «admin», так как работа системы поддержки принятия решений предназначена для единственного пользователя – непосредственно аудитора информационной безопасности.

В дальнейшем возможно расширение системы при добавлении в неё в качестве пользователей сотрудников исследуемой информационной системы персональных данных, что позволит им в самостоятельном порядке проводить анализ и определять оценку уровня защищённости.

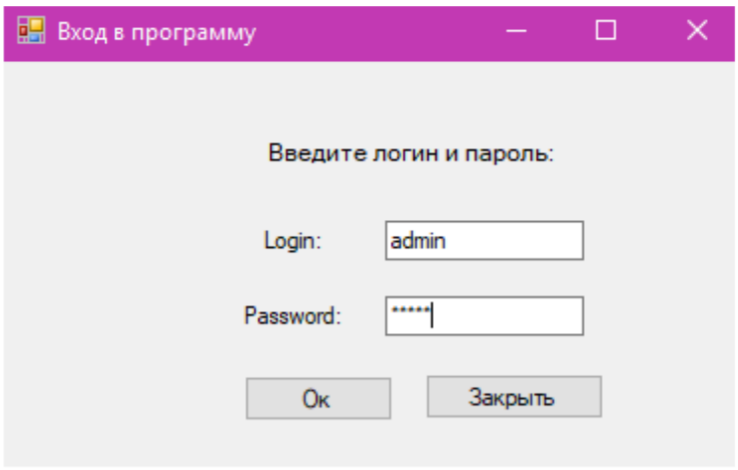

Рисунок 22 – Окно входа в программу

При неверном вводе данных, окно выдаст сообщение:

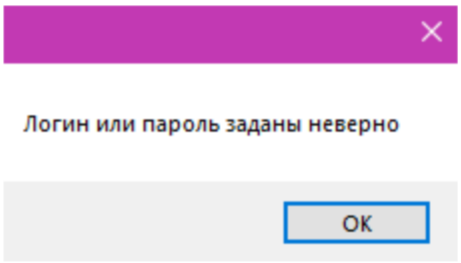

Рисунок 23 – Сообщение о неверном вводе логина и пароля

При успешном входе откроется основное окно работы с программой. Данное окно предусматривает заполнение некоторого бланка, который состоит из следующих элементов:

– тип обрабатываемых персональных данных (при нажатии на соответствующую кнопку можно прочесть про каждый тип используемых персональных данных, которые также приведены в Постановлении Правительства №1119);

– количество обрабатываемых персональных данных – значение должно быть целочисленным;

– наличие сотрудников оператора – необходимо отметить, обрабатываются ли в информационной системе данные о сотрудниках;

– тип актуальных угроз – из трёх приведённых моделей необходимо выбрать одну, соответствующую анализируемой информационной системе (существуют

недекларированные возможности ОС, существуют недекларированные возможности ПО, отсутствуют недекларированные возможности ОС и ПО).

Допустим, исследуемая информационная система персональных данных описывается следующими параметрами:

– тип обрабатываемых ПДн – общедоступные;

– количество субъектов ПДн – 900;

– информация о сотрудниках оператора в данной ИСПДн отсутствует;

– отсутствуют недекларированные возможности ОС и ПО.

Окно с вводом основным данных об ИСПДн изображено на рисунке 24:

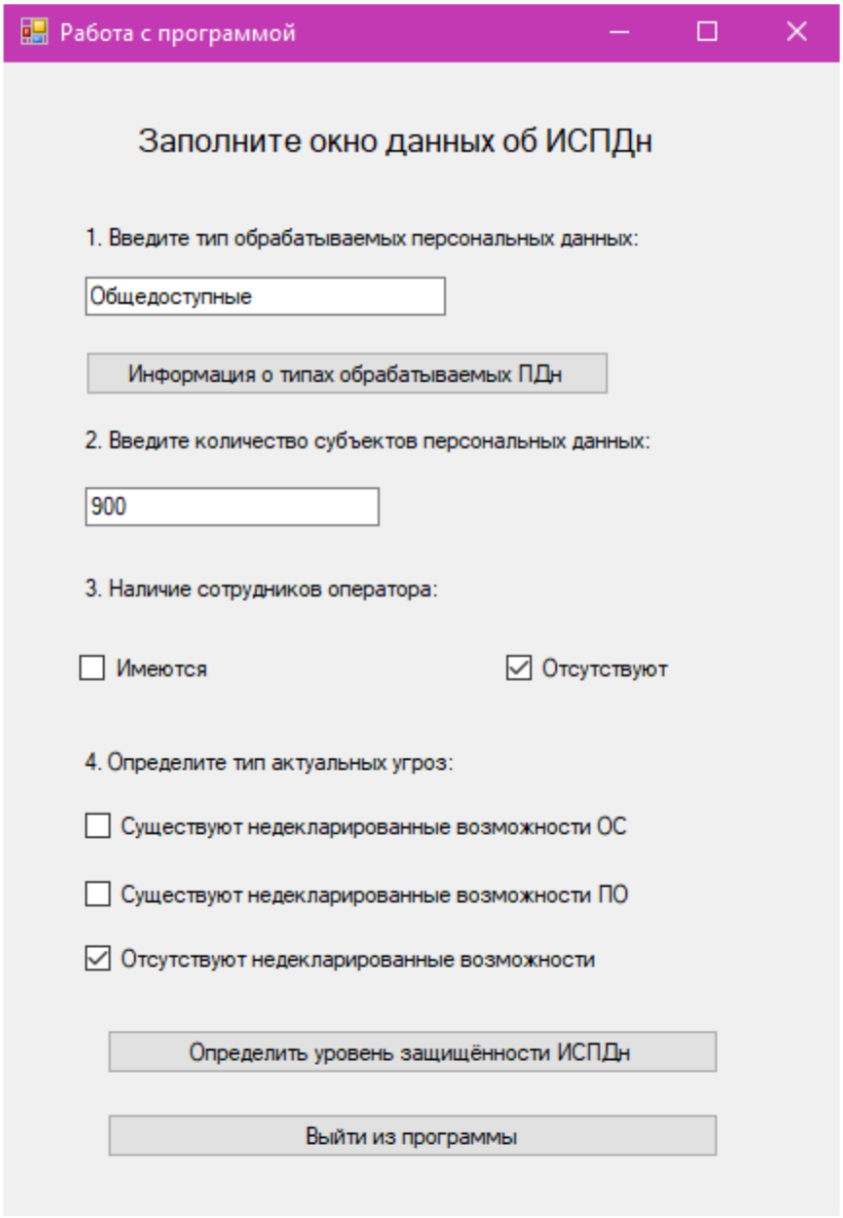

Рисунок 24 – Основное окно работы с программой

При некорректно введённых данных откроется окно с сообщением:

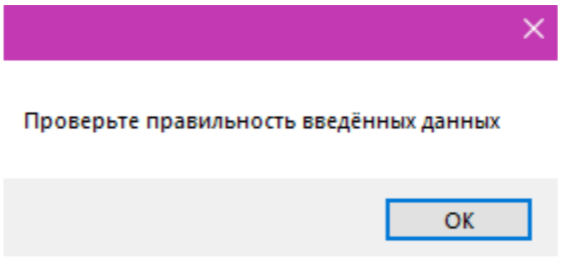

Рисунок 25 – Сообщение о некорректно заполненных полях в основном окне работы с программой

При нажатии на кнопку «Информация о типах обрабатываемых ПДн» будет выведено окно с описанием типов обрабатываемых персональных данных:

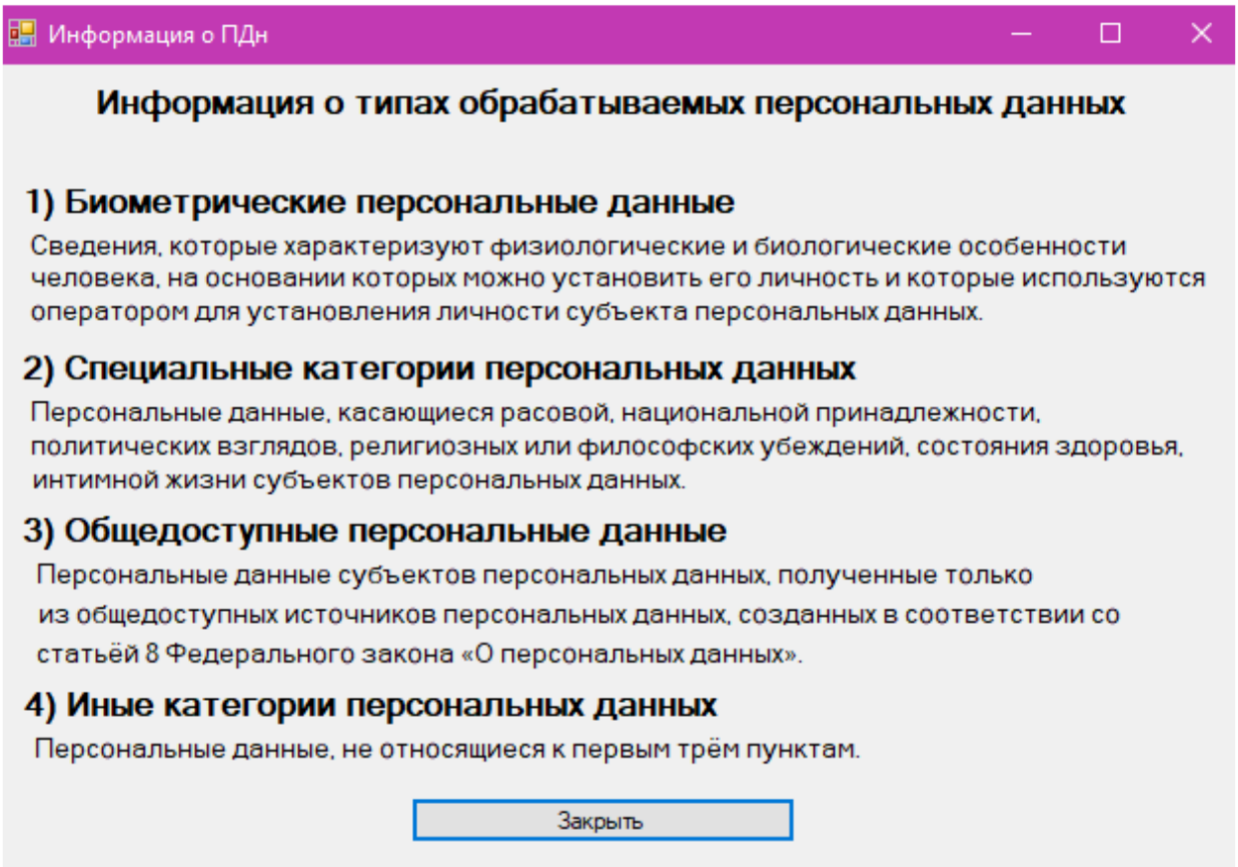

Рисунок 26 – Информация о типах обрабатываемых ПДн

После заполнения необходимых полей откроется окно с определением уровня защищённости исследуемой информационной системы персональных

данных. Система классифицирует исследуемую ИСПДн по 4-му уровню защищённости:

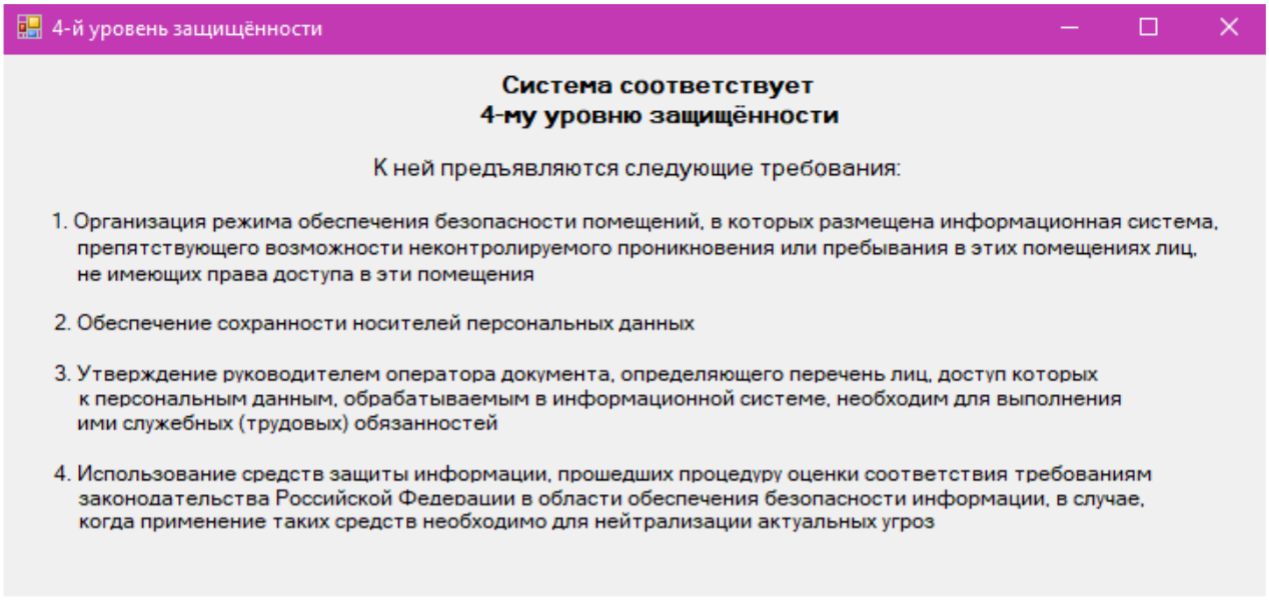

Рисунок 27 – Окно вывода уровня защищённости анализируемой инфор-мационной системы персональных данных

Далее идёт непосредственная работа с модулем интеллектуального анализа данных – нечёткой нейросетью.

В строке Input задаются значения входных данных, представленные требованиями к уровням защищённости, которые следует оценить с точки зрения их выполнимости и невыполнимости. Таким образом, эксперт или аудитор проводит оценку данных требований к уровням защищённости во время исследования ИСПДн следующим образом:

– значение режима обеспечения безопасности помещений, где обрабатываются ПДн (X1) – 1 (L);

– сохранность носителей (X2) – 0,7 (M);

– перечень лиц, допущенных к ПДн (X3) – 1 (L);

– средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства РФ (X4) – 0,6 (M).

Результат работы нечёткой модульной сети в редакторе ANFIS представлен на рисунке 28:

Рисунок 28 – Результат работы модульной нейронной сети

Итоговые показатели помимо этого можно визуализировать в виде поверхности для наиболее наглядного представления данных.

Визуализация поверхности открывается в верхнем меню редакторов FIS, ANFIS, функций принадлежности, либо в окне просмотра правил через пункты View -> Surface, либо с использованием комбинации горячих клавиш Ctrl+6.

Данная трёхмерная поверхность отображает взаимосвязь любых двух входных переменных от выходной переменной. По осям X и Y откладываются значения для входных переменных. По оси Z, соответственно – для выходных.

На рисунке ниже показана визуализированная поверхность итогового нечёткого вывода, показывающая зависимость входных переменных X1 и X2 с выходным значением Y. В зависимости от выбранных входных переменных визуализированная поверхность будет иметь различный вид.

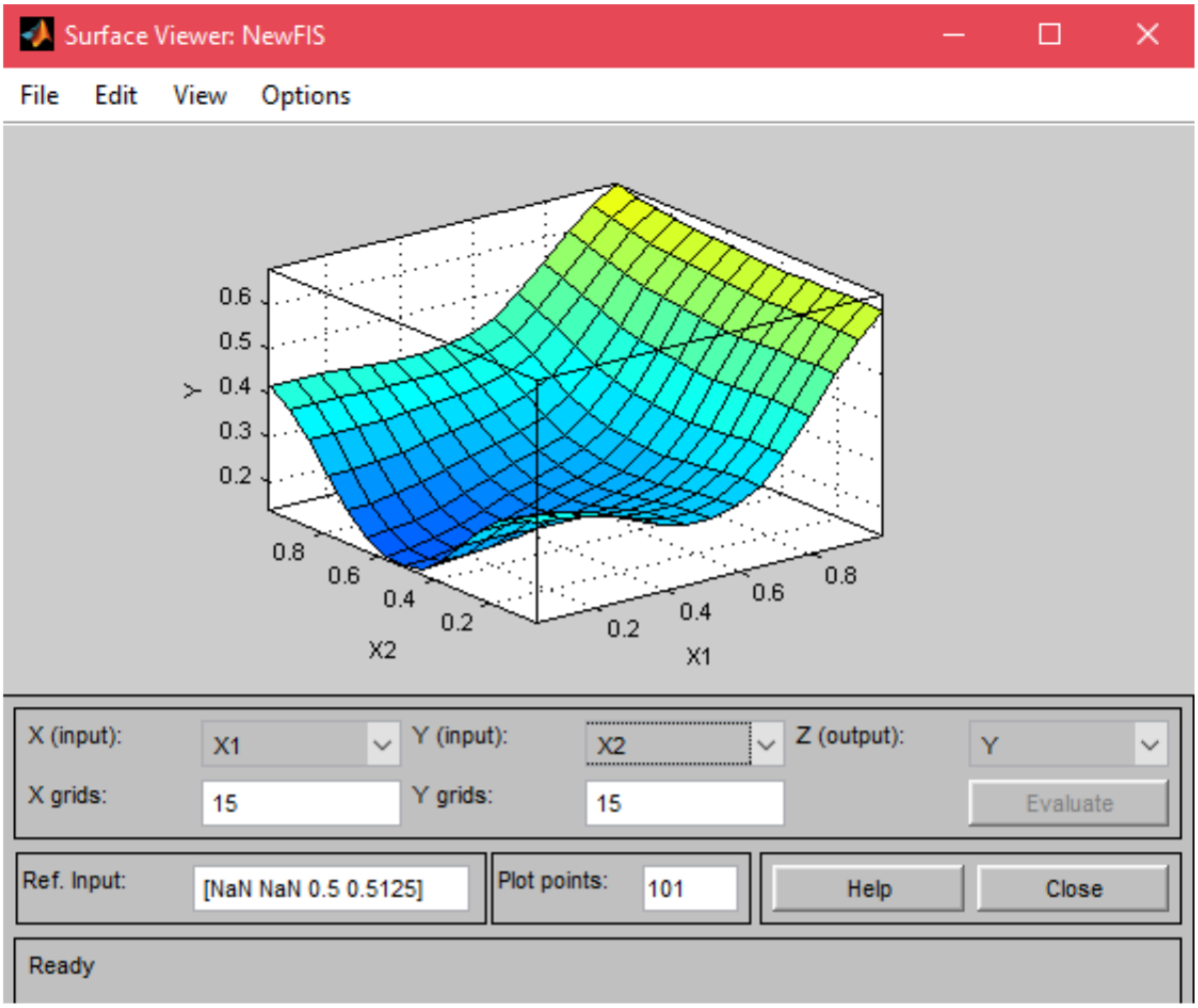

Рисунок 29 – Визуализация поверхности

Следовательно, итоговая выходная оценка приняла значение 0,8. Это говорит о том, что исследуемая ИСПДн соответствует требованиям нормативно-правовых актов на 80%. Данная оценка показывает, что уровень защищённости информационной системы является выше среднего. Для того чтобы система выдавала наиболее высокий результат, следует изменить значение одного из показателей (X2 или X4) с уровня M на уровень L. Таким образом, для данного уровня защищённости ИСПДн дополнительного рассмотрения и проработки требуют показатели сохранности носителей и средства защиты информации, прошедшие процедуру оценки соответствия требованиям нормативно-правовой документации.

