Министерство образования и науки 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 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2017 г.

БАКАЛАВРСКАЯ РАБОТА

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

Исполнитель
студент группы 355-об _____ (подпись, дата) А.В. Дмитриева

Руководитель
доцент, канд. техн. наук _____ (подпись, дата) С.Г. Самохвалова

Консультант
по безопасности и
экологичности
доцент, канд. техн. наук _____ (подпись, дата) А.Б. Булгаков

Нормоконтроль
инженер кафедры _____ (подпись, дата) В.В. Романико

Благовещенск 2017

Министерство образования и науки 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
«_____»_____2017 г.

З А Д А Н И Е

К бакалаврской работе студента Дмитриевой Анастасии Витальевны

1. Тема бакалаврской работы: Проектирование и реализация модуля 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 бакалаврской работе: предметная область, нормативно-правовая документация, перечень литературы

4. Содержание бакалаврской работы (перечень подлежащих разработке вопросов):

1) анализ предметной области;

2) описание системы поддержки принятия решений;

3) проектирование и реализация модуля системы поддержки принятия решений;

4) безопасность и экологичность

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

а) организационная структура ФГБОУ ВО «АмГУ» Факультета математики и информатики;

б) информационные потоки ФГБОУ ВО «АмГУ» деканата Факультета математики и информатики;

в) классификация ИСПДн по уровням защищённости;

г) требования к уровням защищённости;

д) архитектура системы поддержки принятия решений;

е) база правил для нечёткой нейронной сети;

ж) обучающая выборка для нечёткой нейронной сети;

и) техническое задание на проектирование

6. Консультанты по бакалаврской работе (с указанием относящихся к ним разделов) консультант по части безопасности и экологичности: Булгаков А.Б., доцент, канд. техн. наук

7. Дата выдачи задания _____г.

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

Задание принял к исполнению (_____г.): _____

(подпись студента)

РЕФЕРАТ

Бакалаврская работа содержит 63 страницы, 28 рисунков, 4 таблицы, 23 источника.

АУДИТ, ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ, УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, НЕЧЁТКАЯ ЛОГИКА, ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ ДАННЫХ, НЕЙРОННАЯ СЕТЬ, ГИБРИДНАЯ СЕТЬ

В бакалаврской работе ставится задача исследования объекта защиты – информационной системы деканата факультета математики и информатики ФГБОУ ВО «Амурского государственного университета», а также проектирования и реализации модуля системы поддержки принятия решений по проведению процесса аудита данной информационной системы персональных данных, который представляет собой модульную нейронную сеть и реализует функцию интеллектуального анализа данных.

Модуль интеллектуального анализа данных базируется на теории нечёткой логики. В качестве входных данных будут использованы требования к уровню защищённости информационной системы персональных данных, а именно степень соответствия реальных показателей требований требуемым. Задача данного модуля: оценка текущего уровня защищённости.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

ФГБОУ ВО «АмГУ» – Федеральное государственное бюджетное общеобразовательное учреждение высшего образования «Амурский государственный университет»;

ИБ – информационная безопасность;

НДВ – недекларированные возможности;

ОС – операционная система;

ПО – программное обеспечение;

ПДн – персональные данные;

ИСПДн – информационная система персональных данных;

СППР – система поддержки принятия решений;

УП – учебный план;

ИИ – искусственный интеллект;

DFD – Data Flows Diagram (диаграмма потоков данных);

FIS – Fuzzy Inference System (система нечёткого вывода);

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

СанПиН – санитарные правила и нормы;

ПЭВМ – персональная электронная вычислительная машина.

ВВЕДЕНИЕ

В настоящее время проблема обеспечения информационной безопасности персональных данных становится одной из ключевых. Персональные данные представляют собой информационные ресурсы, которые непосредственно задействованы во многих сферах жизни общества и всего государства. Информационные системы создаются чаще всего для выполнения функций, связанных с обработкой персональных данных. Но не всегда эти системы соответствуют заявленным требованиям. Эффективность работы данных систем оценивается при помощи проведения аудита.

Аудит информационных систем персональных данных – это один из механизмов обеспечения информационной безопасности. Основной целью данного мероприятия является оценка уровня защищённости системы и выработки конкретных рекомендаций для повышения оценки информационной безопасности и, соответственно, для дальнейшего совершенствования функционала и обеспечивающих подсистем.

Существуют различные виды аудита. Например, такие как активный аудит – данный вид аудита оперативно реагирует на подозрительную активность и предоставляет средства автоматического реагирования на неё. Аудит на соответствие стандартам проводит оценки на основании определённых стандартов, в которых приведено некоторое абстрактное описание, которому исследуемая система должна соответствовать.

Наиболее эффективным и совершенным видом аудита является так называемый экспертный аудит. При проведении данного вида аудита наиболее подробно и во всех аспектах исследуется информационная система. Выявляются существенные недостатки в топологии сети, информационных технологиях, которые могут снижать показатели защищённости. Также необходимо проанализировать все основные информационные потоки исследуемой системы, определить перечень информации, подлежащей защите, и модель угроз, соответствующую конкретному объекту защиты.

Результатом проведения данного вида аудита является подробный перечень рекомендаций, а также оценки показателей, по которым необходимо проанализировать и оценить исследуемую систему.

Для помощи аудитору в проведении экспертного аудита может быть создана система поддержки принятия решений, которая сможет оценить показатели защищённости конкретной информационной системы персональных данных и в соответствии с этим помочь в выработке рекомендаций по улучшению данных показателей.

В рамках данной работы будет рассмотрен и реализован один из модулей системы поддержки принятия решений – модуль интеллектуального анализа данных, основанный на теории нечёткой логики и реализующий функцию определения оценки показателей защищённости информационной системы персональных данных.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Организационная структура объекта исследования

Данный раздел отражает предметную область – объект исследования, для которого будет разработана подсистема системы поддержки принятия решений. Организационную систему управления предприятием можно определить как совокупность следующих подсистем: организационной структуры и организационного механизма предприятия.

Организационная структура определяет расположение всех элементов и ресурсов: что, кто и где находится внутри предприятия.

Организационный механизм определяет связи и взаимодействие уже существующих элементов и ресурсов: кто, когда и как должен делать с кем и с чем взаимодействовать, что использовать [1].

Объектом исследования в данной работе представлена информационная система деканата факультета математики и информатики ФГБОУ ВО «Амурского государственного университета».

Организационная структура, рассматривающая факультет по отношению к внешним составляющим Университета, отражена в приложении А.

Согласно уставу ФГБОУ ВО «АмГУ», Университет имеет следующие основные виды деятельности:

1) образовательная деятельность по образовательным программам высшего образования и среднего профессионального образования, основным общеобразовательным программам, основным программам профессионального обучения, дополнительным профессиональным программам и дополнительным общеобразовательным программам;

2) научная деятельность;

3) организация проведения общественно значимых мероприятий в сфере образования и науки [2].

Единоличным исполнительным органом Университета является ректор Университета, который осуществляет текущее руководство деятельностью

Университета. Учёный совет Университета является коллегиальным органом, осуществляющим общее руководство Университетом. Руководят отдельными направлениями деятельности Университета проректоры. В подчинении у проректора по учебной работе находятся факультеты Университета, управление по воспитательной и внеучебной работе и центр содействия трудоустройству выпускников и студентов. Проректор по научной работе связан с научной деятельностью вуза. В подчинении проректора по информатизации и новым образовательным технологиям находится деятельность, связанная с дополнительным образованием, в частности общеобразовательный лицей, а также центр информационных и образовательных технологий. В подчинении главного бухгалтера находится деятельность бухгалтерии, которая решает все основные финансовые вопросы.

В подчинении декана находится факультет математики и информатики. В состав факультета входят три кафедры: кафедра математического анализа и моделирования, кафедра общей математики и информатики и кафедра информационных и управляющих систем. За каждой кафедрой закреплён заведующий кафедрой.

1.2 Описание процессов и информационных потоков объекта защиты

Для описания процессов объекта защиты необходимо в данной работе применить структурный анализ, который представляет собой метод исследования системы, которое начинается с ее общего обзора и затем детализируется, приобретая иерархическую структуру со все большим числом уровней. Для таких методов характерно разбиение на уровни абстракции с ограничением числа элементов на каждом из уровней (обычно от 3 до 6-7); ограниченный контекст, включающий лишь существенные на каждом уровне детали; дуальность данных и операций над ними; использование строгих формальных правил записи; последовательное приближение к конечному результату [3].

Для описания процессов и документооборота используется диаграмма потоков данных (DFD – Data Flows Diagram). С помощью данной диаграммы функциональные требования моделируемой системы разбиваются на функцио-

нальные компоненты (процессы) и представляются в виде сети, связанной потоками данных [4].

На рисунке Б.1 приложения Б отражены основные внешние информационные потоки. Внешними сущностями на данной диаграмме выступают:

1) ректор;

2) проректор по учебной работе;

3) студенты;

4) преподаватели.

Так работу каждого процесса деканата регламентируют приказы, поступающие от ректора и проректоров по соответствующим направлениям деятельности. В виде выходных потоков проректору по учебной работе приходит отчётность о проделанной работе:

1) отчёты по воспитательной работе;

2) отчёты по успеваемости;

3) отчёты по посещаемости;

4) отчёты о назначенной стипендии.

При поступлении в учебное заведение студенты обязаны заполнить специальную форму заявления на поступление, где указывают личные сведения. Также преподаватели при вступлении в должность дают свои персональные данные для обработки.

Рисунок Б.2 приложения Б показывает внутренние потоки данных и основные процессы, соответствующие работе информационной системе деканата факультета. Деканат ФМиИ выполняет следующие работы:

1) формирование групп студентов;

2) создание рабочих учебных планов и заявок на учебные поручения;

3) учёт посещаемости студентов;

4) учёт успеваемости студентов;

5) назначение стипендии по итогам сданной сессии;

6) формирование отчётности.

Все процессы напрямую взаимодействуют с информационной системой деканата, которая на схеме представлена в виде хранилища данных «База данных деканата ФМиИ».

Заявления на поступление от абитуриентов, попадает в работу «формирование групп студентов». Сведения о профессорско-преподавательском составе попадают в процессы «Формирование групп студентов» и «Создание рабочих учебных планов и заявок на учебные поручения». Приказы ректора распространяются на все работы. Выходы к внешним сущностям исходят из процессов «Назначение стипендии по итогам сданной сессии», «Формирование отчётности», а также из «Формирования групп студентов» при оповещении поступивших студентов.

В базу данных по работе каждого процесса приходят следующие типы входных данных:

1) данные о группах студентов;

2) данные по УП (учебным планам) и расписаниям;

3) данные о посещаемости;

4) данные об успеваемости студентов;

5) данные о стипендиях.

Выходные данные из БД для каждого процесса:

1) данные о группах студентов;

2) данные по дисциплинам;

3) входные данные для создания отчётности, являющиеся объединением всех входных данных по каждому процессу.

Рисунок Б.3 приложения Б показывает декомпозицию первого из процессов – «Формирование групп студентов». Основные работы данного процесса:

1) приём заявления на поступление;

2) формирование списков зачисленных студентов;

3) разделение студентов на группы по направлениям подготовки.

Преподаватели от факультета участвуют в приёмной комиссии и принимают заявления от абитуриентов на поступление. По прошествии конкурса

формируются списки зачисленных, а на их основании затем формируется приказ на зачисление студентов. Студенты разделяются на группы в зависимости от направления подготовки, на которое они поступили. К каждой сформированной группе ставится куратор.

Рисунок Б.4 приложения Б отражает декомпозицию процесса «Создание рабочих учебных планов и заявок на учебные поручения». Здесь можно выделить следующие работы:

1) создание рабочего учебного плана;

2) распределение групп студентов для составления заявок на учебные поручения;

3) согласование сформированного рабочего УП и заявок на учебные поручения;

Для создания рабочего учебного плана используется список дисциплин, соответствующий каждой отдельной учебной группе. В нём определяется требуемая нагрузка для студентов, количество часов, а также метод оценивая полученных в итоге знаний: зачёт или экзамен. Дисциплины из плана распределяются на соответствующие кафедры, то есть формируются созданные рабочие УП и заявки на учебные поручения. После этого созданные рабочие УП и заявки согласуются.

На рисунке Б.5 приложения Б изображена декомпозиция процесса «Учёт посещаемости студентов». В ней можно выделить следующие работы:

1) сбор списков посещаемости;

2) подсчёт количества пропусков;

3) формирование итоговых данных по посещаемости;

Преподаватели ведут списки посещаемости в специализированных журналах. Всю эту информацию собирают для базы данных деканата, где после этого ведётся подсчёт количества пропущенных студентами занятий. Информация окончательно формализуется, согласовывается и далее поступает в виде входных данных в процесс «формирование отчётности».

На рисунке Б.6 приложения Б отражена декомпозиция процесса «Учёт успеваемости студентов». Выделяются следующие работы:

1) сбор ведомостей по итогам аттестаций;

2) составление графика проведения сессий;

3) сбор ведомостей по итогам сданной сессии;

4) формализация накопленных сведений.

Каждый семестр студентам необходимо проходить академические аттестации для выявления текущего уровня успеваемости. Ведомости по итогам аттестаций собираются и фиксируются в базе данных.

Информационная система также фиксирует графики проведения сессий, которые складываются из информации учебного плана и время проведения экзамена. По итогам сданной сессии формируются экзаменационные ведомости, заполняемые преподавателями. Информация по ведомостям поступает в базу данных деканата. После все сведения об успеваемости формализуются, поступают на вход следующего процесса, а также на вход работы «формирование отчётности».

На рисунке Б.7 приложения Б показана декомпозиция процесса «Назначение стипендии по итогам сданной сессии». В этом процессе задействованы следующие работы:

1) отбор студентов с хорошей и отличной успеваемостью;

2) отбор студентов для социальной стипендии;

3) обработка сведений по стипендиям для передачи их в бухгалтерию.

По сведениям, поступившим с предыдущего процесса, – данным об успеваемости студентов осуществляется анализ и отбор студентов с хорошей и отличной успеваемостью (а именно тех, кто сдал сессию на 4 и 5), после этого проходит отбор тех студентов, кто обязан получать социальную стипендию (эти сведения также отражены в базе данных). Полученная информация формализуется и отправляется в бухгалтерию, а также в виде отчётности – проректору по учебной работе.

Итоговая работа «Формирование отчётности» собирает данные о проделанной работе по всем процессам, отправляя отчётные сведение проректору по учебной работе.

1.3 Перечень информации, обрабатываемой информационной системой объекта исследования и подлежащей защите

В данном разделе приводится перечень информации, которая обрабатывается информационной системой вуза и которая подлежит защите.

Информация, подлежащая защите, составляет государственную тайну, а также конфиденциальные сведения.

В соответствии с «Перечнем сведений конфиденциального характера», утвержденным Указом Президента РФ от 6.03.97г. №188. К сведениям конфиденциального характера данный перечень относит:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским Кодексом РФ и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

5) сведения, связанные с коммерческой деятельностью; доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них [5].

Следовательно, защите подлежат конфиденциальные сведения, составляющие персональные данные.

Персональные данные поступают в информационную систему от заявлений на поступление абитуриентов, где указывается основная, идентифицирующая человека информация. Также персональные сведения поступают от сотрудников деканата при оформлении трудового договора и устройства на работу.

Перечень персональных данных студентов:

1) фамилия, имя, отчество;

2) дата рождения;

3) адрес проживания (адрес прописки и реальный);

4) контактный телефон;

5) паспортные данные (серия, номер, год выдачи, кем выдан);

6) информация об образовании;

7) прочие данные.

Перечень персональных данных сотрудников:

1) фамилия, имя, отчество;

2) дата рождения;

3) адрес проживания;

4) контактный телефон;

5) паспортные данные;

6) информация об образовании (наименования образовательного учреждения, специальность, дата начала и дата окончания обучения);

7) учёная степень, должность, учёное звание;

8) информация о трудовом стаже (место работы, должность, период работы);

9) данные о повышении квалификации.

Федеральный закон «О персональных данных» №152-ФЗ трактует понятие «персональные данные» следующим образом: персональные данные — любая информация, относящаяся к прямо или косвенно определенному или опре-

деляемому физическому лицу (субъекту персональных данных). Конфиденциальность персональных данных трактуется в соответствии с данным законом: Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом [6].

1.4 Основные угрозы объекта исследования

Под угрозой безопасности понимается возможность воздействия на информационную систему, которое прямо или косвенно может нанести ущерб её безопасности. Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе защиты [7].

Существует три основных типа угроз: угрозы, обусловленные действиями субъекта (антропогенные); угрозы, обусловленные техническими средствами (техногенные); угрозы, обусловленные стихийными источниками.

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:

1) внешние:

а) криминальные структуры;

б) представители надзорных организаций и аварийных служб;

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

2) внутренние:

а) основной персонал;

б) представители службы безопасности;

в) вспомогательный персонал (уборщики).

Конкретно для данного предприятия в качестве основных антропогенных источников угроз можно выделить следующие: основной персонал, вспомогательный персонал.

К техногенным источникам угроз относятся следующие:

1) некачественные основные технические средства;

2) некачественное периферийное оборудование;

3) некачественная поддерживающая инфраструктура.

Для данного объекта исследования можно выделить основные техногенные источники угроз: сбои в работе основных технических средств, сбои в работе периферийного оборудования.

Естественные источники угроз следующие:

1) пожары;

2) наводнения;

3) землетрясения;

4) стихийные бедствия;

5) радиоактивное излучение;

6) различного рода форс-мажорные обстоятельства.