ЗАКЛЮЧЕНИЕ

В результате работы над выпускной квалификационной работой было проведено исследование предметной области, которое было представлено описанием процесса проведения аудита информационных систем персональных данных. Были рассмотрены существующие угрозы и способы их классификации. В разделе также были приведены нормативно-правовые документы, регулирующие отношения в области обработки персональных данных. Был проведён сравнительный анализ существующих программных средств, решающих задачи аудита ИСПДн. В пункте описания жизненного цикла программных средств было приведено обоснование выбора модели жизненного цикла. Далее шло описание и выбор программных средств для проектирования и реализации системы поддержки принятия решений.

Второй раздел рассматривал непосредственно процесс проектирования СППР. С помощью методологий UML и IDEF0 были построены модели и диаграммы основных процессов и функций, выполняемых создаваемым программным средством. Диаграммами в методологии UML являлись следующие: диаграмма вариантов использования, последовательности, состояний, активности, а также компонентов. С помощью методологии IDEF0 была спроектирована архитектура системы поддержки принятия решений, отражающая основные функциональные возможности системы.

Третий раздел описывал процесс реализации системы поддержки принятия решений. В нём было представлено описание интерфейса системы, созданного при помощи языка программирования C#, а также модуля интеллектуального анализа данных, который основывался на теории нечёткой логики, использовал для анализа нечёткие нейронные сети и проектировался в среде MATLAB.

Таким образом, были разрешены поставленные задачи:

– возможность описания информационной системы персональных данных и определение уровня её защищённости по исследуемым входным показателям. Информационная система была описана категорией обрабатываемых персональных данных, типом персональных данных, а также моделью угроз По данным входным показателям был выявлен четвёртый уровень защищённости информационной системы персональных данных, а также определены требования к данному уровню защищённости;

– оценка уровня защищённости информационной системы персональных данных в зависимости от предъявляемых к ней требований, в соответствии с нормативной документацией. При введённых значениях выполнимости требований к уровню защищённости была сформирована итоговая оценка уровня защищённости, составившая 80% и говорившая об уровне защищённости выше среднего;

– помощь аудитору в формировании рекомендаций о состоянии защищённости информационной системы.

Система поддержки принятия решений позволит провести анализ любой информационной системы персональных данных и предоставит оценку о состоянии её защищённости в соответствии с нынешней нормативно-правовой документацией.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Аверченков, В. И., Аудит информационной безопасности органов исполнительной власти [Электронный ресурс] : учебное пособие / В. И. Аверченков [и др.]. – Электрон. текстовые данные. – Брянск : Брянский государственный технический университет, 2012 г. – 100 с. – Режим доступа: http://www.iprbookshop.ru/6992.html. – ЭБС «IPRbooks»

2 Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков. – Электрон. текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 268 с. – 978-89838-487-6. – Режим доступа: http://www.iprbookshop.ru/6991.html

3 Аверченков, В. И. Основы математического моделирования технических систем [Электронный ресурс] : учебное пособие / В. И. Аверченков, В. П. Федоров, М. Л. Хейфец. – Электрон. текстовые данные. – Брянск : Брянский государственный технический университет, 2012. – 271 с. – Режим доступа: http://www.iprbookshop.ru/7003.html. – ЭБС «IPRbooks»

4 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : офиц. текст. ФСТЭК, 2008 г. – 69 с.

5 Бармен, Скотт, Разработка правил информационной безопасности : учебное пособие / Скотт Бармен. Вильямс, 2002 г. – 208 с. – ISBN 5-8459-0323-8, ISBN 1-57870-264-X.

6 Бахтизин, В. В., Технология разработки программного обеспечения: учебное пособие / В. В. Бахтизин, Л. А. Глухова. Минск: БГУИР, 2010 г. – 267 с.

7 Биллиг, В. А., Основы объектного программирования на C# (C# 3.0, Visual Studio 2008) [Электронный ресурс] : учебное пособие / В. А. Биллиг. – Электрон. текстовые данные. – Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. – 583 с.

8 Блинов, А. М., Информационная безопасность : учеб. пособие. Часть 1 / А. М. Блинов. СПБГУЭФ, 2010 г. – 96 с.

9 Буч, Грейди, Язык UML. Руководство пользователя = The Unified Modeling Language user guide : учебное пособие / Грейди Буч, Джеймс Рамбо, Айвар Джекобсон. ДМК Пресс, Питер, 2004 г. – 432 с. – ISBN 5-94074-260-2.

10 Буч, Грейди, Краткая история UML // Язык UML. Руководство пользователя = The Unified Modeling Language User Guide : учебное пособие / Грейди Буч, Джеймс Рамбо, Айвар Джекобсон. ДМК Пресс, 2006 г. – С. 14. – 496 с. – ISBN 5-94074-334-X.

11 Галаган, Т. А., Технология разработки программного обеспечения: сборник учебно-методических материалов для направления подготовки 09.04.04 Программная инженерия : учебно-методический материал / Т. А. Галаган. Благовещенск : Амурский государственный университет, 2018 г. – 51 с. 31

12 Гатчин, Ю. А., Теория информационной безопасности и методология защиты информации : учеб. пособие / Ю. А. Гатчин, В. В. Сухостат. СПбГУ ИТМО, 2010 г. – 98 с.

13 Горбань, А. Н., Нейронные сети на персональном компьютере: учебное пособие / А. Н. Горбань, Д. А. Россиев. Новосибирск : Наука, 1996 г. – 276 с. – ISBN 5-02-031196-0.

14 ГОСТ Р ИСО/МЭК 12207–2010, Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств, 2010 г. – 105 с.

15 Громов, Ю. Ю. Представление знаний в информационных системах : учебное пособие / Ю. Ю. Громов [и др.]. Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2012. – 169 с.

16 Гудов, А. М., Технология разработки программного обеспечения : учебное пособие / А. М. Гудов, С. Ю. Завозкин, С. Н. Трофимов. Кемерово : Кемеровский государственный университет, 2009 г. – 138 с.

17 Дмитриева, А. В., Описание модуля системы поддержки принятия решений по проведению аудита информационной системы персональных данных : статья / А. В. Дмитриева, С. Г. Самохвалова. АмГУ, Молодёжь XXI века: шаг в будущее, 2018 г. – 2 с.

18 Дмитриева, А. В., Проектирование и реализация модуля интеллектуального анализа данных для проведения аудита информационных систем персональных данных : статья / А. В. Дмитриева, С. Г. Самохвалова. АмГУ, «Вестник Амурского государственного университета» Серия: Естественные и экономические науки №79, 2017 г. – 7 с. – ISSN-2073-0268.

19 Дмитриева, А. В., Подход в использовании гибридных нейронных сетей при построении системы поддержки принятия решений для помощи в проведении аудита информационных систем персональных данных : статья / А. В. Дмитриева, С. Г. Самохвалова. Электронный журнал «Постулат» №5, №6, 2018 г.–8с.

20 Дьяконов, В. П., MATLAB 6.5/7.0/7 SP1/7 SP2 + Simulink 5/6. Инструменты искусственного интеллекта и биоинформатики. Библиотека профессионала : учебное пособие / В. П. Дьяконов. «СОЛОН-Пресс», 2005 г. – 456 с. – ISBN 5-98003-255-X.

21 Дьяконов, В. П., MATLAB 5 с пакетами расширений : учебное пособие / В. П. Дьяконов, И. В. Абраменкова, В. В. Круглов. Нолидж, 2001 г. – 880 с.

22 Заде, Лютфи., Понятие лингвистической переменной и его применение к принятию приближенных решений : учебное пособие / Лютфи Заде. Мир, 1976 г. – 166 с.

23 Казанский, А. А., Объектно-ориентированное программирование на языке Microsoft Visual C# в среде разработки Microsoft Visual Studio 2008 и .NET Framework. 4.3 [Электронный ресурс] : учебное пособие и практикум / А.А. Казанский. – Электрон. текстовые данные. – Москва: Московский государственный строительный университет, ЭБС АСВ, 2011. – 180 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/19258.html

24 Крат, Ю. Г., Основы информационной безопасности : учеб. пособие / Ю.Г. Крат, И.Г. Шрамкова. Хабаровск : Изд-во ДВГУПС, 2008 г. –112 с. 8

25 Крышкин, О., Настольная книга по внутреннему аудиту: Риски и бизнес-процессы : учебное пособие / Олег Крышкин. Альпина Паблишер, 2013 г. – 477 с. – ISBN 978-5-9614-4449-0.

26 Ларман, Крэг, Применение UML 2.0 и шаблонов проектирования = Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development : учебное пособие / Крэг Ларман. Вильямс, 2006 г. – 736 с. – ISBN 0-13-148906-2.

27 Леоненков, А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH : учебное пособие / А. В. Леоненков. – СПб, БХВ Петербург, 2005. – 736 с.

28 Либерти, Д., Язык программирования C# // Программирование на C# : учебное пособие / Д. Либерти. Санкт-Петербург. Символ-Плюс, 2003 г. – С. 26. – 688 с. – ISBN 5-93286-038-3.

29 Майо, Д., Самоучитель Microsoft Visual Studio 2010 = Microsoft Visual Studio 2010: A Beginner's Guide (A Beginners Guide) : учебное пособие / Д. Майо. «БХВ-Петербург», 2010 г. – 464 с. – ISBN 978-5-9775-0609-0.

30 Мак-Каллок, У. С., Логическое исчисление идей, относящихся к нервной активности : статья / У. С. Мак-Каллок, В. Питтс. Изд-во иностр. лит., 1956 г. – С. 363–384.

31 Макаренко, С. И. Информационная безопасность : учебное пособие для студентов вузов / С. И. Макаренко. Ставрополь : СФ МГГУ им. М. А. Шолохова, 2009 г. – 372 с.

32 Манык, П. В. Правовые основы безопасности виртуальной среды : статья / П. В. Манык. Журнал Information Security. Информационная безопасность, 2016 г. – № 2(35). – 33 с.

33 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных : офиц. текст. ФСТЭК, 2008 г. – 10 с.

34 Миркес, Е. М., Логически прозрачные нейронные сети и производство явных знаний из данных : учебное пособие / Е. М. Миркес, А. Н. Горбань [и др.] Новосибирск : Наука. Сибирское предприятие РАН, 1998 г. – 296 с. – ISBN 5-02-031410-2.

35 Новак, В., Математические принципы нечёткой логики = Mathematical Principles of Fuzzy Logic : учебное пособие / В. Новак, И. Перфильева, И. Мочкрож. Физматлит, 2006 г. – 352 с. – ISBN 0-7923-8595-0.

36 Новиков, А. М., Методология образования. Издание второе [Электронный ресурс] : учебное пособие / А. М. Новиков, Д. А Новиков. – Электрон. текстовые данные. – Москва, СИНТЕГ, 2007. – 668 с.

37 Орловский, С. А., Проблемы принятия решений при нечеткой исход-ной информации : учебное пособие / С. А. Орловский. Наука, 1981 г. – 208 с. 50 38 Петренко, С. А., Аудит безопасности Intranet : учебное пособие / С. А. Петренко, А. А. Петренко. ДМК Пресс, 2002 г. – 406 с.

39 Пилипенко, В. Ф., Безопасность: теория, парадигма, концепция, культура : словарь-справочник / В. Ф. Пилипенко. ПЕР СЭ-Пресс, 2005 г. – 195 с. 40 Постановление правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119, утверждённое 1 ноября 2012 г : офиц. текст – Москва : Кремль, 2012. – 4 с.

41 Приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных», утверждённый в 2013 г. : офиц. текст. ФСТЭК, 2013. – 22 с.

42 Рендольф, Ник, Visual Studio 2010 для профессионалов = Professional Visual Studio 2010 : учебное пособие / Ник Рендольф, Дэвид Гарднер [и др.] «Диалектика», 2011 г. – 1184 с. – ISBN 978-5-8459-1683-9.