Для данного предприятия свойственны следующие естественные источники угроз: пожары, различного рода форс-мажорные обстоятельства.

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

1) акустический;

2) вибро-акустический;

3) оптико-визуальный;

4) побочные электромагнитные излучения и наводки;

5) другие каналы утечки информации.

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

Помимо этого, невозможно точно спрогнозировать поведение системы в момент воздействия на неё нарушителя.

Из этого следует, что система может находиться в безопасном состоянии только при принятии мер по устранению всевозможных реализаций угроз.

1.5 Понятие аудита информационных систем персональных данных

Аудит – процесс получения качественных и количественных оценок о текущем состоянии информационной безопасности организации, компании в соответствии с определенными критериями и показателями безопасности [8].

Процесс аудита регулируется Федеральным законом №307 «Об аудиторской деятельности».

Аудит предназначен для оценки состояния информационной системы и разработки рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных ресурсов информационной системы от угроз информационной безопасности [9].

Можно выделить следующие цели проведения аудита:

1) анализ возможных рисков, связанных с реализацией угроз в отношении информационных ресурсов;

2) оценка текущего уровня защищённости информационной системы;

3) оценка соответствия текущего состояния защищённости требуемому в соответствии с нормативно-правовыми актами;

4) поиск слабых мест в системе защиты;

5) выработка соответствующих рекомендаций по повышению уровня безопасности системы.

Аудит информационных систем персональных данных подразумевает собой исследование информационной системы на основании документов, регулирующих отношения в области обработки персональных данных, которые рассматриваются в следующем разделе.

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

Первым основополагающим документом в области обработки ПДн является Федеральный закон №152 «О персональных данных». Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной

власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств [6]. Он даёт основные понятия, касающиеся ПДн, определяет основные принципы и условия обработки ПДн, даёт пояснения, касательно обработки специальных категорий ПДн, а также биометрических ПДн. Помимо этого он описывает права субъектов ПДн, а также обязанности операторов при осуществлении процессов обработки ПДн.

Следующим не менее 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 [10]. Данный документ определяет типы актуальных угроз, характерные для той или иной ИСПДн:

1) угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе;

2) угрозы 2-го типа актуальны для информационной системы, если для неё в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе;

3) угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недек-

ларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Далее Постановление устанавливает 4 уровня защищённости для ИСПДн, в соответствии с категорией обрабатываемых ПДн, актуальных угроз и количества субъектов ПДн (в зависимости от формы отношений между организацией и субъектами). Выделяются следующие категории обрабатываемых ПДн:

1) биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

2) специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

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

4) иные категории персональных данных – персональные данные, не относящиеся к первым трём пунктам.

Помимо этого разделяют ИСПДн по количеству субъектов ПДн:

1) менее 100 000 субъектов;

2) более 100 000 субъектов.

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 В.

В этом же постановлении рассматриваются требования для обеспечения того или иного уровня защищённости. Взаимосвязь требований к обеспечению ИБ ИСПДн с уровнями защищённости отражена в таблице Приложения Г.

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»: Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных [11]. Данный документ рассматривает такие меры, как: механизмы идентификации и аутентификации, управление доступом, различные виды антивирусной защиты, контроль обеспечения целостности данных и другие. 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 системах 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.

Второй документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных». В данном документе рассматриваются угрозы утечки информации по техническим каналам, угрозы несанкционированного доступа к информационным ресурсам, а также приведены типовые модели угроз для различных видов ИСПДн.

Объект исследования – вуз, также содержит локальные нормативные документы, касающиеся обработки персональных данных.

1) политика в отношении обработки персональных данных в ФГБОУ ВО «Амурский государственный университет»;

2) положение ПОД СМК 18-2016 Об обработке персональных данных в ФГБОУ ВО «АмГУ».

Первый документ отражает следующие принципы построения системы безопасности ПДн:

1) минимизация информации о ПДн – университет обрабатывает ПДн, предоставленные самим субъектом, при этом формы, предложенные Университетом для заполнения, содержат перечень необходимых и достаточных сведений о ПДн для достижения целей взаимодействия Университета с субъектом (минимальный набор);

2) законность – предполагает осуществление защитных мероприя-тий и разработку системы безопасности ПДн в соответствии с действующим законодательством, направленном на защиту ПДн и сохранения конфиденциальности ПДн;

3) системность – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий, и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

4) комплексность – предполагает согласованное применение разнородных средств при построении целостной системы защиты;

5) непрерывность защиты – направлена на предотвращения глубокого анализа злоумышленниками применяемых средств защиты и в результате предотвращение внедрения средств преодоления защиты;

6) своевременность – предполагает утверждающий характер мер обеспечения безопасности ПДн;

7) разумная достаточность – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения;

8) персональная ответственность – предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника на основании полученного им доступа к ПДн;

9) минимизация полномочий – предоставления пользователям минимальных прав доступа в соответствии со служебной необходимостью;

10) обоснованность и реализуемость – организационные меры, информационные технологии, технические и программные средства, средства и меры защиты ПДн должны быть обоснованы достижением заданного уровня безопасности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности ПДн;

11) специализация и профессионализм – организация мер и реализация средств защиты должны осуществляться профессионально подготовленными специалистами, а эксплуатация средств защиты проинструктированными сотрудниками Университета;

12) субъект персональных данных имеет право на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных, уточнить их при обращении в Университет (например, при смене паспорта) на основании заявления [12].

Второй документ определяет порядок обработки персональных данных, защиту персональных данных от несанкционированного доступа и разглашения, обеспечение защиты прав и свобод субъектов персональных данных, при обработке их персональных данных, развитие комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся в ФГБОУ ВО «АмГУ» [13]. В данном документе рассматриваются основные понятия, связанные с процессом обработки персональных данных. Такие, например, как: автоматизированная обработка персональных данных, актуальные угрозы безопасности персональных данных, информационная система обработки персональных данных и другие. В нём приведён перечень сведений, составляющих персональные данные, основные требования к их обработке, список уполномоченных лиц, занимающих определённые должности и имеющих доступ к персональным дан-

ным на постоянной основе. Помимо этого в нём размещены формы заявлений-согласий субъектов на обработку персональных данных.

В соответствии с требованиями данных положений и нормативно-правовых документов проводится процесс аудита информационных систем персональных данных.

2 ОПИСАНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

2.1 Описание функций, реализуемых системой поддержки принятия решений

Система поддержки принятия решений предназначена для оказания помощи в принятии решений на основе использования всевозможных данных, нормативных документов, обычных документов, знаний и моделей для идентификации и решения проблем [14].

В соответствии с целями процесса проведения аудита ИСПДн, в данном разделе рассматривается набор функций, которые должна осуществлять будущая система поддержки принятия решений.

1) 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);

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

3) 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;

4) 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;

5) 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.

2.2 Описание архитектуры системы поддержки принятия решений

Данный раздел описывает возможную архитектуру СППР. Данная архитектура схематически представлена на рисунке Д.1 приложения Д.

Модули идентификации ИСПДн и построения модели угроз осуществляют первоначальную загрузку и обработку сведений об ИСПДн и ПДн, которые могут быть получены при помощи методов извлечения знаний. Потенциальными источниками знаний могут стать: эксперты, базы данных, нормативно-правовые документы, справочники, учебники и т.д. [15] Могут быть использованы как коммуникативные методы, так и текстологические. К коммуникативным методам относятся такие методы, как:

1) активные:

а) индивидуальные: анкетирование, диалог, интервью, экспертные игры;

б) групповые: «мозговой штурм», ролевые игры, круглый стол;

2) пассивные: наблюдение, протокол «мыслей вслух», лекции.

К текстологическим относятся следующие методы:

1) анализ учебников;

2) анализ литературы;

3) анализ документов.

В данных модулях проводится классификация ПДн в соответствии с Постановлением Правительства №1119, а также построение модели угроз на основании методической документации, утверждённой ФСТЭК.

Модуль определения уровня защищённости ИСПДн, как видно из названия, осуществляет определение уровня защищённости в соответствии с требованиями нормативной документации (Постановление Правительства №1119).

База знаний регулярно взаимодействует с источниками знаний и пополняется новыми сведениями, полученными в ходе работы системы поддержки принятия решений.

В подсистеме предварительной обработки информации об ИСПДн анализируются требования, предъявляемые к уровням защищённости ИСПДн, а именно насколько выполняются данные требования в текущей системе по сравнению с требуемыми требованиями, оговоренными в нормативной документации. Оценка данных показателей проводится экспертом. Эти показатели являются входными данными для модуля интеллектуального анализа данных, который представлен на рисунке Д.2 Приложения Д. Данный модуль состоит из четырёх частей, которые представляют собой один из четырёх уровней защищённости. Чем выше уровень защищённости, тем больше требований будет к нему предъявлено. Данная подсистема подробно рассматривается в главе 3. Выходом её является оценка показателей текущего уровня защищённости системы.

По итогу оценки предыдущей подсистемы формируются соответствующие рекомендации по улучшению состояния защищённости.

3 ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ МОДУЛЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

3.1 Описание математической модели

Подсистема интеллектуального анализа данных базируется на теории нечёткой логики. Нечёткая логика предназначена для формализации человеческих способностей к неточным или приближенным рассуждениям, которые позволяют более адекватно описывать ситуации с неопределённостью [16]. Математический раздел нечёткой логики является в своём роде обобщением классической логики и теории множеств. Нечёткая логика основывается на понятии нечёткого множества, которое впервые было предложено Лютфи Заде в 1965 году.

Теория нечёткой логики позволяет отойти от привычных понятий обычной классической логики, вводя в высказывания степень неопределённости. Именно поэтому высказывания в нечёткой логике могут принимать не только значения «Истина» или «Ложь» («0» или «1»), но и любые значения 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.

Математическое определение нечёткого множества. Множество A есть множество пар чисел вида:

$$< x, \mu_A(x) >,$$

где x – элемент некоторого множества X;

$\mu_A(x)$ – функция принадлежности, которая показывает степень принадлежности (соответствия) x заданному множеству A.

Данную функцию можно задать в форме отображения:

$$\mu_A: X \rightarrow [0, 1].$$

Данное отображение говорит о том, что каждому $x \in X$ ставится в соответствие определённое действительное число из множества [0, 1]. При этом если $\mu_A(x) = 1$, то элемент абсолютно точно принадлежит множеству A. И наоборот. Если $\mu_A(x) = 0$, то элемент абсолютно точно не принадлежит множеству A.

В общем случае запись нечёткого множества имеет вид:

$A = \{< x, \mu_A(x) >\}$.

Чаще всего функции принадлежности задаются графически и имеют различные формы и виды. Точки по оси *x* задают множество. Точки по оси *y* – соответствующие функции принадлежности. Например, на рисунке 1 представлена треугольная форма функции принадлежности:

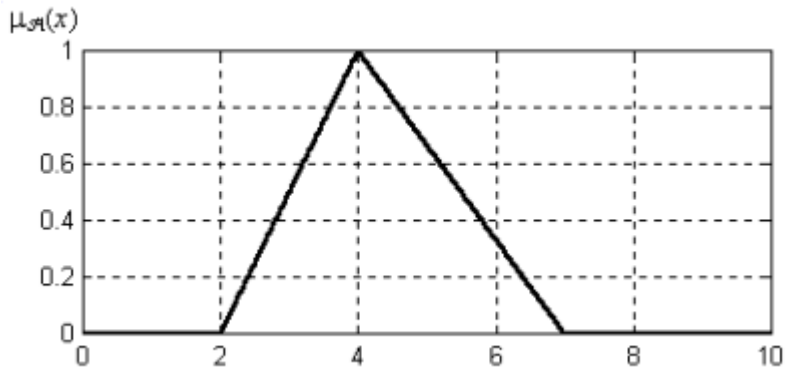

Рисунок 1 – функция принадлежности треугольной формы

И в общем случае аналитически она описывается следующим образом:

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

где a, b и c могут принимать свободные действительные значения.

Конкретно для данного примера $a=2$, $b=4$, $c=7$. Соответственно, для значения a функция принадлежности будет $\mu_A(a) = 0$, для значения b функция принадлежности $\mu_A(b) = 1$, а для значения c функция принадлежности будет равна $\mu_A(c) = 0$.

Также существуют трапециевидные функции принадлежности. Помимо них существуют Z-образные и S-образные функции принадлежности, описываемые своими собственными математическими моделями.

В теории нечёткой логики также используются понятия нечёткой переменной и лингвистической переменной.

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

$$< \alpha, X, A >,$$

где α – наименование нечёткой переменной;

X – множество нечёткой переменной;

$A = \{< x, \mu_A(x) >\}$ – нечёткое множество на множестве X.

Лингвистическая переменная является обобщением нечёткой переменной и имеет вид:

$$< \beta, T, X, G, M >,$$

где β – наименование лингвистической переменной;

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

X – множество нечётких переменных, входящих в определение лингвистической переменной β;

G – синтаксическая процедура, описывающая процесс генерирования из множества T новых термов. Могут использоваться логические связки «ИЛИ», «И» и модификаторы типа «немного», «очень», «НЕ»;

M – семантическая процедура, которая ставит в соответствие терму, сгенерированному процедурой G, некоторое осмысленное содержание посредству формирования соответствующего нечёткого множества.

Нечётким множествам свойственны аналогичные логические операции как в теории классической логики. К ним применимы такие операции, как например: логическое отрицание, конъюнкция, дизъюнкция, импликация, эквивалентность.

В теории нечёткой логики также задействовано определение правила нечётких продукций. Нечёткие продукции нашли своё применение в системах искусственного интеллекта. Они используются для представления знаний и вывода заключений той или иной предметной области в экспертных системах, а также для описания, анализа и моделирования сложных слабо формализуемых систем и процессов [17].

Экспертные системы имеют дело с задачами ИИ на верхнем уровне, формируют управленческие решения с учётом сложившейся или прогнозируемой ситуации, накапливают эвристические знания и пытаются имитировать поведение эксперта [18].

Правило нечёткой продукции имеет следующий вид:

$(i): Q; P; A => B; S, F, N,$

где *(i)* – наименование нечёткой продукции;

Q – область её применения. Предназначена для описания предметной области, которую представляет продукция;

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

$A => B$ – ядро нечёткой продукции, где:

A – условие ядра или посылка, или антецедент;

B – заключение ядра или консеквент;

«=>» – знак логического следования (или секвенции);

S – метод определения значения степени истинности заключения ядра. Данный метод в общем случае реализует алгоритм нечёткого вывода. Отдельный такой алгоритм будет рассмотрен в следующих разделах. Его также можно назвать методом активизации или методом композиции;

F – коэффициент определённости нечёткой продукции. Также он называется весовым коэффициентом. Принимает значения в интервале [0, 1] и определяет количественную оценку степени истинности нечёткой продукции;

N – постусловия продукции. Описывает возможные действия при реализации ядра продукции.

Ядро продукции является центральным элементом данного понятия, который выражает послание в форме: «ЕСЛИ A, ТО B».

Совокупность нечётких продукций образует продукционную систему.

3.2 Описание системы нечёткого вывода

Процесс нечёткого вывода можно охарактеризовать как алгоритм получения нечётких заключений на основе нечётких условий (посылок). Он объединяет в себе вышерассмотренные понятия нечётких и лингвистических переменных, функций принадлежности и нечётких логических операций, таких, к примеру, как нечёткая импликация и нечёткая композиция. Системы нечёткого вывода являются частным случаем нечётких продукционных систем.

Центральным элементом систем нечёткого вывода являются нечёткие лингвистические высказывания. Различаются следующие виды нечётких лингвистических высказываний:

1) высказывание «β есть α», где β – название лингвистической переменной, α – значение лингвистической переменной, которому ставится в соответствие определённый лингвистический терм из терм-множества T;

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

3) составные высказывание, полученные от первых двух видов с использованием логических связок «ИЛИ», «И», «НЕ», «ЕСЛИ_ТО».

Из нечётких высказываний формируются в свою очередь правила нечётких продукций условий и последующих заключений, рассмотренные в предыдущем разделе. 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 можно записать следующим образом:

ПРАВИЛО <#>: ЕСЛИ "β_1 есть α'", ТО "β_2 есть α''",

где "β_1 есть α'" является условием правила нечёткой продукции, а "β_2 есть α''", соответственно, заключением. При этом β_1 не равен β_2.

Чтобы получить заключения из условий, необходимо применить механизмы или алгоритмы нечёткого вывода.

В общем случае алгоритм нечёткого вывода состоит из следующих этапов, схематически представленных на рисунке 2:

Рисунок 2 – Этапы алгоритма нечёткого вывода

Формирование базы правил. На данном этапе создаётся множество правил нечётких продукций – база правил нечётких продукций. База правил должна быть полной, согласованной и непротиворечивой во избежание неадекватности полученного вывода.

Правила в общем виде задаются следующим образом:

ПРАВИЛО_№1: ЕСЛИ «Условие_1», ТО «Заключение_1» (F_1)

ПРАВИЛО_№2: ЕСЛИ «Условие_2», ТО «Заключение_2» (F_2)

…

ПРАВИЛО_№n: ЕСЛИ «Условие_n», ТО «Заключение_n» (F_n)

F_i ($i \in \{1, 2, \dots, n\}$) – весовой коэффициент или коэффициент определённости нечёткой продукции, принимающий значение в интервале [0, 1]. Если весовой коэффициент не задан явно, то по умолчанию его значение равно 1.

Для задания базы правил необходимо определить совокупность правил нечётких продукций $P = \{R_1, R_2, \dots, R_n\}$, совокупность входных лингвистических переменных $V = \{\beta_1, \beta_2, \dots, \beta_n\}$ и совокупность выходных лингвистических переменных $W = \{\omega_1, \omega_2, \dots, \omega_n\}$.

Фаззификация входных переменных. По-другому этот этап называют введением нечёткости. На данном этапе происходит процесс нахождения функций принадлежности лингвистических термов на основании обычных исходных данных – каждому обычному численному значению отдельной входной переменной в системе нечёткого вывода ставится в соответствие значение функции принадлежности отдельного терма лингвистической переменной. Итог данного этапа: совокупность функций принадлежности по всем термам лингвистических переменных.

Агрегирование подусловий. На этом этапе осуществляется определение степени истинности подусловий по всем правилам системы нечёткого вывода. Если подусловие имеет вид 1 или 2 рассмотренных выше нечётких лингвистических высказываний, степень его истинности принимает значение соответствующей ему функции принадлежности. Если же высказывание составное (соединённое посредству логических связок), то для определения степени истинности используются операторы нечёткой конъюнкции или нечёткой дизъюнкции.

Активизация подзаключений. На этом этапе происходит процесс нахождения степеней истинности подзаключений для каждого правила нечётких продукций. На данном этапе рассматриваются подзаключения каждого правила и весовые коэффициенты этих правил. Степень истинности каждого подзаключения определяется как алгебраическое произведение значения истинности подусловия, полученного на предыдущем этапе, и весового коэффициента соответствующего правила.

После этого необходимо найти функции принадлежности для каждого подзаключения рассматриваемых выходных лингвистических переменных. Для этого может быть использован один из методов:

1) min-активизация:

$\mu'(y) = \min\{c_j, \mu(y)\};$

2) prod-активизация:

$\mu'(y) = c_j * \mu(y);$

3) average-активизация:

$\mu'(y) = 0.5 * (c_j + \mu(y)),$

где $\mu(y)$ – функция принадлежности терма некоторой выходной переменной ω_j, определённой на множестве Y;

c_j – степень истинности подзаключения, определённая на данном этапе.

Аккумулирование заключений. На данном этапе происходит нахождение функций принадлежности для каждой выходной лингвистической переменной из множества $W = \{\omega_1, \omega_2, \dots, \omega_n\}$. Здесь происходит объединение всех степеней истинности заключений для получения функции принадлежности каждой выходной переменной, потому как заключения, относящиеся к одной и той же лингвистической переменной, принадлежат разным правилам системы нечёткого вывода.

Дефаззификация выходных переменных. Итоговый этап работы системы нечёткого вывода. По-другому этот этап называют введением чёткости. Он подразумевает собой процесс нахождения обычного (чёткого) значения для каждой выходной переменной. В данном этапе для приведения к 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, описанном в следующем разделе.

3.2.1 Описание алгоритма нечёткого вывода типа Сугено

Существует несколько широко используемых алгоритмов нечёткого вывода, реализующие этапы нечёткого вывода, рассмотренные выше. Как правило, различаются они только определёнными параметрами, фиксированными и специфичными для каждого отдельного алгоритма. Одним из таких алгоритмом является алгоритм Сугено. Он также используется при формировании гибридных сетей в модуле ANFIS пакета Matlab, который рассматривается в последующих разделах.

Состоит он из следующих этапов:

1) формирование базы правил. Правила должны формироваться в следующем виде:

ПРАВИЛО <#>: ЕСЛИ "β_1есть α' " И "β_2есть α'' ", ТО "$w = \varepsilon_1 * a_1 + \varepsilon_2 * a_2$",

где ε_1 и ε_2 – весовые коэффициенты. Итоговое значение *w* определяется как некоторое действительное число;

2) фаззификация входных переменных аналогична описанному в предыдущем разделе этапу;

3) агрегирование подусловий. Чтобы найти степень истинности подусловий, используется логическая операция min-конъюнкции;

4) активизация подзаключений. Используется метод min-активизации для нахождения степени истинности всех подзаключений, а затем производится расчёт чётких значений выходных переменных. Для этого используется форма задания правил из 1-го этапа, где вместо a_1 и a_2 подставляются значения входных переменных до их фаззификации;

5) аккумулирование заключений. Данный этап обозначен формально, т.к. расчёты осуществляются с обычными действительными числами;

6) дефаззификация выходных переменных. Для этого этапа используется модификация метода центра тяжести для одноточечных множеств:

$$y = \frac{\sum_{i=1}^{n} c_j * w_i}{\sum_{i=1}^{n} c_j},$$

где c_j – степень истинности подзаключения, определённая на этапе 4;

w_i – чёткое значение, полученное на этапе 4.

3.3 Описание лингвистических переменных

Для реализации модуля интеллектуального анализа данных необходимо определить входные и выходные показатели. Ими будут являться требования к уровням защищённости, отражённые в таблице приложения Г, а также итоговая оценка уровня защищённости ИСПДн.

Данные требования могут определяться однозначно и неоднозначно.

Однозначно определяемые требования:

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

2) должностное лицо, ответственное за обеспечение безопасности ПДн (X5);

3) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн (X7);

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

И неоднозначно определяемые требования:

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

2) сохранность носителей (X2);

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

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

Данное разделение означает, что однозначно определяемым показателям можно дать оценку 1 или 0, соответственно, при выполнении или не выполнении данного требования в системе. В то время как оценка неоднозначно определяемых показателей может принимать значения в интервале [0, 1].

Необходимо на основании данных сведений определить лингвистические переменные.

Для однозначно определяемых лингвистических переменных определены два лингвистических терма:

1) S – требование не выполняется;

2) L – требование не выполняется.

Соответственно, числовые значения для данных термов: $X_j = 0$ для терма S и $X_j = 1$ для терма L.

Для неоднозначно определяемых лингвистических переменных вводятся три лингвистических терма, описанные следующим образом:

1) S – низкий уровень выполнения требования;

2) M – средний уровень выполнения требования;

3) L – высокий уровень выполнения требования.

Соответственно, числовые значения для данных термов принадлежат интервалам: $(X_i) \in [0; 0{,}3)$ для терма S, $(X_i) \in [0{,}3; 0{,}9)$ для терма M и $(X_i) \in [0{,}9; 1]$ для терма L.

Для выходной, результирующей оценки Y_i определяются пять лингвистических термов следующего вида:

1) S – низкая оценка уровня защищённости;

2) SM – оценка уровня защищённости ниже среднего;

3) M – средняя оценка уровня защищённости;

4) ML – оценка уровня защищённости выше среднего;

5) L – высокая оценка уровня защищённости.

Соответственно, числовые значения для данных термов принадлежат интервалам: $(Y_i) \in [0; 0{,}1]$ для терма S $(Y_i) \in (0{,}1; 0{,}3]$ для терма SM, $(Y_i) \in (0{,}3; 0{,}7)$, для терма M, $(Y_i) \in [0{,}7; 0{,}9)$, для терма ML и $(Y_i) \in [0{,}9; 1]$ для терма L.

3.4 Описание модуля ANFIS - адаптивных систем нейро-нечёткого вывода в пакете Matlab

Модуль интеллектуального анализа данных представляет собой модульную нейронную сеть.

Нейронные сети – это математический аппарат, созданный на основе функционирования биологических нейронов, и призванный решать класс задач, связанный с продукциями и введением нечёткости данных. Это такие задачи, как: прогнозирование, экстраполяция, интерполяция, распознавание образов и другие.

Нейронные сети представляют собой устройства параллельных вычислений, состоящие из множества простых процессоров. Каждый процессор такой сети имеет дело только с сигналами, которые он периодически получает, и сигналами, которые он периодически посылает другим процессорам [19].

Основным их достоинством является то, что новую информацию о проблемной области можно получить на основе прогнозов. При этом они способны обучаться посредству уже имеющейся доступной информации.

Построение нейросети сводится к следующим этапам:

1) конфигурирование структуры нейронной сети;

2) обучение нейронной сети на основе уже имеющихся данных о предметной области;

3) проверка нейронной сети с использованием некоторых данных для тестирования;

4) использование нейронной сети для решения поставленных задач о предметной области.

Отдельным случаем нейронных сетей являются так называемые нечёткие нейронные сети или гибридные сети. Они объединяют в себе достоинства нейронных сетей и систем нечёткого вывода. Поэтому они являются наиболее удобным и менее трудоёмким механизмом для решения поставленных задач.

В среде Matlab механизм гибридных сетей реализован в модуле ANFIS – Adaptive Neuro-Fuzzy Inference System (адаптивная система нейро-нечёткого вывода). Гибридная сеть, построенная с использованием данного инструмента, представляет собой нейронную сеть с единственным выходом и несколькими входами, являющимися лингвистическими переменными.

Термы входных переменных в данном случае описываются стандартными функциями принадлежности, а термы выходной переменной – константой или линейной функциями принадлежности.

ANFIS реализует алгоритм Сугено, который был рассмотрен в предыдущем разделе. При этом все весовые коэффициенты равны единице.

В пакете Matlab помимо этого находятся редакторы, позволяющие пользователю самостоятельно настраивать элементы сети: функции принадлежности, базу правил, а также выводить визуализированную поверхность полученных данных.

3.5 Построение нейронной сети в модуле ANFIS

Построение нечёткой нейронной сети начинается с определения базы правил для входных показателей.

Пусть исследуемая информационная система персональных данных классифицируется по 4-му уровню защищённости, а именно: категория обрабатываемых данных – общедоступные данные; количество субъектов персональных данных не превышает 100 000; третий тип актуальных угроз, связанный с отсутствием недекларированных возможностей в ОС и ПО. Тогда входными параметрами, определяемыми экспертом, будут:

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

2) сохранность носителей (X2);

3) перечень лиц, допущенных к ПДн (X3);

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

Сумма правил составляет 54, так как в данном случае три входные лингвистические переменные определяются тремя лингвистическими термами (S, M, L), а четвёртая – двумя (S, L): $2 * 3^3 = 54$.

Правила описываются в форме:

R_j: ЕСЛИ $X1$ есть A_1^j и $X2$ есть A_2^j и $X3$ есть A_3^j и $X4$ есть A_4^j, ТО $Y_j = B_k^j$,

где R_j – j-е правило;

X1, X2, X3, X4 – входные показатели;

Y_j – значение выхода j-го правила;

A_1^j, A_2^j, A_3^j, A_4^j, B_k^j – нечёткие подмножества.

Фрагмент правил представлен на рисунке 3:

	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
22						
23	11	S	M	S	M	SM
24						
25	12	S	M	L	L	M
26						
27	13	S	L	S	S	SM
28						
29	14	S	L	L	M	M
30						
31	15	S	L	S	L	M

Рисунок 3 – Фрагмент базы правил для нечёткой нейронной сети

Полная база правил отражена в приложении Е.

Далее необходимо создать на основе данных правил обучающую выборку. Для этого в каждом правиле для каждой входной переменной случайно выбирается значение из интервалов, соответствующее тому или иному лингвистическому терму. Для этого можно использовать численный метод Монте-Карло. Фрагмент обучающей выборки изображён на рисунке 4:

№	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 4 – Фрагмент обучающей выборки

Полная выборка отражена в приложении Ж.

Для работы с редактором ANFIS, необходимо ввести в командную строку Matlab команду anfisedit. Произойдёт открытие редактора нечёткого вывода.

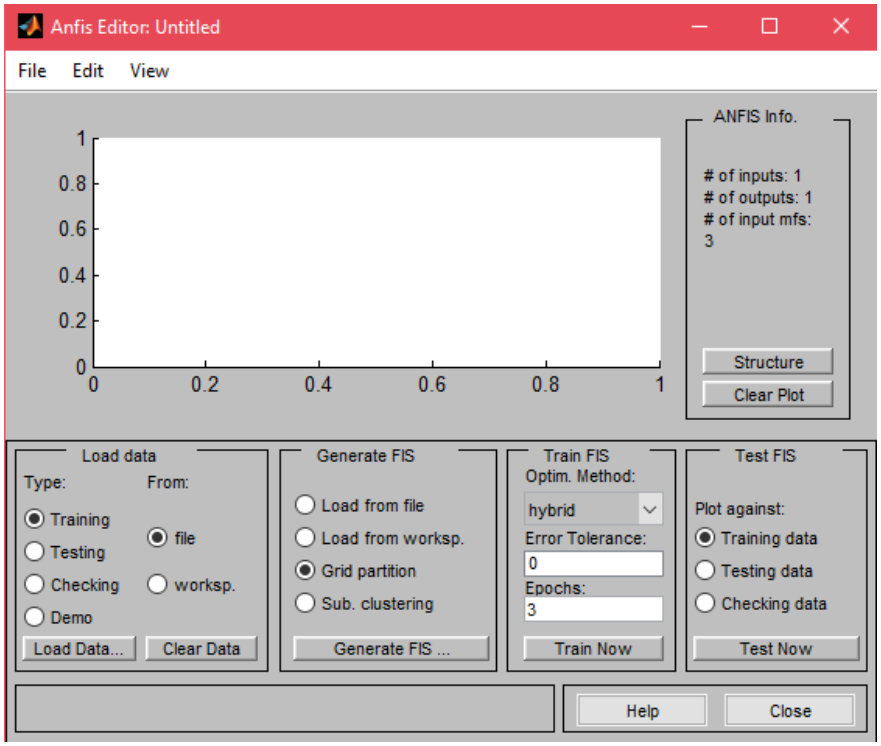

Рисунок 5 – Главное окно модуля ANFIS

Для построения сети необходимо загрузить входные данные с помощью кнопки Load Data. Входными данными является обучающая выборка для нечёткой нейронной сети, сохранённая в текстовом редакторе в формате .dat. В системе существуют следующие типы входных данных:

1) обучающие данные – обязательные данные, использующиеся для построения гибридной сети;

2) тестовые данные – используются для тестирования сети с целью проверки её качества;

3) проверочные данные – выполняют функцию проверки гибридной сети с целью определения факта переобучения сети;

4) демонстрационные данные – загрузка демонстрационных примеров.

После загрузки обучающей выборки из файла главное окно модуля ANFIS принимает вид:

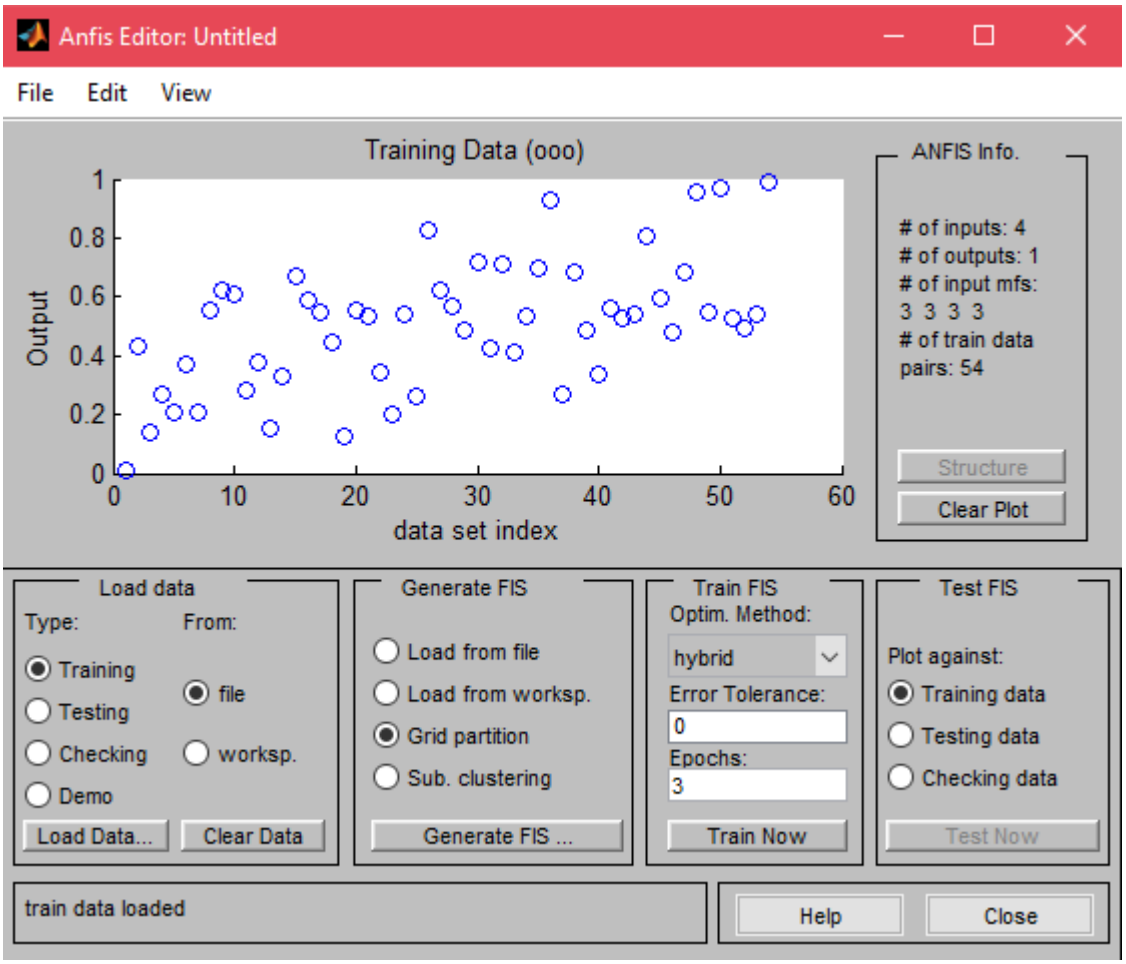

Рисунок 6 – Загрузка данных в модуль ANFIS

Далее необходимо сгенерировать структуру системы нечёткого вывода алгоритма типа Сугено. Для этого служит кнопка Generate FIS.