43 Рутковская, Д., Нейронные сети, генетические алгоритмы и нечеткие системы : учебное пособие / Д. Рутковская, М. Пилиньский, Л. Рутковский. Горячая линия – Телеком, 2004 г. – 452 с. – ISBN 5-93517-103-1

44 Салова, В. В., Интеллектуальная система поддержки принятия решений по проведению аудита информационных систем персональных данных : статья / В. В. Салова, В. И. Васильев. ФГБОУ ВПО УГАТУ. 2014 г. – 9 с.

45 Самуйлов, С.В. Объектно-ориентированное моделирование на основе UML [Электронный ресурс] : учебное пособие / С.В. Самуйлов. – Электрон. текстовые данные. – Саратов : Вузовское образование, 2016. – 37 с. – 2227-8397. – Режим доступа: http://www.iprbookshop.ru/47277.html

46 Семененко, В. А., Информационная безопасность : учебное пособие / В. А. Семененко. МГИУ, 2004 г. – 215 с. – ISBN 5-8459-0323-8, ISBN 1-57870-264-X.

47 Сысоев, Д. В., Введение в теорию искусственного интеллекта [Электронный ресурс] : учебное пособие / Д. В. Сысоев, О. В. Курипта, Д. К. Проскурин. – Электрон. текстовые данные. – Воронеж : Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – 171 с.

48 Таранчук, В. Б., Основные функции систем компьютерной алгебры : учебное пособие / В. Б. Таранчук. Минск : БГУ, 2013 г. – 59 с.

49 Уотсон, Карли, Visual C# 2008: базовый курс. Visual Studio® 2008 = Beginning Visual C# 2008 : учебное пособие / Карли Уотсон, Кристиан Нейгел [и др.] «Диалектика», 2009 г. – 1216 с. – ISBN 978-5-8459-1532-0.

50 Усков, А. А., Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика : учебное пособие / А. А. Усков, А. В. Кузьмин. Горячая Линия – Телеком, 2004 г. – 143 с.

51 Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных» : офиц. текст – Москва: Кремль, 2006. – 22 с.

52 Федеральный закон от 30 декабря 2008 г. N 307-ФЗ «Об аудиторской деятельности» : офиц. текст – Москва : Кремль, 2008. – 40 с.

53 Хайкин, С., Нейронные сети: полный курс = Neural Networks: A Comprehensive Foundation : учебное пособие / С. Хайкин. Вильямс, 2006 г. – 1104 с. – ISBN 0-13-273350-1.

54 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] : учебник / В. Ф. Шаньгин. – Электрон. текстовые данные. – М. : ДМК Пресс, 2010. – 544 с. – Режим доступа: http://www.iprbookshop.ru/7943.– ЭБС «IPRbooks»

55 Шилдт, Герберт. Полный справочник по C# = C#: The Complete Reference : учебное пособие / Герберт Шилдт. Издательский дом «Вильямс», 2004 г. – С. 26–27. – 752 с.

56 Широкова, Г. В., Концепция жизненного цикла в современных организационных и управленческих исследованиях : статья / Г. В. Широкова, Т. Н. Клемина, Т. П. Козырева. Вестник Санкт-Петербургского университета. Серия «Менеджмент». Сер. 8. Вып. 2, 2007 г, с. 3–31

57 Штовба, С. Д., Проектирование нечетких систем средствами MATLAB : учебное пособие / С. Д. Штовба. Горячая линия – Телеком, 2007 г. – 288 с.

58 Ярочкин, В. И. Информационная безопасность: учебник для студентов : учебное пособие / В. И. Ярочкин. Академический Проект; Гаудеамус, 2-е изд., 2004 г. – 544 с.

59 Ясницкий, Л. Н., Введение в искусственный интеллект : учебное пособие / Л. Н. Ясницкий. Издат. центр «Академия», 2005. – 176 с. – ISBN 5-7695-1958-4.

ПРИЛОЖЕНИЕ А

Таблица А – Классификация информационных систем по уровням защищённости

Тип обрабатываемых ИСПДн ПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1 (НДВ ОС)	2 (НДВ ПО)	3 (Без НДВ)
ИСПДн-С (специальные)	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б (биометрические)			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И (иные)	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О (общедоступные)	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				

ПРИЛОЖЕНИЕ Б

Таблица Б – Требования к уровням защищённости

Требования	Уровни защищенности			
	1	2	3	4
Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
Обеспечение сохранности носителей персональных данных	+	+	+	+
Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз	+	+	+	+
Назначение должностного лица, ответственного за обеспечение безопасности персональных данных в ИСПДн	+	+	+	-
Ограничение доступа к содержанию электронного журнала сообщений	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе	+	-	-	-
Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности	+	-	-	-

ПРИЛОЖЕНИЕ В

Схема реализации программных модулей

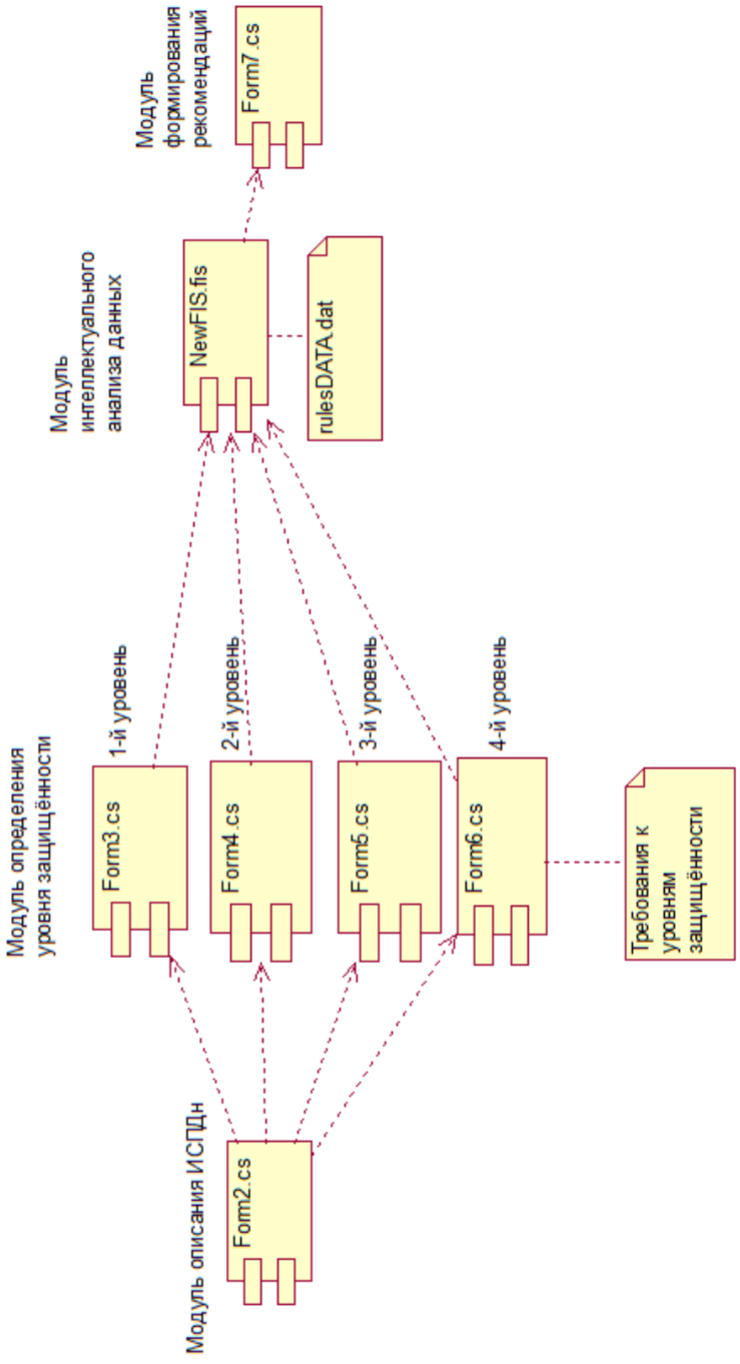

Рисунок В – Схема реализации программных модулей

ПРИЛОЖЕНИЕ Г

База правил для нечёткой нейронной сети

	A	B	C	D	E	F
1		Входные факторы				
2	№	X1	X2	X3	X4	Y
3	1	S	S	S	S	S
4	2	S	S	L	M	M
5	3	S	S	S	L	SM
6	4	S	S	L	S	SM
7	5	S	S	S	M	SM
8	6	S	S	L	L	M
9	7	S	M	S	S	SM
10	8	S	M	L	M	M
11	9	S	M	S	L	M
12	10	S	M	L	S	M
13	11	S	M	S	M	SM
14	12	S	M	L	L	M
15	13	S	L	S	S	SM
16	14	S	L	L	M	M
17	15	S	L	S	L	M
18	16	S	L	L	S	M
19	17	S	L	S	M	M
20	18	S	L	L	L	M
21	19	M	S	S	S	SM
22	20	M	S	L	M	M
23	21	M	S	S	L	M
24	22	M	S	L	S	M
25	23	M	S	S	M	SM
26	24	M	S	L	L	M
27	25	M	M	S	S	SM
28	26	M	M	L	M	ML
29	27	M	M	S	L	M
30	28	M	M	L	S	M
31	29	M	M	S	M	M
32	30	M	M	L	L	ML
33	31	M	L	S	S	M
34	32	M	L	L	M	ML
35	33	M	L	S	L	M

Рисунок Г.1 – База правил для нечёткой нейронной сети

36	34	M	L	L	S	M
37	35	M	L	S	M	M
38	36	M	L	L	L	L
39	37	L	S	S	S	SM
40	38	L	S	L	M	M
41	39	L	S	S	L	M
42	40	L	S	L	S	M
43	41	L	S	S	M	M
44	42	L	S	L	L	M
45	43	L	M	S	S	M
46	44	L	M	L	M	ML
47	45	L	M	S	L	M
48	46	L	M	L	S	M
49	47	L	M	S	M	M
50	48	L	M	L	L	L
51	49	L	L	S	S	M
52	50	L	L	L	M	L
53	51	L	L	S	L	M
54	52	L	L	L	S	M
55	53	L	L	S	M	M
56	54	L	L	L	L	L

Рисунок Г.2 – Продолжение базы правил для нечёткой нейронной сети

ПРИЛОЖЕНИЕ Д

Обучающая выборка для нечёткой нейронной сети

№	X1	X2	X3	X4	Y
1	0.289	0.049	0	0.208	0.013
2	0.162	0.073	1	0.301	0.43
3	0.044	0.147	0	0.97	0.14
4	0.189	0.254	1	0.26	0.27
5	0.17	0.149	0	0.82	0.205
6	0.28	0.146	1	0.983	0.37
7	0.245	0.891	0	0.116	0.208
8	0.042	0.573	1	0.831	0.555
9	0.15	0.673	0	0.953	0.62
10	0.115	0.585	1	0.093	0.611
11	0.266	0.581	0	0.643	0.283
12	0.262	0.844	1	0.948	0.38
13	0.119	0.955	0	0.271	0.153
14	0.138	0.917	1	0.645	0.329
15	0.134	0.919	0	0.961	0.67
16	0.178	0.925	1	0.185	0.591
17	0.204	0.93	0	0.379	0.547
18	0.179	0.912	1	0.959	0.443
19	0.781	0.055	0	0.099	0.127
20	0.376	0.038	1	0.856	0.552
21	0.674	0.179	0	0.912	0.535
22	0.31	0.102	1	0.139	0.341
23	0.562	0.103	0	0.415	0.203
24	0.54	0.148	1	0.966	0.54
25	0.428	0.535	0	0.109	0.259
26	0.802	0.493	1	0.798	0.827
27	0.416	0.572	0	0.903	0.624
28	0.687	0.899	1	0.196	0.566
29	0.753	0.35	0	0.415	0.485
30	0.728	0.841	1	0.916	0.719
31	0.4	0.98	0	0.242	0.426
32	0.754	0.918	1	0.63	0.709
33	0.41	0.976	0	0.995	0.412
34	0.419	0.97	1	0.235	0.534
35	0.363	0.902	0	0.39	0.694

Рисунок Д.1 – Обучающая выборка для нечёткой нейронной сети

```
36 0.74  0.996  1  0.914 0.926
37 0.972 0.273  0  0.092 0.272
38 0.996 0.113  1  0.797 0.687
39 0.943 0.196  0  0.931 0.488
40 0.923 0.295  1  0.064 0.337
41 0.983 0.225  0  0.525 0.558
42 0.921 0.158  1  0.999 0.53
43 0.997 0.68   0  0.03  0.544
44 0.93  0.738  1  0.589 0.803
45 0.907 0.687  0  0.957 0.598
46 0.949 0.649  1  0.209 0.48
47 0.923 0.513  0  0.653 0.684
48 0.911 0.613  1  0.923 0.956
49 0.97  0.915  0  0.082 0.548
50 0.956 0.931  1  0.706 0.968
51 0.989 0.99   0  0.9   0.526
52 0.901 0.935  1  0.026 0.494
53 0.938 0.965  0  0.4   0.539
54 0.903 0.974  1  0.982 0.988
```

Рисунок Д.2 – Продолжение обучающей выборки для нечёткой нейронной сети

ПРИЛОЖЕНИЕ Е

Техническое задание на проектирование

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование системы

1.1.1 Полное наименование системы

Полное наименование: «Система поддержки принятия решений по проведению аудита информационных систем персональных данных».