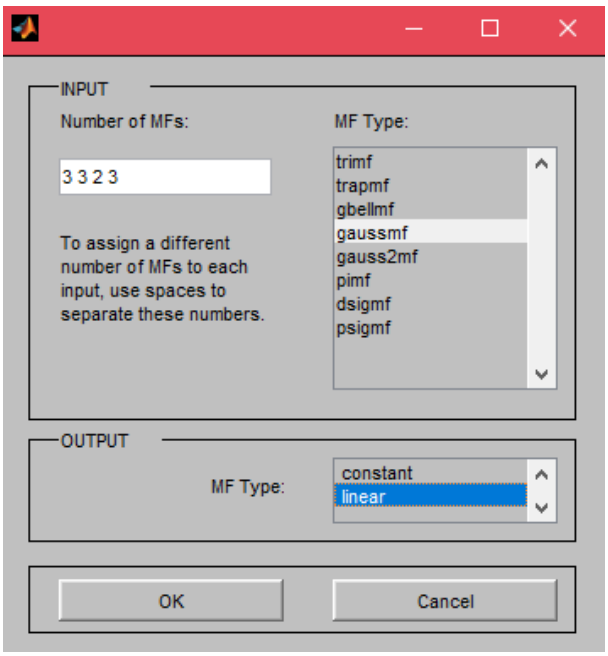

Рисунок 7 – Окно генерации структуры нечёткого вывода

Для входных переменных настраиваются параметры: количество функций принадлежности для входных переменных и их тип. Для выходной переменной – только тип функции принадлежности: линейная или константа.

Кнопка Structure главной рабочей области отображает структуру нечёткой нейронной сети:

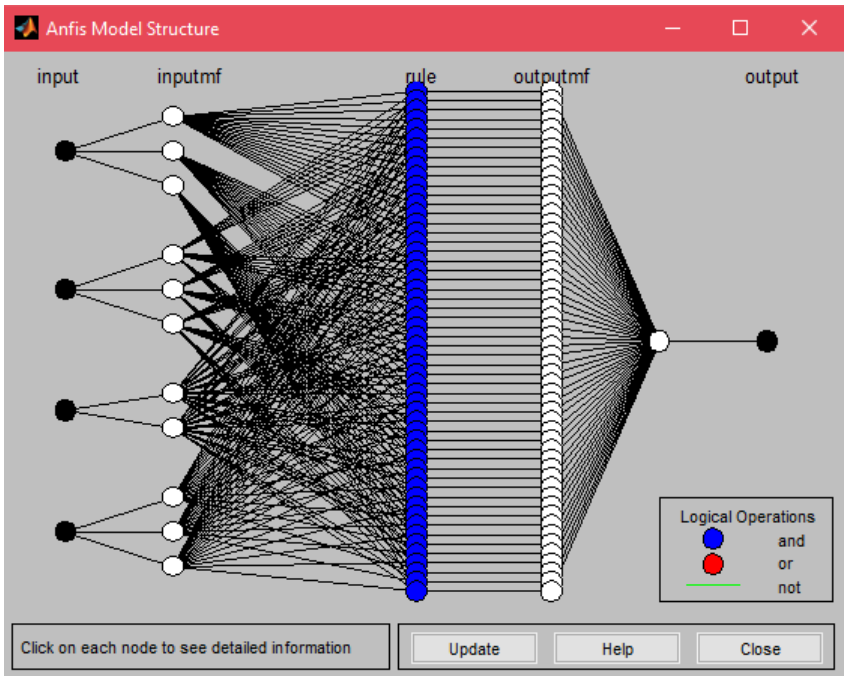

Рисунок 8 – Структура нечёткой нейронной сети

Затем необходимо провести обучение нейронной сети. Перед обучением происходит настройка параметров. Во-первых, это определение метода обучения. Гибридный, основывающийся на комбинации метода обратных квадратов и метода убывания обратного градиента, или же метод обратного распространения. Во-вторых, это установка уровня ошибки обучения. И, в-третьих, это установление количества итераций обучения. Для рассматриваемой сети данное значение будет равно 40. После этого нужно нажать на кнопку Train now.

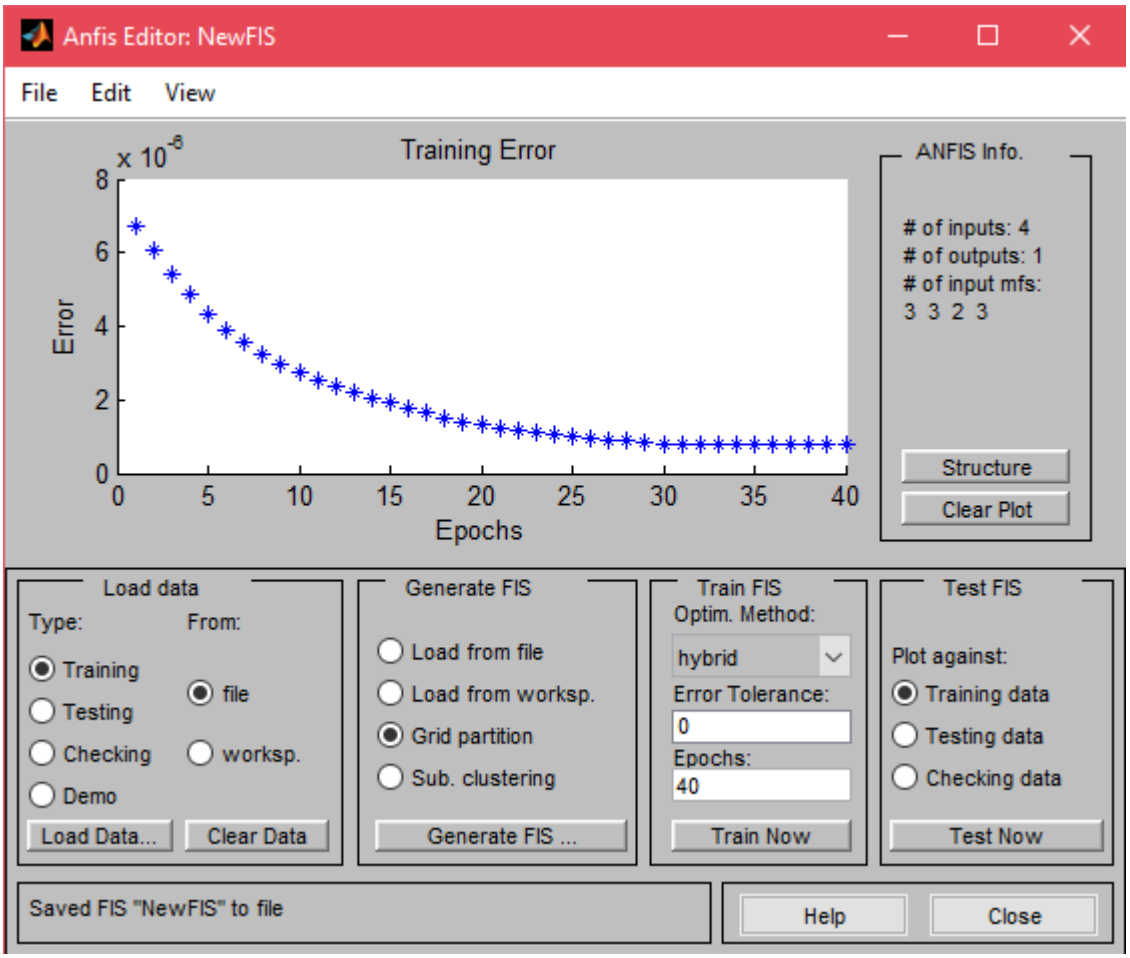

Рисунок 9 – Процесс обучения нечёткой нейронной сети

Данный график отображает зависимость ошибки обучения от количества итераций обучения.

Сгенерированную структуру нечёткой нейронной сети можно сохранить в файл, нажав последовательно на кнопки в верхнем меню File –> Export –> To file.

Далее нейронную сеть можно настраивать в специальных редакторах, также предусмотренных в пакете Matlab.

Один из таких редакторов – редактор системы нечёткого вывода, позволяет настраивать функции принадлежности гибридной сети, задавать определённые параметры, переименовывать входные и выходные переменные или же добавлять новые. Вызывается он в командной строке при помощи команды mfedit, либо из верхнего меню редактора ANFIS: Edit –> FIS Properties.

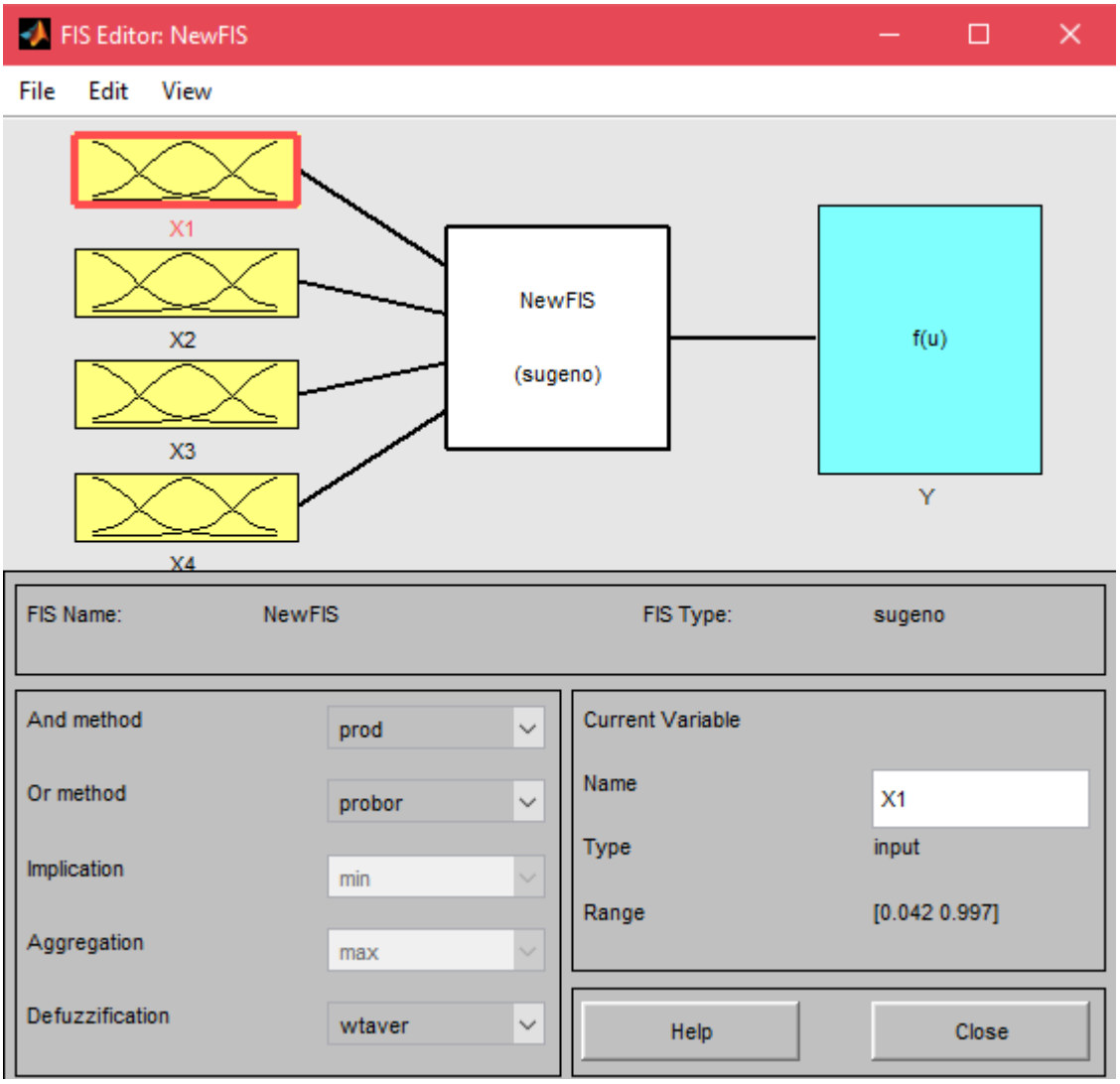

Рисунок 10 – Главное окно редактора системы нечёткого вывода

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

Щёлкнув дважды по переменной, можно открыть окно редактирования конкретных функций принадлежности.

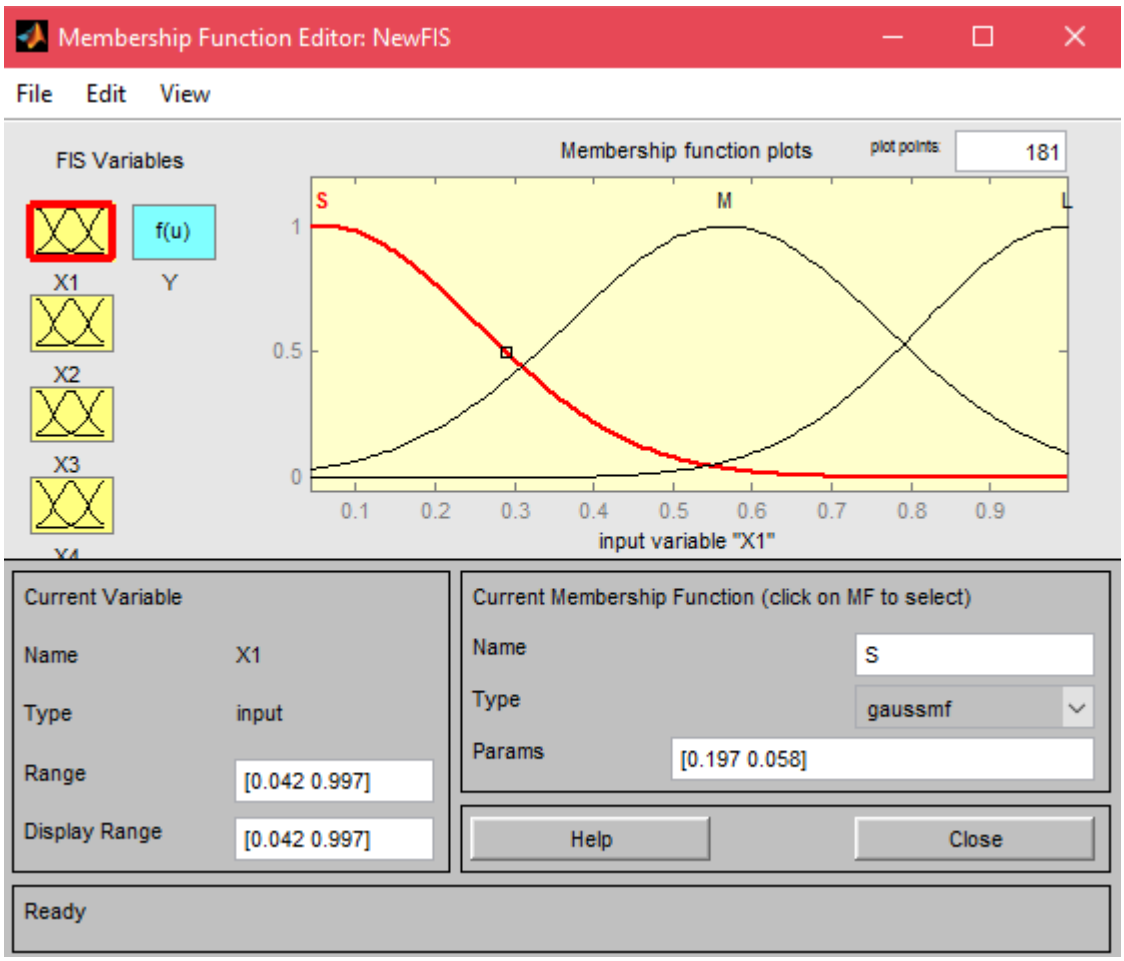

Рисунок 11 – Окно редактирования функций принадлежности

Данное окно 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 связок между входными переменными, изменять составляющие правил, выбирать их весовые коэффициенты, удалять старые и добавлять новые правила.

Окно редактирования базы правил изображено на рисунке 12.

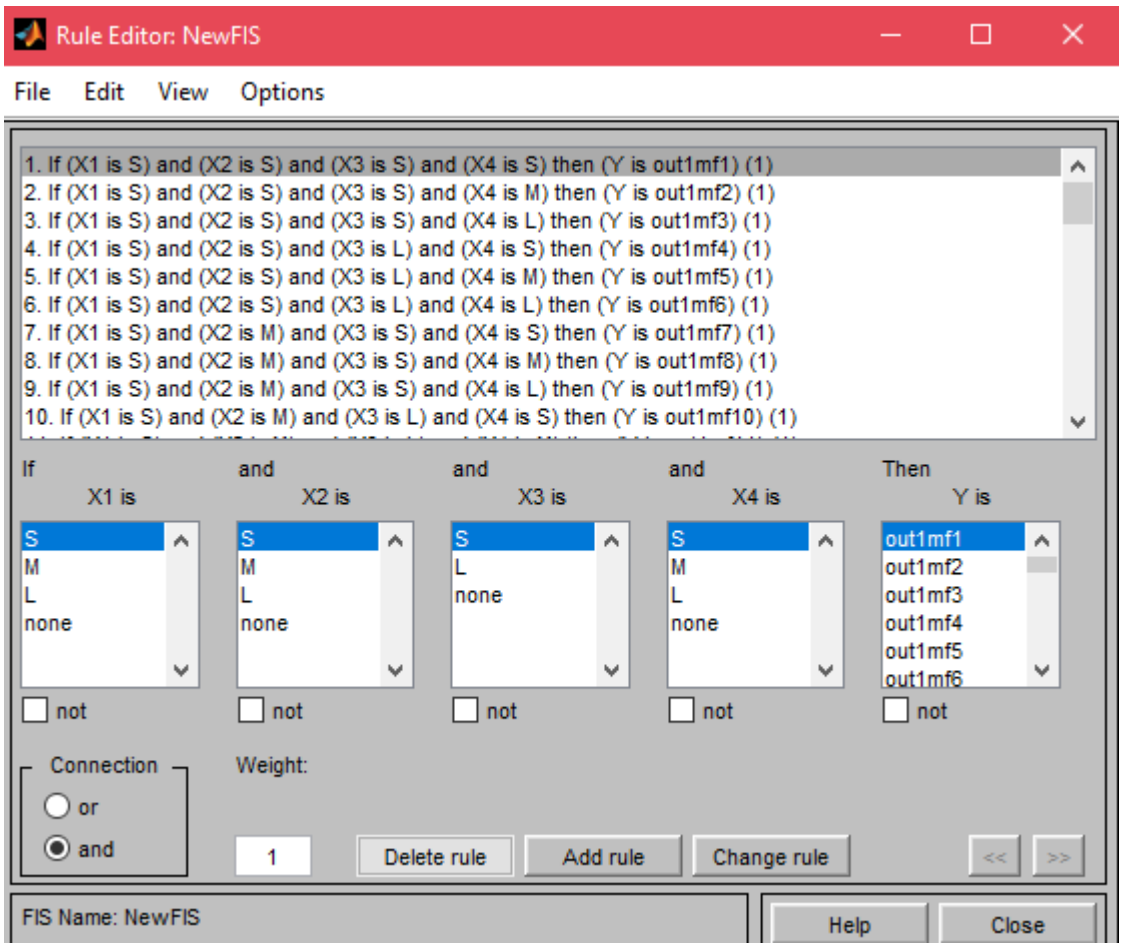

Рисунок 12 – Окно редактирования базы правил

3.6 Тестирование нейронной сети

После завершение процесса генерации гибридной нечёткой сети и её редактирования можно приступить к её проверке.

Для этого необходимо открыть окно просмотра правил. Сделать это можно через редактор FIS, редактор ANFIS или редактор функций принадлежности. Для этого достаточно выбрать в верхнем меню пункт View –> Rules, либо использовать комбинацию клавиш Ctrl+5.

В строке входных данных задаются значения параметров, для которых необходимо произвести оценку защищённости. Допустим, эксперт оценивает требования к уровням защищённости для конкретной ИСПДн следующим образом:

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

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

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

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

Тогда итоговый выходной показатель будет равен 0,8. Это значит, что данная информационная система персональных данных соответствует требованиям нормативно-правовой документации на 80%. Данная оценка говорит о том, что уровень защищённости системы выше среднего. Для того чтобы система выдавала наиболее высокий результат, следует увеличить значение одного из показателей (X2 или X4) с уровня M на уровень L.

Рисунок 13 – Результат работы нечёткой нейронной сети

Данные показатели можно также визуализировать в виде поверхности для наиболее наглядного представления данных.

Для этого необходимо в верхнем меню редакторов FIS, ANFIS, функций принадлежности или в окне просмотра правил выбрать пункт View -> Surface, либо использовать комбинацию клавиш Ctrl+6.

Данная 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 поверхность нечёткого вывода, отображающая связь входных показателей X1 и X2 с выходным значением Y.

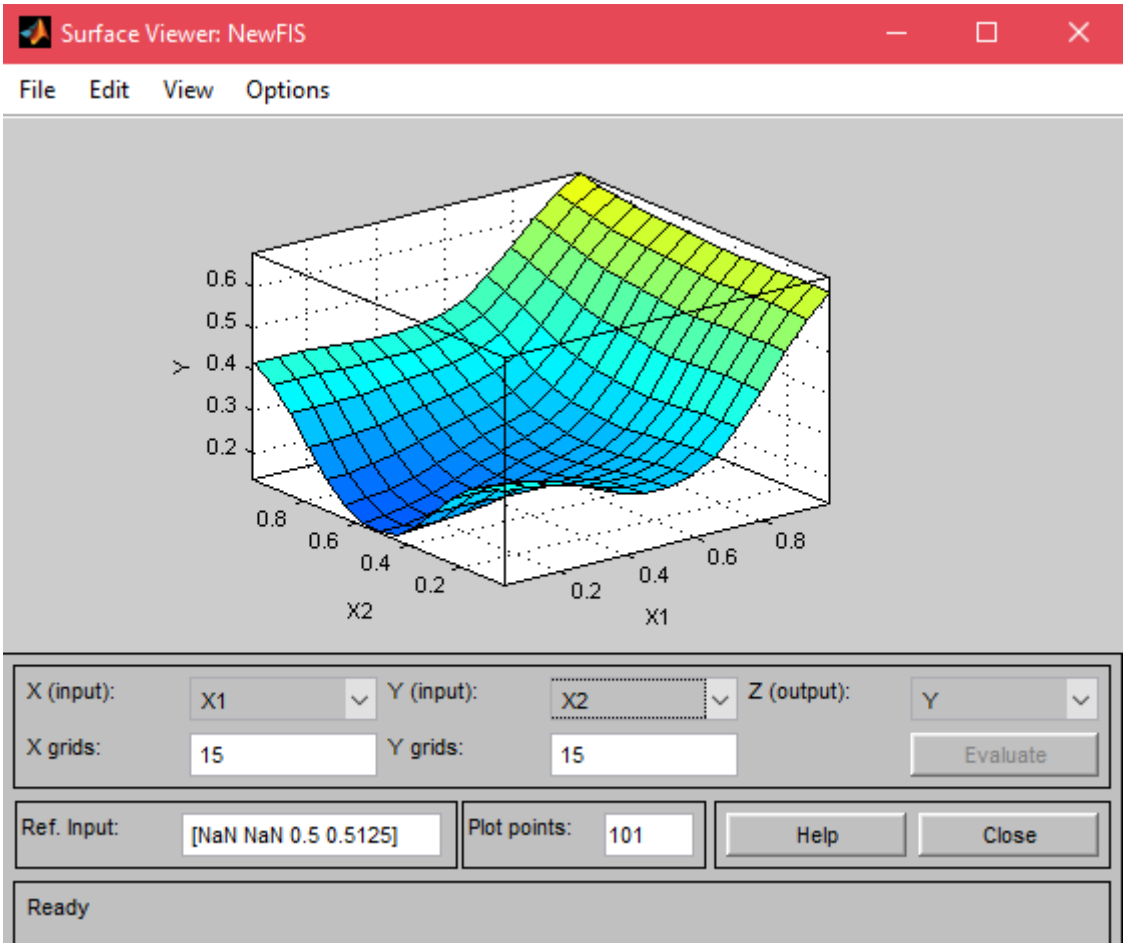

Рисунок 14 – Визуализация поверхности

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

4.1 Безопасность

Для оценки состояния безопасности объекта исследования, необходимо было провести анализ соответствия реальных показателей требуемым показателям, которые оговариваются в СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» [20].

При организации рабочего места пользователя в деканате ФМиИ удовлетворяются следующие требования к ПЭВМ:

1) дизайн ПЭВМ имеет окраску корпуса в спокойные мягкие тона с диффузным рассеиванием света. Корпус ПЭВМ, клавиатура и другие блоки и устройства ПЭВМ имеют матовую поверхность с коэффициентом отражения 0,4 - 0,6, на них также отсутствуют блестящие детали, которые могут создавать блики;

2) конструкция ПЭВМ обеспечивает возможность поворота корпуса в горизонтальной и вертикальной плоскости с фиксацией в заданном положении для обеспечения фронтального наблюдения экрана видеодисплейного терминала;

3) конструкцией видеодисплейного терминала предусмотрено регулирование яркости и контрастности;

4) необходимые допустимые значения электромагнитных полей, создаваемых ПЭВМ, не превышают показатели, установленные СанПиН 2.2.2/2.4.1340-03;

5) допустимые визуальные параметры устройств отображения информации удовлетворяют требованиям СанПиН 2.2.2/2.4.1340-03.

При организации рабочего места пользователя удовлетворяются следующие требования к помещению деканата:

1) помещение деканата оборудовано защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации;

2) рабочие места с ПЭВМ располагаются вдали от силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

Не удовлетворяются следующие требования к помещению деканата:

1) окна в помещении, где эксплуатируется вычислительная техника, не ориентированы на север и восток;

2) площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов составляет менее 4,5 $м^2$;

При организации рабочего места пользователя удовлетворяются следующие требования к микроклимату помещения деканата:

1) в помещении, оборудованном ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ;

2) содержание вредных химических веществ в воздухе не превышает предельно допустимых концентраций вредных веществ в воздухе рабочей зоны в соответствии с действующими гигиеническими нормативами;

При организации рабочего места пользователя удовлетворяются следующие требования к уровням шума и вибрации помещения деканата:

1) шумящее оборудование (печатающие устройства, серверы и т.п.), уровни шума которого превышают нормативные, размещено вне помещения с ПЭВМ.

При организации рабочего места пользователя удовлетворяются следующие требования к освещению помещения деканата:

1) рабочий стол размещён таким образом, что видеодисплейный терминал ориентирован боковой стороной к световым проёмам, чтобы естественный свет падал преимущественно слева;

2) искусственное освещение в помещении деканата осуществляется системой общего равномерного освещения;

3) для обеспечения нормируемых значений освещенности в помещении деканата для использования ПЭВМ проводится чистка стекол оконных рам и

светильников не реже двух раз в год, а также проводится своевременная замена перегоревших ламп.

При организации рабочего места пользователя удовлетворяются следующие общие требования:

1) расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора) составляет не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м;

2) экран видеомонитора находится от глаз пользователя на расстоянии 600 - 700 мм и не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов;

3) рабочий стул (кресло) является подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от переднего края сиденья, при этом регулировка каждого параметра является независимой, легко осуществляемой и имеет надежную фиксацию;

4) также помимо этого поверхность сиденья, спинки и других элементов стула (кресла) является полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

При организации рабочего места пользователя удовлетворяются следующие требования к организации и оборудованию:

1) отсутствует возможность регуляции высоты рабочей поверхности стола для взрослых пользователей, но при этом высота поверхности стола составляет 725 мм;

2) рабочий стол имеет пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног - не менее 650 мм;

Однако отсутствует подставка для ног. Клавиатура расположена на поверхности стола менее чем на расстоянии 100 - 300 мм от края, обращенного к пользователю.

В соответствии с проведённым анализом, могут быть предложены следующие рекомендации:

1) окна должны быть оборудованы вертикальными жалюзи, т.к. они не ориентированы преимущественно на север и юг;

2) необходимо также увеличить расстояние между рабочими местами с ПЭВМ, чтобы оно составляло более 4,5 $м^2$;

3) необходимо установить подставку для ног для каждого рабочего места;

4) необходимо расположить клавиатуры более чем на расстоянии 10-30 см от края.

Модуль системы поддержки принятия решений реализован в пакете Matlab, конкретно в редакторе адаптивных систем нейро-нечёткого вывода ANFIS. Пакет Matlab представляет собой мощную операционную среду, которая позволяет выполнять огромное число математических решений и научно-технических расчётов. Данная среда имеет мощные средства для ведения диалога, графики и комплексной визуализации вычислений, а также встроенный компилятор и возможность создания исполняемых файлов [21].

Помимо этого для более удобной работы интерфейс программы можно настраивать следующим образом:

1) изменять в командном окне: количество отображаемых на странице строк, цветовую гамму вводимого кода;

2) изменять в окне редактора: цвет выделения текущей строки, а также цветовую гамму границ;

3) изменять размер вкладок и их отступ;

4) изменять размеры шрифтов в командном окне и окне редактора, а также их тип;

5) настраивать сочетания клавиш для быстрого доступа к определённым функциям программы;

6) настраивать панель инструментов быстрого доступа;

7) настраивать генератор отчётов;

8) настраивать специальные инструменты, такие как, например, получение изображений, обработка изображений, параллельные вычисления, 3D-графика, инструмент баз данных, и другие.

Благодаря данным настройкам программного продукта становится возможной установка параметров рабочих окон таким образом, чтобы максимально удобно и безопасно воспринимать и обрабатывать данные.

Пользовательский интерфейс программного продукта соответствует требованиям, предъявляемым к программному обеспечению. Элементы управления заметны и понятны, что позволяет увеличить скорость выполнения работы. Элементы меню сгруппированы, командные кнопки расположены внизу окон, т.е. в той части окна, которая, как правило, сканируется взглядом в последнюю очередь. Пиктограммами снабжены только самые важные элементы меню.

Для отображения математических данных и кода в командном окне и окне редактора используется стандартный шрифт Monospaced. Для оконных профилей и области инструментов используется шрифт SansSerif. Данные шрифты позволяют легко воспринимать текстовую информацию.

Цветовая гамма содержит не более трёх цветов во избежание затруднения зрительного восприятия. Основная область имеет белый цвет. Цвет текста преимущественно чёрный. Окно модуля нейро-нечёткого вывода имеет серый цвет.

Оформление интерфейса программного продукта подразумевает собой акцентирование внимания на наиболее важных задачах, выполняемых программой и отсутствие отвлекающих элементов, затрудняющих восприятие информации.

4.2 Экологичность

Для деканата ФМиИ ФГБОУ ВО «АмГУ» должен быть предусмотрен процесс утилизации отходов. Основным видом отходов для деканата являются бумажные отходы.

Бумажные отходы, содержащие сведения, отнесённые к персональным данным, а вместе с тем требующие защиты, необходимо утилизировать при по-

мощи технических средств (шрёдера, уничтожителя бумаги и т.д.), либо термических (путём сжигания).

Если на бумаге, подлежащей утилизации, не имеется данных, отнесённых к категории персональных и, соответственно, не требующих защиты, то она утилизируется стандартным способом.

4.3 Чрезвычайные ситуации

Чрезвычайная ситуация – обстановка на определённой территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей [22].

ГОСТ Р 22.0.02-94 «БЧС. Термины и определения основных понятий» также определяет следующие понятия, относящиеся к чрезвычайным ситуациям:

Источник чрезвычайных ситуаций – это опасное природное явление, авария, или опасное техногенное происшествие, в результате чего произошла или может возникнуть чрезвычайная ситуация.

Безопасность в чрезвычайных ситуациях – это состояние защищённости населения, объектов народного хозяйства и окружающей природной среды от опасностей в чрезвычайных ситуациях [23].

В пункте 1.4 главы 1 были рассмотрены основные угрозы объекта исследования. В качестве угроз, относящихся к чрезвычайным ситуациям, а соответственно, составляющих категорию естественных источников угроз, для предметной области были выделены пожары.

К обеспечению пожарной безопасности предъявляются следующие требования.

Необходимо обеспечить выполнение и соблюдение утверждённых правил пожарной безопасности, регулярное проведение инструктажей, регулярные проверки электрических установок и электрических сетей на предмет выявле-

ния неисправностей. Данные требования выполняются для объекта исследования.

Помещение деканата должно быть оборудовано противопожарными сигнализациями, а также огнетушителями – инструментами для подавления локальных очагов возгорания. Данные требования выполняются для объекта исследования.

При обеспечении эвакуации людей предельно допустимые расстояния между эвакуационными выходами должны быть в пределах 15 до 250 м. В здании должно быть не менее двух эвакуационных выходов. Данные требования выполняются для объекта исследования.

При разработке генерального плана необходимо обеспечить безопасные расстояния от границ территории Университета до жилых и общественных зданий. Необходимо обеспечить должное количество въездов на территорию здания. Также необходимо зонировать здания и сооружения по родственному и функциональному назначению. Помимо этого необходимо обеспечить ограждение территории здания. Территория Университета имеет чётко определённые безопасные расстояния до жилых и общественных зданий. Помимо этого оно зонировано по родственному и функциональному назначению, а также имеет должное количество въездов на территорию и ограждение территории.

ЗАКЛЮЧЕНИЕ

В ходе выполнения бакалаврской работы была исследована информационная система персональных данных деканата факультета математики и информатики ФГБОУ ВО «Амурского государственного университета». Были проанализированы основные информационные потоки, а также перечень обрабатываемой в информационной системе информации и основные угрозы, характерные для данной системы.

Помимо этого был проанализирован один из механизмов обеспечения информационной безопасности – процесс аудита информационных систем персональных данных и соответствующая нормативная документация, регулирующая отношения в области обработки персональных данных.

Была рассмотрена архитектура системы поддержки принятия решений, которая бы обеспечивала помощь в осуществлении процесса аудита, а именно – давала бы оценку состоянию защищённости информационной системе персональных данных и вырабатывала бы на её основе рекомендации по улучшению состояния защищённости.

Далее в работе рассматривался процесс построения модуля интеллектуального анализа данных, основанный на теории нечёткой логики и нечётких нейронных сетей, который осуществлял оценивание входных показателей, а именно требований к уровню защищённости информационной системы персональных данных. Данный модуль был построен в пакете Matlab с использованием адаптивной системы нейро-нечёткого вывода ANFIS. Работа данного модуля показала, что на основании предоставленных входных параметров результирующая оценка уровня защищённости оказалась выше среднего и составила 80%.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мамонова, В.Г. Моделирование бизнес-процессов: учебное пособие / В.Г. Мамонова, Н.Д. Ганелина, Н.В. Мамонова. Новосибирск: Новосибирский государственный технический университет, 2012. – 43 с.