1.1.2 Краткое наименование системы

Краткое наименование: СППР по проведению аудита ИСПДн.

1.2 Основания для проведения работ

Основанием для проведения работ являются следующие материалы:

– ГОСТ 34.602-89 – техническое задание на проектирование автоматизированной системы управления;

– требования к системе.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Разрабатываемая система поддержки принятия решений предназначена для помощи в проведении аудита информационной системы персональных данных, а именно для выявления качественной оценки уровня защищенности существующей ИСПДн.

2.2 Цели создания системы

Целью работы является создание интеллектуальной системы поддержки принятия решений для помощи в проведении аудита, а именно – описание ИСПДН, построение моделей угроз и злоумышленников, оценка текущего уровня защищенности информационной системы персональных данных и формирование рекомендаций по улучшению состояния защищенности.

3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

Объектом автоматизации проектируемой системы является процесс аудита существующей ИСПДн, которую требуется проинспектировать, описать, выявить для нее уровень защищенности и дать ему количественную оценку.

Аудит информационных систем персональных данных – это один из механизмов обеспечения информационной безопасности.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

Проектируемая система поддержки принятия решений будет выполнять следующие функции:

– составление описания исследуемой информационной системы персональных данных;

– классификация исследуемой информационной системы персональных данных по уровням защищенности;

– построение моделей угроз и злоумышленников;

– оценка уровня защищенности информационной системы персональных данных;

– выработка рекомендаций по повышению показателей уровня защищенности исследуемой информационной системы персональных данных.

4.1.1 Требования к структуре и функционированию системы

В Системе предлагается выделить следующие функциональные подсистемы:

– подсистема сбора и обработки данных, которая предназначена для накопления сведений о персональных данных, обрабатываемых ИСПДн, и приведения их к требуемому виду;

– подсистема построения моделей угроз и злоумышленников, которая предназначена для анализа состояния ИСПДн и построения на основании сведений о ней моделей угроз и злоумышленников;

– подсистема определения уровня защищенности ИСПДн, которая предназначена для анализа персональных данных и моделей угроз, и на их основании определения текущего уровня защищенности;

– подсистема интеллектуального анализа данных, которая предназначена для определения оценки защищенности информационной системы.

– подсистема формирования рекомендаций для повышения уровня защищенности информационной системы.

4.1.2 Требования к численности и квалификации персонала системы и режиму его работы

4.1.2.1 Требования к численности персонала

В состав персонала необходимо выделение следующих лиц: пользователь – аудитор – 1 человек.

Данное лицо должно выполнять следующие функциональные обязанности: аудитор выполняет первичную загрузку исходных сведений о персональных данных, а также сведений об ИСПДн в СППР, проверяет полученные данные в ходе работы каждого модуля системы, корректирует их, если необходимо.

4.2 Требования к функциям, выполняемым системой

4.2.1 Подсистема сбора и обработки данных

Функции, подлежащие автоматизации:

– приведение первичных данных – сведения о персональных данных, сведения об ИСПДн к требуемому виду;

– идентификация ИСПДн: определение категории ПДн и их объем;

– предварительная обработка данных об ИСПДн: определение требований к ИСПДн.

4.2.2 Подсистема определения уровня защищенности ИСПДн

Функция, подлежащая автоматизации: на основании сведений о персональных данных и модели угроз и злоумышленников определение уровня защищенности ИСПДн и отнесение ее к конкретному классу ИСПДн.

4.2.3 Подсистема интеллектуального анализа данных

Функция, подлежащая автоматизации: на основании текущего уровня защищенности ИСПДн и выявленным требованиям к ИСПДн определение оценки защищенности ИСПДн при помощи модульной нейронной сети.

4.2.4 Подсистема формирования рекомендаций

Функция, подлежащая автоматизации: на основании полученного показателя – оценки защищенности ИСПДн формирование рекомендаций по улучшению состоянии безопасности ИСПДн.

4.3 Требования к видам обеспечения

4.3.1 Требования к математическому обеспечению

Математическое обеспечение предъявляется к подсистеме интеллектуального анализа данных. Используется теория нечеткой логики для построения системы правил и далее – нечеткой нейронной сети.

Для построения обучающей выборки нейронной сети используется метод Монте-Карло.

4.3.3 Требования к лингвистическому обеспечению

Для реализации подсистемы интеллектуального анализа данных должен использоваться язык пакета MATLAB, в частности язык графического редактора ANFIS.

Для организации диалога системы с пользователем должен применяться графический оконный пользовательский интерфейс. Данный интерфейс должен быть написан на языке C# с использованием программной среды Microsoft Visual Studio.

4.3.4 Требования к техническому обеспечению

Система должна быть реализована с использованием специально выделенного сервера Заказчика.

4.3.5 Требования к методическому обеспечению

В состав входят следующие компоненты:

– Федеральный закон «О персональных данных»: 27 июля 2006 г. №152-ФЗ;

– Приказ «Об утверждении порядка проведения классификации информационных систем персональных данных»: утвержден ФСТЭК России 2008 г.;

– Постановление правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: утверждено 2012 г. №1119.

4.3.6 Требования к патентной чистоте

Обзор существующей литературы по предметной области выявил отсутствие систем-аналогов.

5 ИСТОЧНИКИ РАЗРАБОТКИ

Техническое Задание было разработано на основании следующих документов и информационных материалов:

– Федеральный закон «О персональных данных»: 27 июля 2006 г. №152-ФЗ;

– Приказ «Об утверждении порядка проведения классификации информационных систем персональных данных»: утвержден ФСТЭК России 2008 г.;

– Постановление правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: утверждено 2012 г. №1119;