2. Устав Федерального государственного бюджетного общеобразовательного учреждения высшего образования «Амурский государственный университет»: офиц. текст – Благовещенск: ФГБОУ ВО «АмГУ», 2016. – 38 с.

3. Ступина, А.А. Моделирование управляемых процессов: конспект лекций / А.А. Ступина, С.Н. Ежеманская, Л.Н. Корпачёва, А.В. Фёдорова. ФГОУ ВПО СибФУ. – Красноярск, 2008. – 158 с.

4. Александров, Д.В. Моделирование и анализ бизнес-процессов [Электронный ресурс]: учебник / Александров Д.В. – Электрон. текстовые данные. – Саратов: Ай Пи Эр Медиа, 2017. – 226 с. – Режим доступа: http://www.iprbookshop.ru/61086.html. – ЭБС «IPRbooks»

5. Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера»: офиц. текст – Москва: Кремль, 1997. – 1 с.

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

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

8. Петренко, С.А., Аудит безопасности Intranet: учебное пособие / С.А. Петренко, А.А. Петренко. ДМК Пресс, 2002 г. – 406 с.

9. Аверченков, В.И. Аудит информационной безопасности органов исполнительной власти [Электронный ресурс]: учебное пособие / В.И. Аверченков [и др.]. – Электрон. текстовые данные. – Брянск: Брянский государствен-

ный технический университет, 2012. – 100 с. – Режим доступа: http://www.iprbookshop.ru/6992.html. – ЭБС «IPRbooks»

10. 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.

11. 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.

12. Политика в отношении обработки персональных данных в ФГБОУ ВО «Амурский государственный университет»: офиц. текст – Благовещенск: ФГБОУ ВО «АмГУ», 2016. – 7 с.

13. Положение ПОД СМК 18-2016 Об обработке персональных данных в ФГБОУ ВО «АмГУ»: офиц. текст – Благовещенск: ФГБОУ ВО «АмГУ», 2016. – 35 с.

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

15. Малышева, Е.Н. Экспертные системы [Электронный ресурс]: учебное пособие по специальности 080801 «Прикладная информатика (в информационной сфере)» / Е.Н. Малышева. – Электрон. текстовые данные. – Кемерово: Кемеровский государственный институт культуры, 2010. – 86 с. – Режим доступа: http://www.iprbookshop.ru/22126.html. – ЭБС «IPRbooks»

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

17. 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.

18. 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»

19. 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. – Режим доступа: http://www.iprbookshop.ru/30835.html. – ЭБС «IPRbooks»

20. Постановление от 2003 года о введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы»: офиц. текст. Министерство Здравоохранения Российской Федерации, 2003. – 24 с.

21. Дьяконов, В.П. Справочник по применению системы PC MatLAB: учебное пособие / В.П. Дьяконов. – М.: Физматлит, 1993. – 112 с.

22. Занько, Н.Г. Безопасность жизнедеятельности: учебник / Н.Г. Занько, К.Р. Малаян, О.Н. Русак. 14-е изд., стер., Под ред. О.Н. Русака. – СПб.: Издательство «Лань», 2012. – 672 с.

23. ГОСТ Р 22.0.02-94 «БЧС. Термины и определения основных понятий»: офиц. текст. М.: ИПК Издательство стандартов, 2000. – 36 с.

ПРИЛОЖЕНИЕ А

Организационная структура ФГБОУ ВО «АмГУ» Факультета математики и информатики

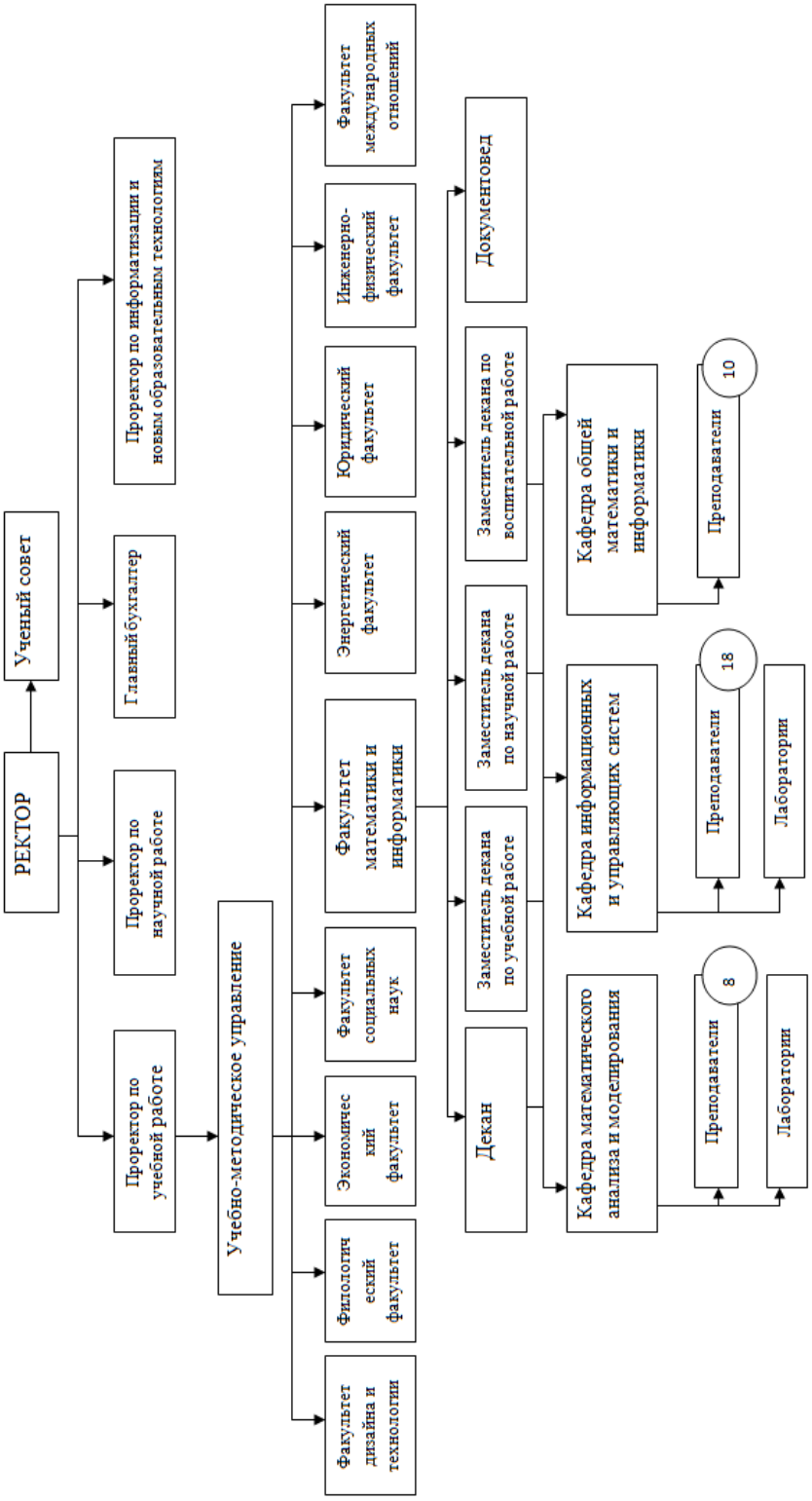

Рисунок А.1 – Организационная структура ФГБОУ ВО «АмГУ» Факультета математики и информатики

ПРИЛОЖЕНИЕ Б

Информационные потоки ФГБОУ ВО «АмГУ» деканата Факультета математики и информатики

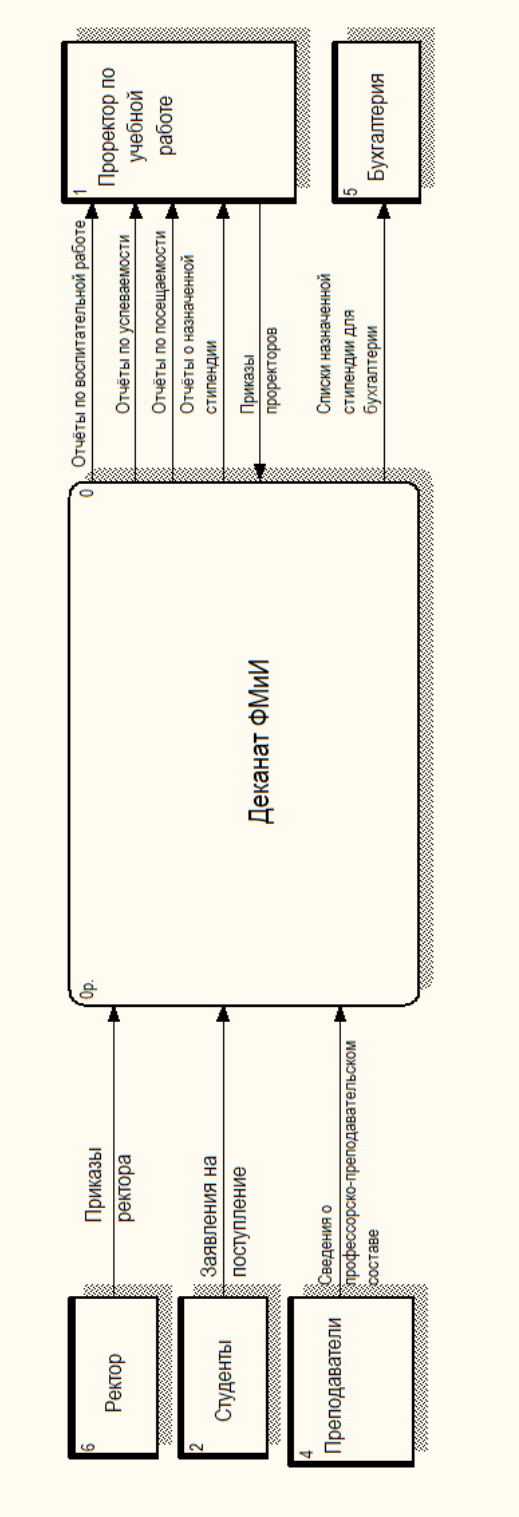

Рисунок Б.1 – Внешние информационные потоки

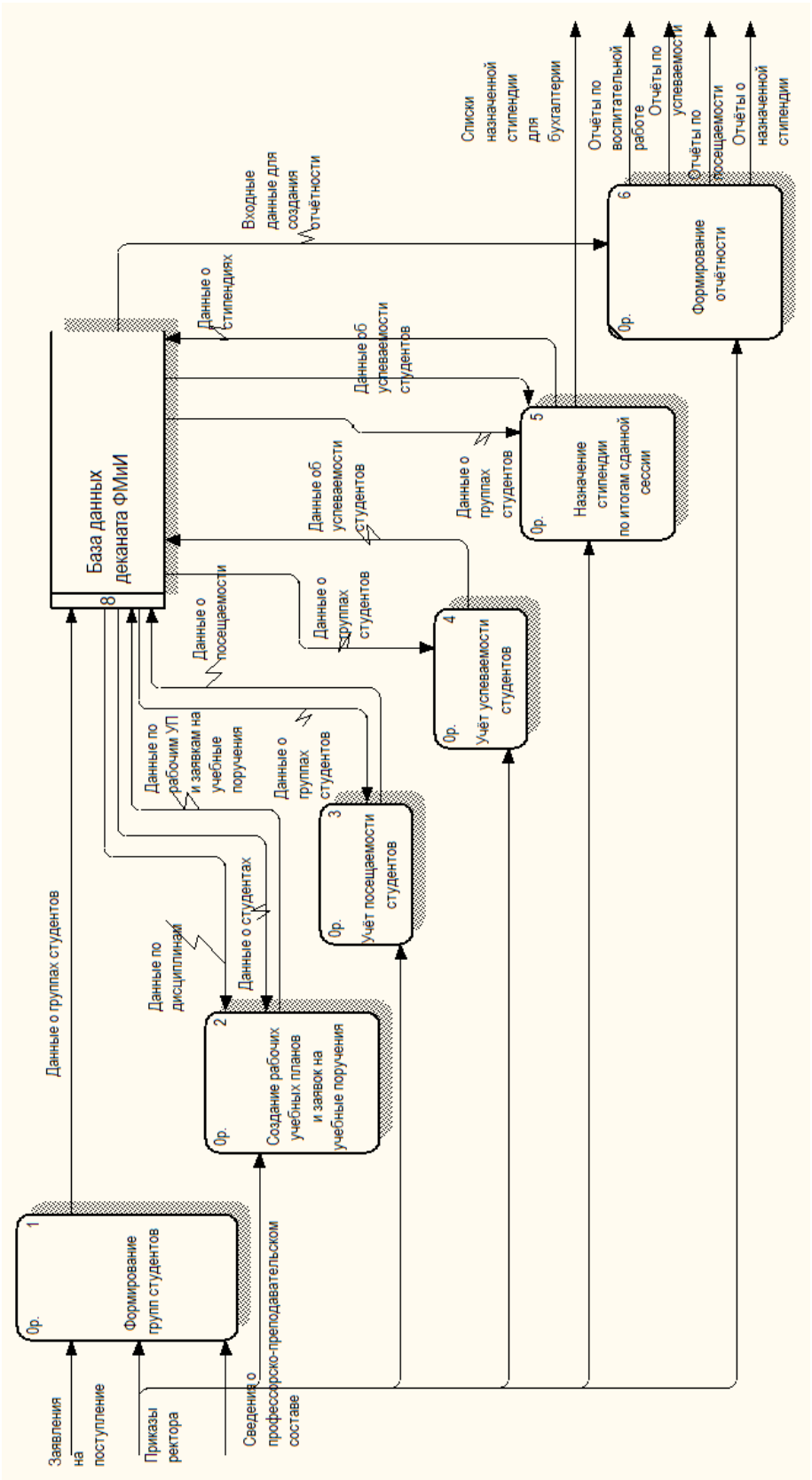

Рисунок Б.2 – Внутренние информационные потоки

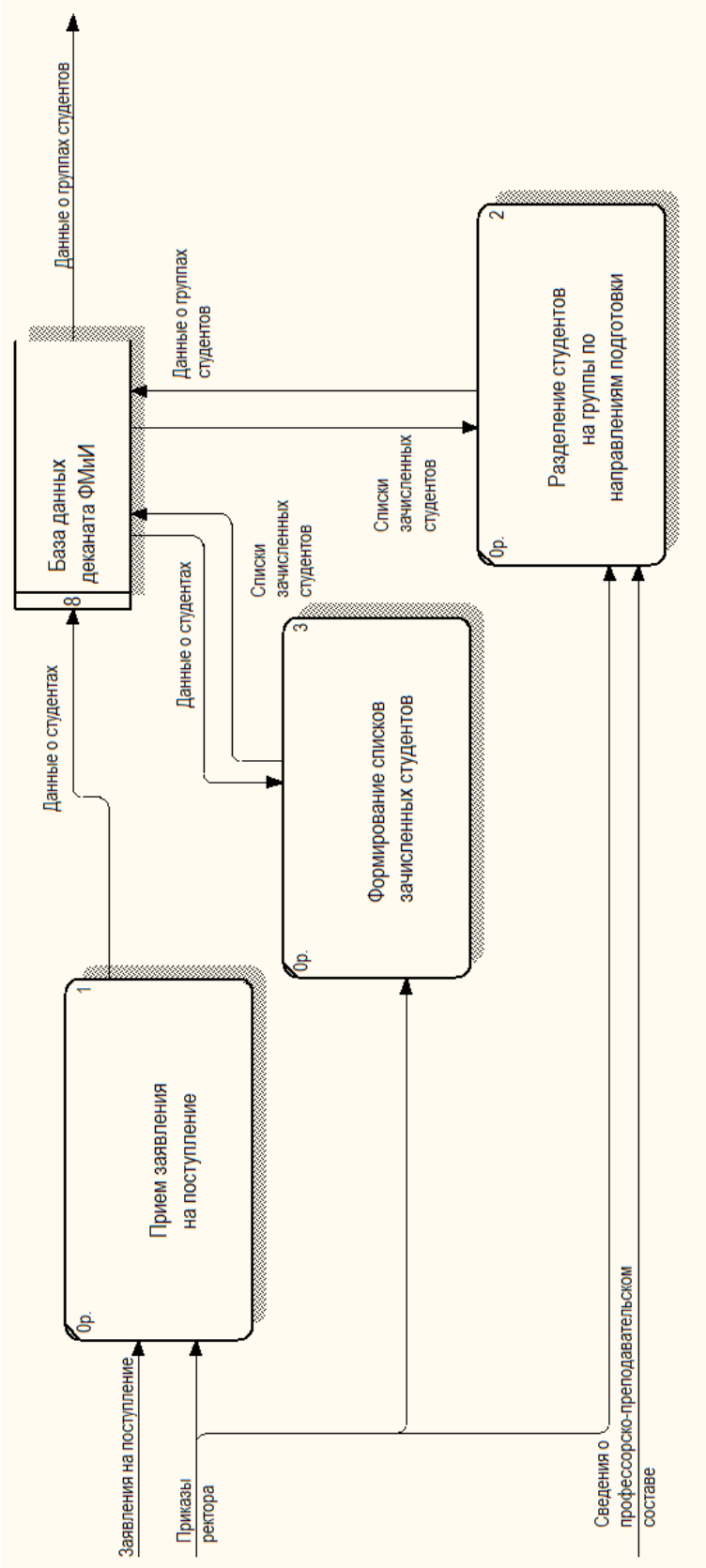

Рисунок Б.3 – Декомпозиция процесса «Формирование групп студентов»

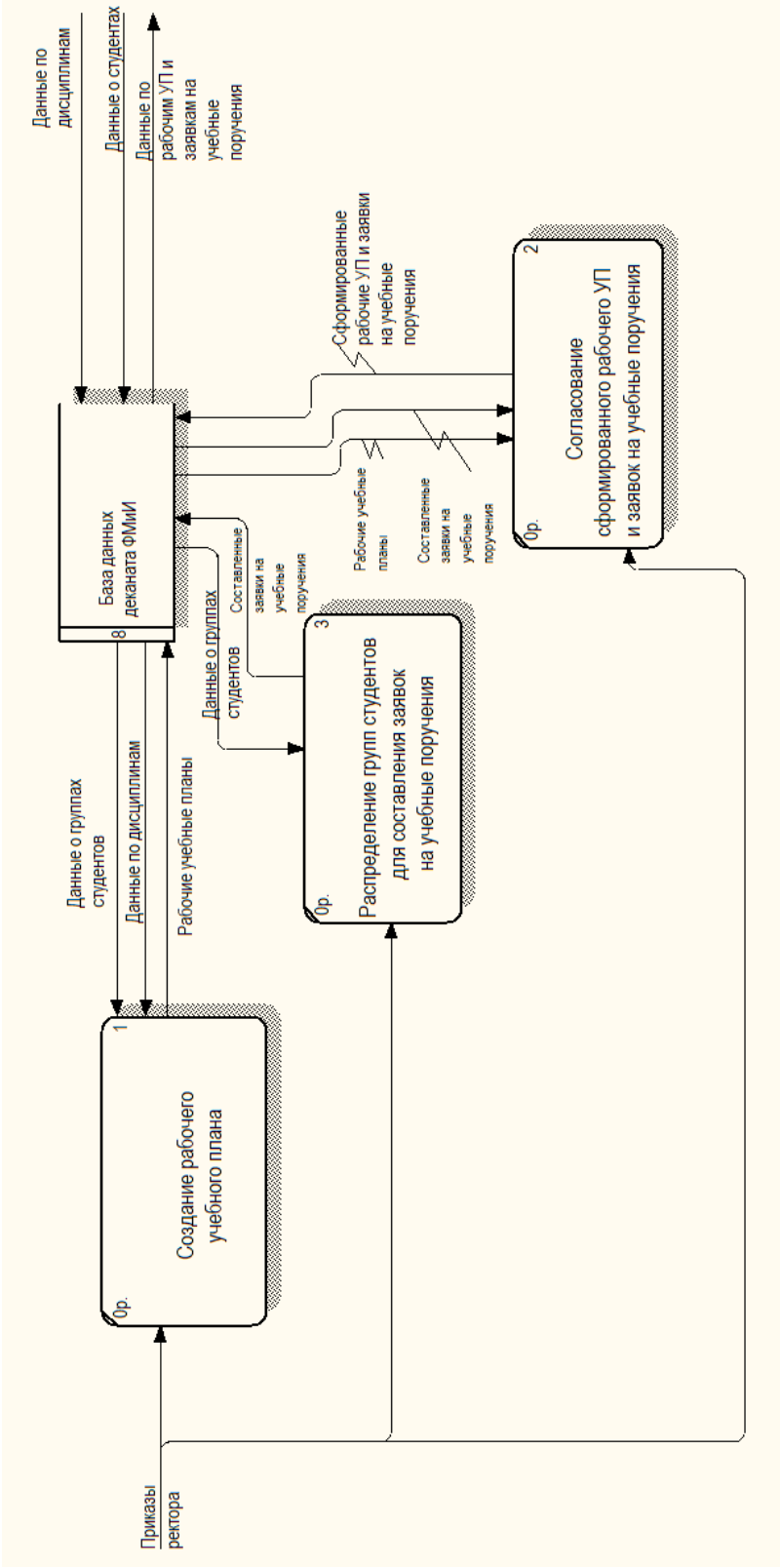

Рисунок Б.4 – Декомпозиция процесса «Создание рабочих учебных планов и заявок на учебные поручения»

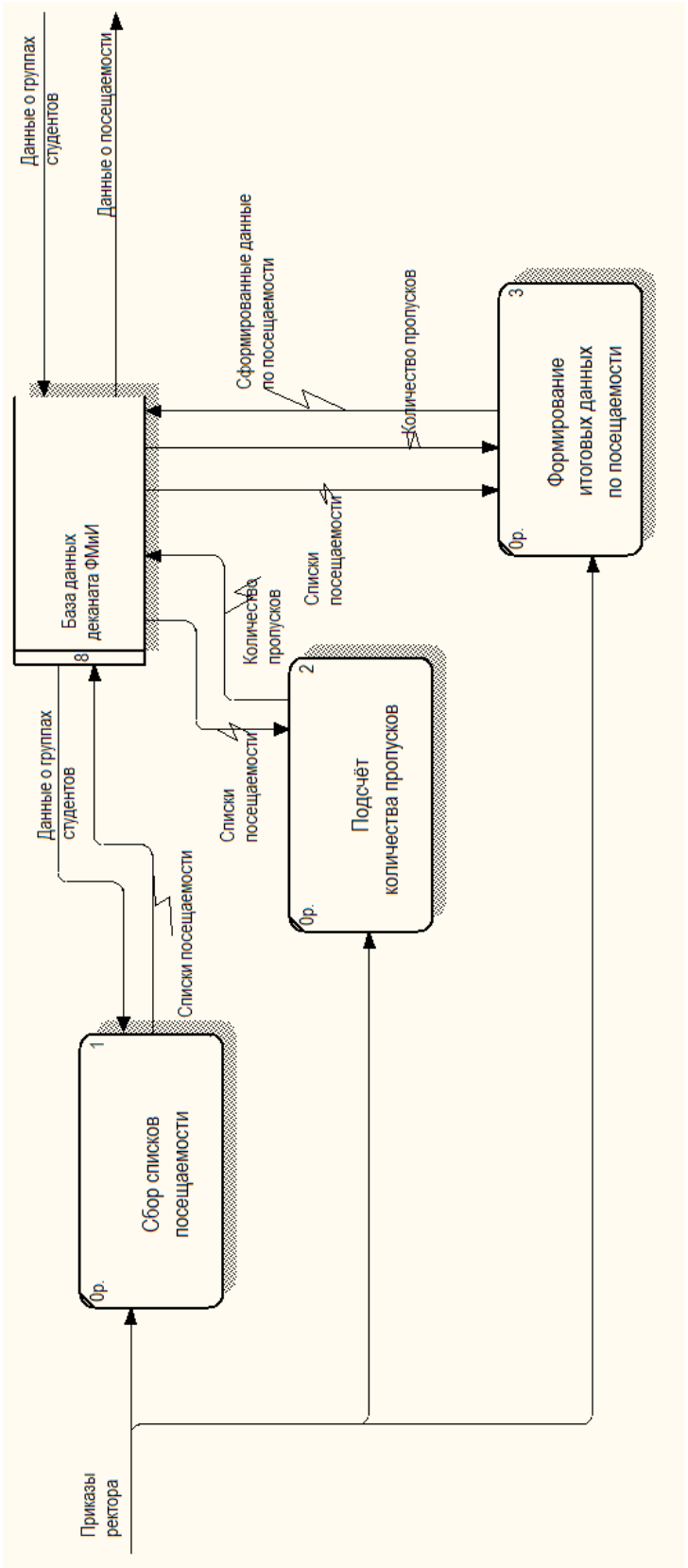

Рисунок Б.5 – Декомпозиция процесса «Учёт посещаемости студентов»

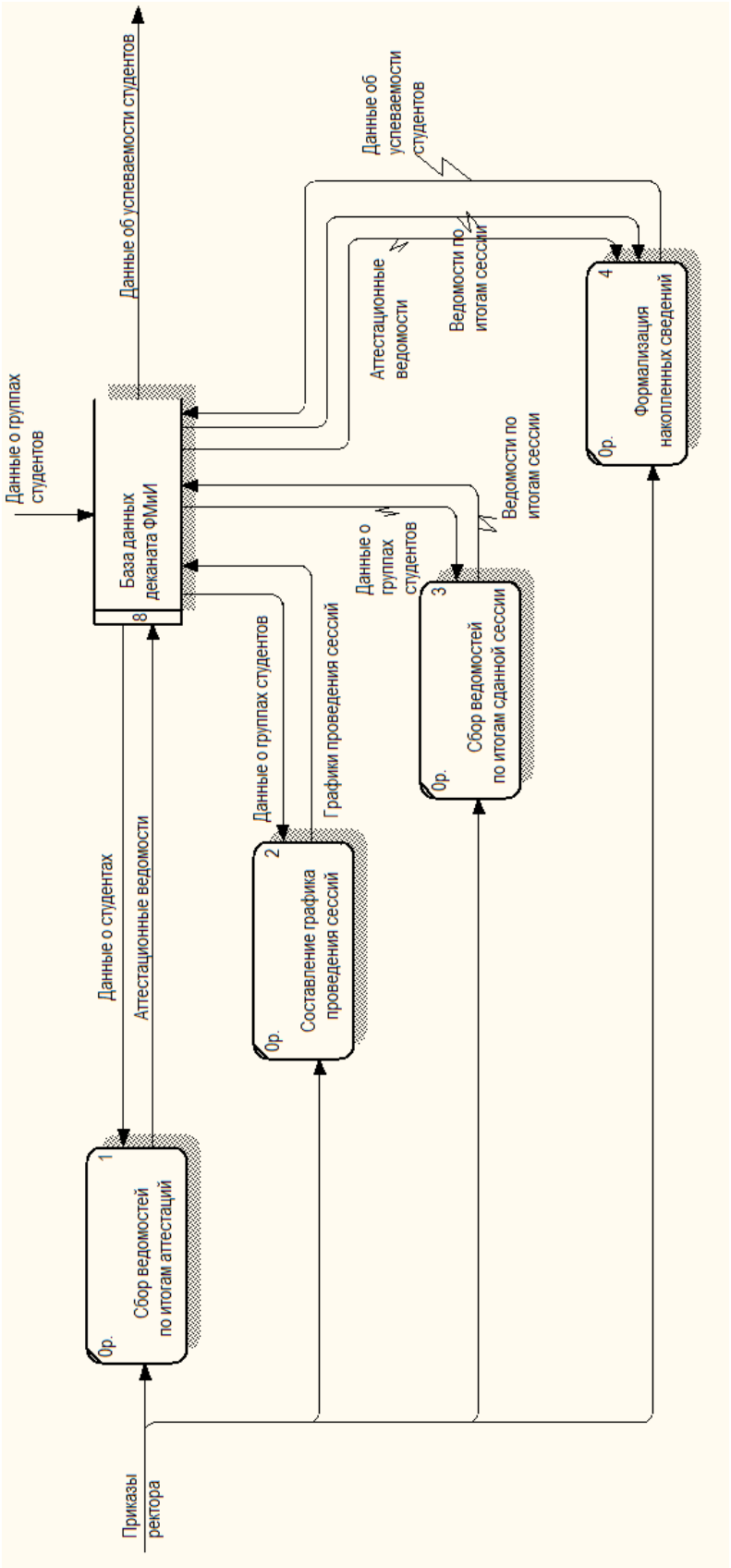

Рисунок Б.6 – Декомпозиция процесса «Учёт успеваемости студентов»

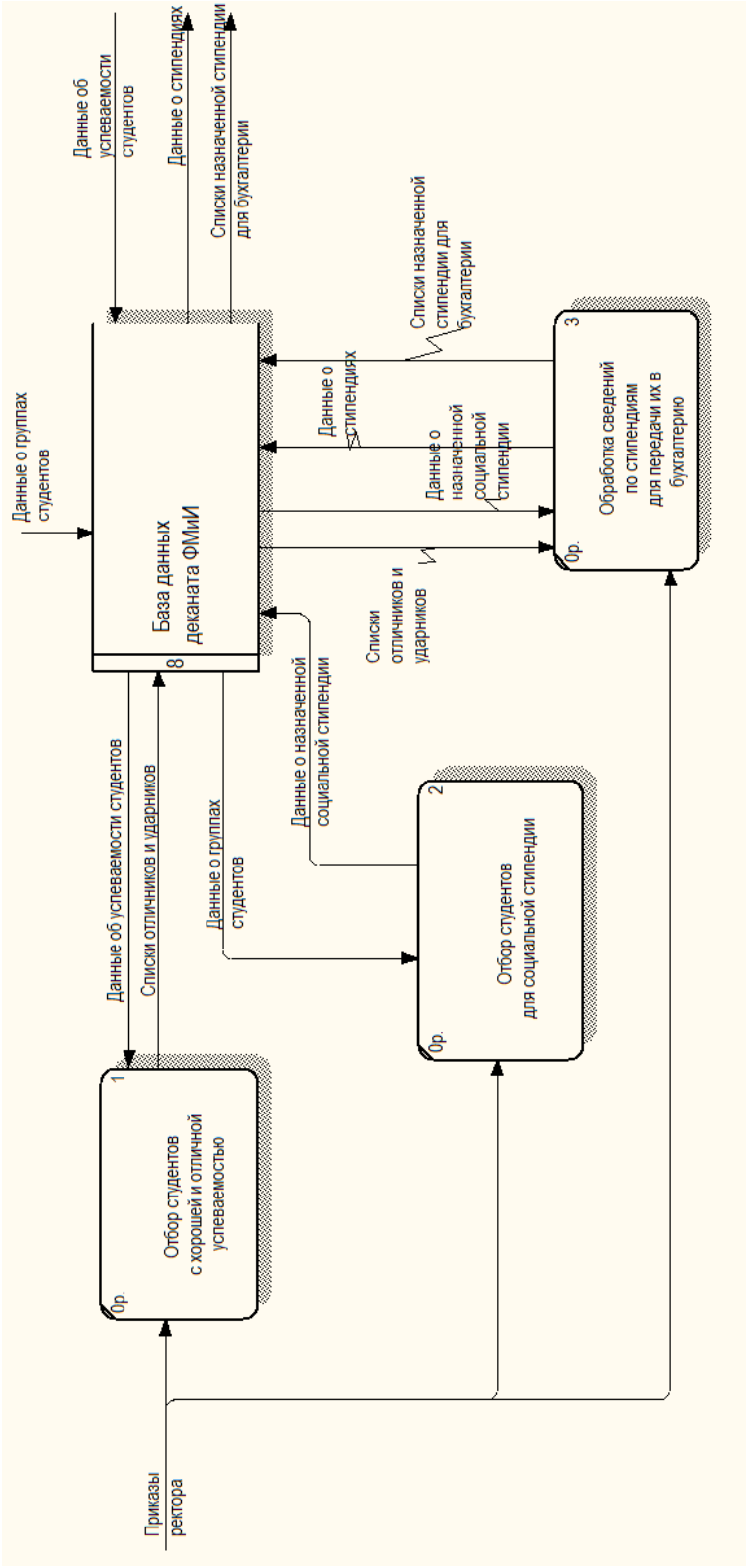

Рисунок Б.7 – Декомпозиция процесса «Назначение стипендии по итогам сданной сессии»

ПРИЛОЖЕНИЕ В

Классификация ИСПДн по уровням защищённости

Таблица В.1 – Классификация ИСПДн 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 Г

Требования к уровням защищённости

Таблица Г.1 – 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 Д

Архитектура системы поддержки принятия решений

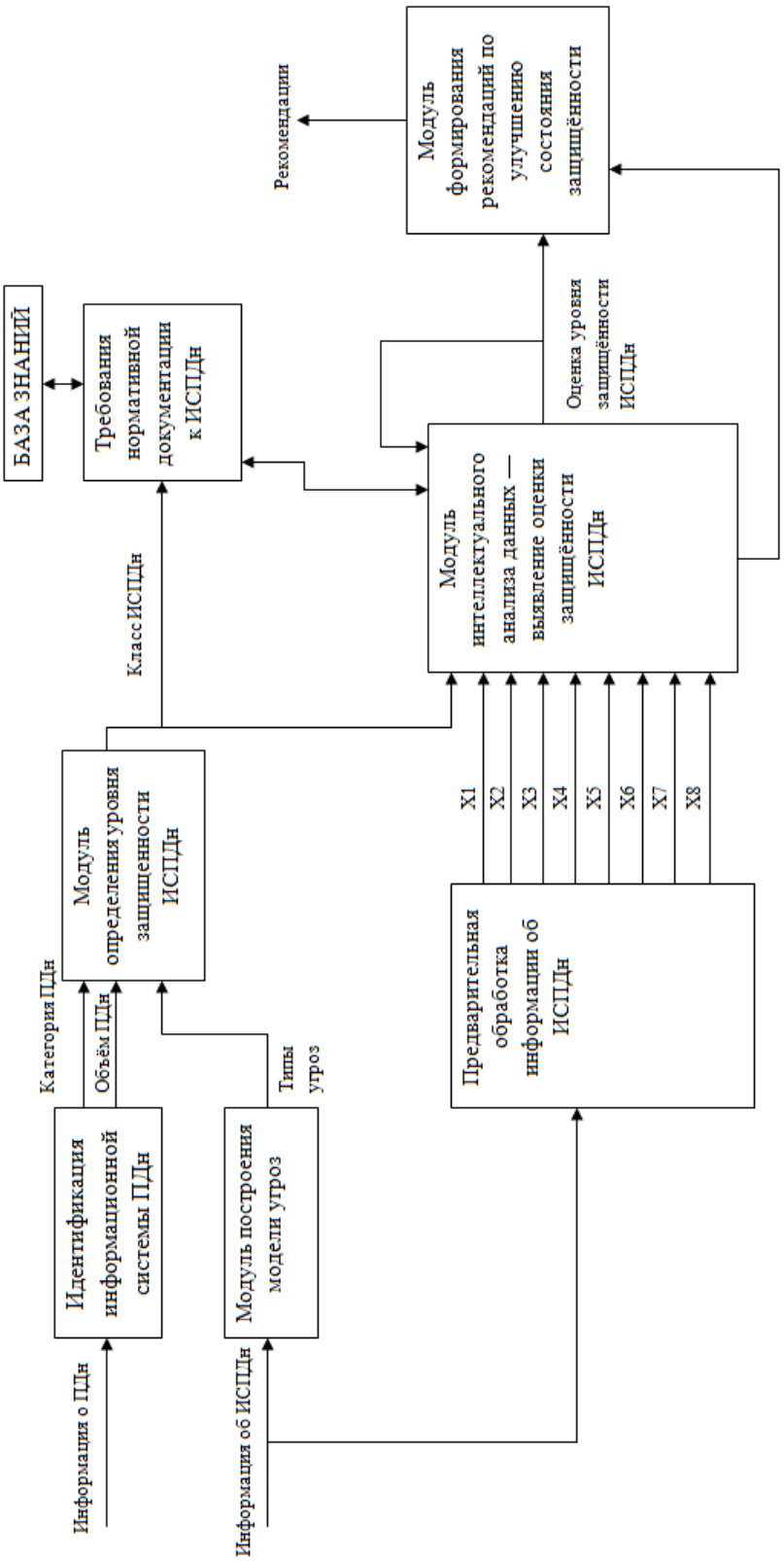

Рисунок Д.1 – Общая схема архитектуры СППР

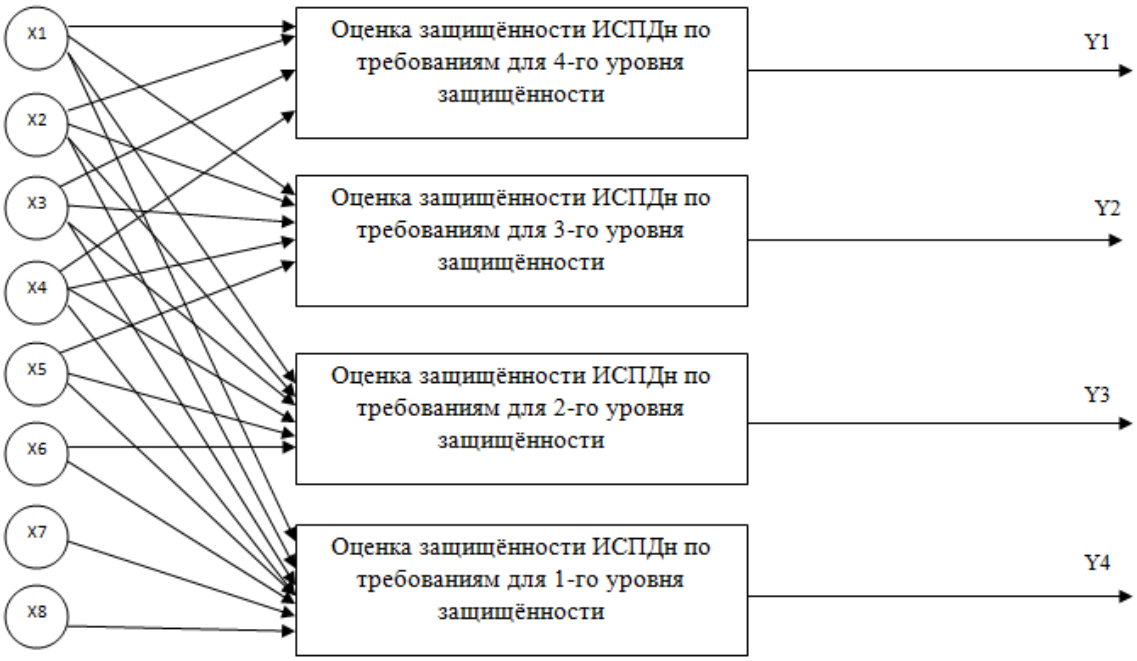

Рисунок Д.2 – Схема модуля интеллектуального анализа данных – выявление оценки защищённости ИСПДн

ПРИЛОЖЕНИЕ Е

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 Е.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 Е.2 – Продолжение базы правил для нечёткой нейронной сети

ПРИЛОЖЕНИЕ Ж

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 Ж.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 Ж.2 – Продолжение обучающей выборки для нечёткой нейронной сети

ПРИЛОЖЕНИЕ И

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:

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

2) Устав ФГБОУ ВО «АмГУ»;

3) требования к системе.

1.3 Наименование организаций – Заказчика и Разработчика

Заказчик: ФГБОУ ВО «Амурский государственный университет», кафедра ИиУС

Адрес фактический: г. Благовещенск, Игнатьевское шоссе, 21.

Телефон / Факс: +7 (416) 239-45-00

1.3.1 Разработчик

Разработчик: студентка факультета математики и информатики Дмитриева Анастасия Витальевна

Адрес фактический: г. Благовещенск, ул. Кантемирова.

Телефон / Факс: +7 (914) 585-12-35

1.4 Плановые сроки начала и окончания работы

Начало работ: 6.02.2017

Срок окончания работ: июнь 2017

1.5 Порядок оформления и предъявления заказчику результатов работ

Работы по созданию интеллектуальной СППР по проведению аудита ИСПДн сдаются Разработчиком поэтапно в соответствии с календарным планом Проекта. По окончании каждого из этапов работ Разработчик сдает Заказчику соответствующие отчетные документы этапа, состав которых определены Договором.

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 деканата факультета математики и информатики ФГБОУ ВО «Амурского государственного университета», а именно для выявления качественной оценки защищенности существующей в университете 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:

1) составление описания исследуемой информационной системы персональных данных;

2) классификация исследуемой информационной системы персональных данных по уровням защищенности;

3) построение моделей угроз и злоумышленников;

4) оценка уровня защищенности информационной системы персональных данных;

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

4.1.1 Требования к структуре и функционированию системы

Система поддержки принятия решений должна быть централизованной, т.е. все данные должны располагаться в центральном хранилище. В Системе предлагается выделить следующие функциональные подсистемы:

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

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

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

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

5) подсистема формирования рекомендаций для повышения уровня защищенности информационной системы.

СППР должна поддерживать следующие режимы функционирования:

1) основной режим, в котором подсистемы СППР выполняют все свои основные функции.

2) профилактический режим, в котором одна или все подсистемы СППР не выполняют своих функций.

В основном режиме функционирования СППР должна обеспечивать:

1) работу пользователей в режиме – 24 часов в день, 7 дней в неделю (24x7);

2) выполнение своих функций – сбор, обработка, хранение данных, выявление оценки, предоставление рекомендаций и отчетности.

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:

1) администратор – 1 человек;

2) пользователь – аудитор – 1 человек.

Данные лица должны 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.

Администратор следит за работой всей системы, реагирует на изменения, отлаживает неисправности, дает рекомендации по работе.

4.1.3 Показатели назначения

4.1.3.1 Требования к приспособляемости системы к изменениям

Обеспечение приспособляемости системы должно выполняться за счет:

1) своевременности администрирования;

2) модернизации процессов сбора и обработки данных в соответствии с новыми требованиями;

4.1.3.2 Требования сохранению работоспособности системы в различных вероятных условиях

При выходе из строя подсистем сбора и обработки данных, построения моделей угроз, определения уровня защищенности ИСПДн, интеллектуального анализа данных, формирования рекомендаций необходимо обеспечить своевременное уведомление администратора.

4.1.4 Требования к надежности

4.1.4.1 Состав показателей надежности для системы в целом

Надежность должна обеспечиваться за счет:

1) применения технических средств, системного и базового программного обеспечения, соответствующих классу решаемых задач;

2) соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;

4.1.4.2 Перечень аварийных ситуаций, по которым регламентируются требования к надежности

Под аварийной ситуацией понимается аварийное завершение процесса, выполняемого той или иной подсистемой СППР, а также «зависание» этого процесса.

При работе системы возможны следующие аварийные ситуации, которые влияют на надежность работы системы:

1) сбой в электроснабжении рабочей машины аудитора;

2) сбои программного обеспечения системы.

4.1.4.3 Требования к надежности технических средств и программного обеспечения

К надежности оборудования предъявляются следующие требования:

1) в качестве аппаратных платформ должны использоваться средства с повышенной надежностью;

2) применение технических средств соответствующих классу решаемых задач;

3) аппаратно-программный комплекс системы должен иметь возможность восстановления в случаях сбоев.

Надежность аппаратных и программных средств должна обеспечиваться за счет следующих организационных мероприятий:

1) предварительного обучения пользователей работы с системой;

2) соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;

3) своевременное выполнение процедур резервного копирования данных.

Надежность программного обеспечения подсистем должна обеспечиваться за счет:

1) надежности общесистемного ПО и ПО, разрабатываемого Разработчиком;

2) проведением комплекса мероприятий отладки, поиска и исключения ошибок;

3) ведением журналов системных сообщений и ошибок по подсистемам для последующего анализа и изменения конфигурации.

4.1.5 Требования к эргономике и технической эстетике

К подсистемам СППР предъявляются следующие требования к эргономике и технической эстетике.

В части внешнего оформления интерфейсы по подсистемам должен быть типизированы.

В части диалога с пользователем при возникновении ошибок в работе подсистемы на экран монитора должно выводиться сообщение с наименованием ошибки и с рекомендациями по ее устранению на русском языке.

В части процедур ввода-вывода данных должна быть возможность получения отчетности по мониторингу работы подсистем.

4.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Условия эксплуатации, а также виды и периодичность обслуживания технических средств Системы должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации завода-изготовителя (производителя) на них.

Размещение технических средств и организация автоматизированных рабочих мест должны быть выполнены в соответствии с требованиями ГОСТ 21958-76 «Система «Человек-машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования».

4.1.7 Требования к защите информации от несанкционированного доступа

4.1.7.1 Требования к информационной безопасности

Обеспечение информационной безопасности СППР должно удовлетворять следующим требованиям:

1) защита Системы должна обеспечиваться комплексом программно-технических средств и поддерживающих их организационных мер;

2) защита Системы должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;

3) программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики Системы (надежность, быстродействие, возможность изменения конфигурации).

4.1.8 Требования по сохранности информации при авариях

В Системе должно быть обеспечено резервное копирование данных.

4.1.9 Требования по стандартизации и унификации

Разработка системы должна осуществляться с использованием стандартных методологий функционального моделирования: IDEF0, DFD в рамках рекомендаций по стандартизации Р50.1.028-2001 «Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования».

Для работы с интеллектуальным анализом данных должно использоваться программное обеспечение MATLAB, а именно графический редактор адаптивных сетей ANFIS.

В системе должны использоваться общероссийские классификаторы и единые классификаторы и словари для различных видов алфавитно-цифровой и текстовой информации.

4.2 Требования к функциям, выполняемым системой

4.2.1 Подсистема сбора и обработки данных

Функции, подлежащие автоматизации:

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

2) идентификация ИСПДн: определение категории ПДн и их объем;

3) предварительная обработка данных об ИСПДн: определение требований к ИСПДн.

4.2.2 Подсистема построения моделей угроз и злоумышленников

Функции, подлежащие автоматизации:

1) определение перечня возможных угроз;

2) определение перечня возможных злоумышленников;

3) определение статуса каждой вероятной угрозы.

4.2.3 Подсистема определения уровня защищенности ИСПДн

Функции, подлежащие автоматизации:

1) на основании сведений о персональных данных и модели угроз и злоумышленников определение уровня защищенности ИСПДн и отнесение ее к конкретному классу ИСПДн.

4.2.4 Подсистема интеллектуального анализа данных

Функции, подлежащие автоматизации:

1) на основании текущего уровня защищенности ИСПДн и выявленным требованиям к ИСПДн определение оценки защищенности ИСПДн при помощи модульной нейронной сети.

4.2.5 Подсистема формирования рекомендаций

Функции, подлежащие автоматизации:

1) 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.

4.3.2 Требования к информационному обеспечению

4.3.2.1 Требования к информационной совместимости со смежными системами

Система не должна быть закрытой для смежных систем и должна поддерживать возможность экспорта данных в смежные системы через интерфейсные таблицы или файлы данных.

Система должна обеспечить возможность загрузки данных, получаемых от смежной системы.

4.3.2.2 Требования по использованию классификаторов, унифицированных документов и классификаторов

Система, по возможности, должна использовать классификаторы и справочники, которые ведутся в системах-источниках данных.

Основные классификаторы и справочники в системе должны быть едиными.

4.3.3 Требования к лингвистическому обеспечению

Должны выполняться следующие требования к кодированию и декодированию данных: windows cp1251 для подсистемы сбора и обработки данных; Windows cp1251 информации, поступающей из систем-источников.

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.

4.3.4 Требования к программному обеспечению

К обеспечению качества программных средств предъявляются следующие требования:

1) функциональность должна обеспечиваться выполнением подсистемами всех их функций.

2) надежность должна обеспечиваться за счет предупреждения ошибок - не допущения ошибок в готовых программных средствах;

3) легкость применения должна обеспечиваться за счет применения покупных программных средств;

4) эффективность должна обеспечиваться за счет принятия подходящих, верных решений на разных этапах разработки программного средства и системы в целом;

5) сопровождаемость должна обеспечиваться за счет высокого качества документации по сопровождению;

6) также на каждом этапе в разработке программного средства должна проводится проверка правильности принятых решений по разработке и применению готовых программных средств.

Необходимость согласования вновь разрабатываемых программных средств с фондом алгоритмов и программ отсутствует.

4.3.5 Требования к техническому обеспечению

Система должна быть реализована с использованием специально выделенного сервера Заказчика.

4.3.6 Требования к метрологическому обеспечению

Не предъявляются.

4.3.7 Требования к организационному обеспечению

Основными пользователями системы являются сотрудники функционального подразделения Заказчика – аудитор.

Обеспечивает эксплуатацию Системы подразделение информационных технологий Заказчика.

К защите от ошибочных действий персонала предъявляются следующие требования:

1) должна быть предусмотрена система подтверждения легитимности аудитора при просмотре данных;

2) для аудитора должна быть запрещена возможность удаления преднастроенных объектов и отчетности;

3) для снижения ошибочных действий аудитора должно быть разработано полное и доступное руководство пользователя.

4.3.8 Требования к методическому обеспечению

В состав входят следующие компоненты:

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

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

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

4.3.9 Требования к патентной чистоте

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

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

Работы по созданию системы выполняются в три этапа:

1) проектирование. Разработка эскизного проекта. Разработка технического проекта;

2) разработка рабочей документации. Адаптация программ;

3) ввод в действие.

Конкретные сроки выполнения стадий и этапов разработки и создания Системы определяются Планом выполнения работ, являющимся неотъемлемой частью Договора на выполнение работ по настоящему Частному техническому заданию.

Перечень организаций - исполнителей работ, определение ответственных за проведение этих работ организаций определяются Договором.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

6.1 Виды и объем испытаний системы

Система подвергается испытаниям следующих видов:

1) предварительные испытания;

2) опытная эксплуатация;

3) приемочные испытания.

Состав, объем и методы предварительных испытаний системы определяются документом «Программа и методика испытаний», разрабатываемым на стадии «Рабочая документация».

Состав, объем и методы опытной эксплуатации системы определяются документом «Программа опытной эксплуатации», разрабатываемым на стадии «Ввод в действие».

Состав, объем и методы приемочных испытаний системы определяются документом «Программа и методика испытаний», разрабатываемым на стадии «Ввод в действие» с учетом результатов проведения предварительных испытаний и опытной эксплуатации.

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

7.1. Технические мероприятия

Силами Заказчика в срок до начала этапа «Разработка рабочей документации. Адаптация программ» должны быть выполнены следующие работы:

1) осуществлена подготовка помещения для размещения аппаратно-технического комплекса системы в соответствии с требованиями, приведенными в настоящем техническом задании;

2) осуществлена закупка и установка необходимого аппаратно-технического комплекса;

7.2. Организационные мероприятия

Силами Заказчика в срок до начала этапа работ «Разработка рабочей документации. Адаптация программ» должны быть решены организационные вопросы по взаимодействию с системами-источниками данных. К данным организационным вопросам относятся:

1) организация доступа к базам данных источников;

2) определение регламента информирования об изменениях структур систем-источников;

3) выделение ответственных специалистов со стороны Заказчика для взаимодействия с проектной командой по вопросам взаимодействия с системами-источниками данных.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

На этапе «Проектирование. Разработка эскизного проекта. Разработка технического проекта» разрабатываются следующие документы:

1) пояснительная записка к эскизному проекту;

2) пояснительная записка к техническому проекту;

3) схема функциональной структуры.

На этапе «Разработка рабочей документации. Адаптация программ» разрабатываются следующие документы:

1) ведомость эксплуатационных документов;

2) общее описание системы;

3) технологическая инструкция;

4) руководство пользователя;

5) описание технологического процесса обработки данных;

6) инструкция по формированию и ведению набора данных;

7) состав выходных данных;

8) описание программ.

На этапе «Ввод в действие» разрабатываются следующие документы:

1) акт приёмки в опытную эксплуатацию;

2) акт приемки Системы в промышленную эксплуатацию;

3) акт завершения работ.

Вся документация должна быть подготовлена и передана как в печатном, так и в электронном виде (в формате Microsoft Word).

9 ИСТОЧНИКИ РАЗРАБОТКИ

Настоящее Техническое Задание разработано на основе следующих документов и информационных материалов:

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

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

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

4) Устав ФГБОУ ВО «АмГУ»;

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

6) ГОСТ 21958-76 «Система "Человек-машина". Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования».