МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт **математики, физики и информационных технологий**

Кафедра **«Прикладная математика и информатика»**

01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ И КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

БАКАЛАВРСКАЯ РАБОТА

на тему **Разработка алгоритма анализа информационных угроз на основе нейронной сети (на примере Пенсионного фонда РФ)**

Студент А.В. Смольянинова _____

Руководитель А.И. Туищев _____

Консультант по аннотации Н.В. Ященко _____

Допустить к защите

Заведующий кафедрой А.В. Очеповский _____

«_____» _____ 20___ г.

Тольятти 2017

АННОТАЦИЯ

Тема: Разработка алгоритма анализа информационных угроз на основе нейронной сети (на примере Пенсионного фонда РФ)

Ключевые слова: РАЗРАБОТКА, АЛГОРИТМ, ИНФОРМАЦИОННЫЕ УГРОЗЫ, КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ, НЕЙРОННЫЕ СЕТИ.

Целью ВКР является разработка алгоритма анализа информационных угроз.

Объектом исследования является система защиты данных в ПФР.

Предмет исследования – алгоритм анализа информационных угроз.

Первая глава ВКР описывает организационную структуру Пенсионного фонда РФ, основные аспекты в защите информации и информационных потоков в организации и возможные атаки на систему.

Во второй главе происходит выбор архитектуры нейронной сети и конструирование на её основе алгоритма анализа поступившей на вход информации на наличие атаки. Так же показываются преимущества и недостатки использования нейронных сетей для защиты информации.

В третьей главе описываются возможные атаки, и как система будет реагировать на них с применением нейронной сети. Данная работа производилась под контролем главного специалиста по защите информации в Пенсионном фонде.

ВКР состоит из 45 страниц, 9 таблиц, 14 картинок и 13 формул.

ABSTRACT

The title of graduation work is “The Development of an Informational Threats Algorithm Based on Neural Networks”. The object of the work is neural network. The subject of the graduation work is the model of security system. And the aim of work represents the construction of the neural networks model. The actuality of this work is that nowadays hackers create lots of difficult algorithms to brake security systems and many of the means of protection have become obsolete.

The first part of the work consists of information about customer’s company. It represents its structure and methods of working in security. It shows today’s situation on the firm and weaknesses of used programs and tools. The first part includes an analyzing part of work: which parts of the structure are in danger.

The second part of the graduation work describes mathematics ways to understand which neural network would be better to use. It also shows different types of attacks on networks and how networks can be used for such problems. The part shows not only plusses of using neural networks in the sphere of data security, also it describes all the limitations of applying it.

The third part consists of design and modeling of the system. It shows various areas and functions of security system. This part was developed in the company under the guidance of information security specialists.

The work contains 45 pages, 9 tables, 14 schemas and 13 formulas.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В выпускной квалификационной работе (ВКР) будет рассмотрено решение задач защиты данных в Пенсионном фонде Российской Федерации (ПФР) с использованием нейронной сети в качестве концепции обеспечения безопасности.

Актуальность данной работы связана с тем, что складывается устойчивая тенденция к увеличению количества атак на вычислительные системы и сети. Технологии и методы удаленных сетевых атак постоянно совершенствуются, и существующие средства защиты не позволяют полностью пресекать злонамеренный трафик. Эти обстоятельства делают разработку и внедрение новых методов и средств защиты информации в вычислительных сетях весьма актуальными. На сегодняшний день системы безопасности, работающих с использованием нейросетевых технологий, весьма востребованы.

Цель ВКР: разработка алгоритма анализа информационных угроз на основе нейронной сети.

Объект ВКР: система защиты данных в ПФР РФ.

Предмет ВКР: алгоритм анализа информационных угроз.

Задачи выпускной квалификационной работы:

- ознакомление с актуальными сетевыми атаками в ПФР РФ и методами их предотвращения;
- разработка алгоритма анализа информационных угроз ПФР РФ на основе нейронной сети;
- разработка модели системы безопасности на основе предлагаемого алгоритма.

Глава 1. СЕТЕВЫЕ АТАКИ И МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ

1.1Актуальные модели угроз и средства защиты от них в ПФР

Управление Пенсионного фонда представляет собой подразделение, находящееся в непосредственном подчинении Отделения Пенсионного фонда РФ, которое в свою очередь является зависимым от Отделения Пенсионного фонда РФ федерального значения, расположенного в Москве.

Таким образом, структура подчиненности состоит из таких звеньев, как:

- Управление ПФР по городу
- Отделение ПФР по области (краю, республике)
- Отделение ПФР федерального значения

Схема информационных взаимосвязей этих групп изображена на рисунке 1.1.

Рисунок 1.1 - Схема информационных связей ПФР Самарской области

Анализ основных направлений работы государственного учреждения и задач, им решаемых, позволяет разделить основные производственные процессы учреждения на несколько групп:

1) финансово-экономическая группа;
2) отдел по защите информации, отдел автоматизации;
3) юрисконсульт;
4) специалист по кадрам и делопроизводству;
5) клиентская служба;
6) отдел назначения и перерасчета пенсии;
7) отдел оценки пенсионных прав застрахованных лиц;
8) отдел персонифицированного учета;
9) отдел администрирования страховых взносов, взыскания задолженностей и взаимодействия со страхователями.

В связи с тем, что некоторые отделы связаны друг с другом, они объединены в некое подобие групп. У этих групп есть свои начальники в лицах заместителей начальника Управления (рисунок 1.2).

Рисунок 1.2 - Структура Управления ПФР

Для работы с информационными базами данных в УПФР используются несколько модулей:

- внутренние базы данных – когда специалист работает с данными, уже имеющимися в определенных программах. Например, “Клиентская служба ПФР”.
- внешнее поступление информации в базы данных - например, сайт “Госуслуги”.
- электронный документооборот: получение данных из сторонних организаций, из других управлений, из МФЦ.

Информационная система персональных данных ПФР предназначена для обеспечения деятельности ПФР и его территориальных органов, составляющих единую централизованную систему органов управления средствами обязательного пенсионного страхования и пенсионного обеспечения в Российской Федерации, в которой нижестоящие органы подотчетны вышестоящим.

Целью обеспечения безопасности персональных данных при их обработке в информационной системе ПФР является обеспечение состояния защищенности прав и свобод человека и гражданина при обработке его персональных данных в ПФР, которые гарантирует федеральное законодательство, а также состояния защищенности системы обязательного пенсионного страхования и пенсионного обеспечения в Российской Федерации от внешних и внутренних угроз.

Угрозы могут быть внешними или внутренними в зависимости от дислокации источников угроз вне или внутри контролируемой зоны охраняемых объектов ПФР соответственно.

При этом в случае обработки персональных данных (организации персонифицированного учета) в электронной форме должны обеспечиваться гарантии их достоверности и защиты от искажений и несанкционированного доступа.

Перечень угроз безопасности персональных данных ПФР:

− противоправное распространение персональных данных;

− несанкционированное использование персональных данных, порождающее юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

− несанкционированное блокирование персональных данных;

− несанкционированное уничтожение персональных данных;

− несанкционированное изменение персональных данных;

− неправомерный или случайный доступ к персональным данным;

− неправомерное копирование персональных данных;

− иные неправомерные действия.

Модель угроз безопасности персональных данных предназначена для использования при классификации информационной системы персональных данных ПФР и разработки системы их защиты.

Возможными последствиями нарушения безопасности персональных данных, обрабатываемых в ПФР, являются:

− возникновение социальной напряженности в одном или нескольких регионах Российской Федерации из-за дезорганизации работы органов Пенсионного фонда Российской Федерации;

− разглашение персональных данных граждан и причинение материального ущерба;

− причинение материального ущерба ПФР;

− вред репутации Пенсионного фонда Российской Федерации в обществе.

Объектами угроз в ИСПД ПФР, подлежащими защите, являются информационные ресурсы, содержащие персональные данные, корпоративная сеть передачи данных, информационные технологии, технические и программные средства, используемые для обработки персональных данных, аппаратные и программные средства защиты.

Основными информационными ресурсами, содержащими персональные данные, в ИСПД являются ресурсы:

- подсистемы персонифицированного учета;
- подсистемы назначения и выплаты государственных пенсий;
- «АРМ взаимодействия со страхователями» ПТК «Страхователи»;
- «АРМ Конвертация»;
- комплекса «Герои»;
- ОГБД «Ветераны»;
- программного комплекса «1С»;
- Электронный архив персонифицированного учета;
- Федеральный регистр лиц, имеющих право на получение государственной социальной помощи;
- Федеральный регистр лиц, имеющих право на дополнительные меры государственной поддержки;
- Информационный ресурс по информированию застрахованных лиц;
- Электронный архив выплатных дел.

Основными угрозами безопасности персональных данных является нарушение их конфиденциальности, целостности доступности и аутентичности.

Формирование Модели угроз осуществлено на основе определенных ранее угроз безопасности персональных данных при их обработке. Проведен анализ перечня угроз безопасности персональных данных с учетом оперативной обстановки, складывающейся вокруг ПФР, имеющихся доступных материалов о реально зафиксированных угрозах безопасности персональных данных с учетом опыта ПФР, различных кредитных организаций, а также имеющемся на общедоступном рынке средств защиты и средств технической разведки в информационной сфере.

При этом были выполнены требования нормативных правовых актов и учтены положения методических документов Федеральной службы

безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

Модель нарушителя безопасности персональных данных

Нарушители безопасности персональных данных могут осуществлять целенаправленные действия по нарушению безопасности информации или созданию условий для этого – атаки – как из-за пределов контролируемой зоны (внешние нарушители), так и в пределах контролируемой зоны (внутренние нарушители).

Основными объектами атак являются:

− документация, технические и программные компоненты;

− ресурсы персональных данных;

− ключевая аутентифицирующая и парольная информация;

− криптографически опасная информация;

− аппаратные и программные средства защиты;

− технические и программные компоненты среды функционирования криптосредства;

− данные, передаваемые по каналам связи;

− помещения, в которых размещены ресурсы ИСПД.

Целью атаки является неправомерный доступ к информации или к вычислительным ресурсам ИСПД как с умыслом нанесения ущерба ПФР, так и без такого умысла.

Предполагается, что потенциальные нарушители:

− не могут организовывать или заказывать работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств и среды их функционирования;

− являются, в силу специфики информации ИСПД, одиночками, самостоятельно осуществляющими освоение способов, подготовку и проведение атак.

Привилегированные пользователи ИСПД (администраторы), которые осуществляют техническое управление и обслуживание аппаратных и программных средств ИСПД, в том числе и средств защиты, включая их настройку, конфигурирование и распределение ключевой и парольной документации, относятся к особо доверенным лицам и исключаются из числа потенциальных нарушителей.

Показатели исходной защищенности информационной системы персональных данных, влияющие на актуальность угроз безопасности персональных данных:

1) по территориальному признаку – распределенная информационная система, охватывающая Российскую Федерацию в целом (низкий уровень исходной защищенности);

2) по наличию соединений с сетями общего пользования – информационная система имеет многоточечный выход в телекоммуникационные сети общего пользования (низкий уровень исходной защищенности);

3) по встроенным (легальным) операциям с записями баз персональных данных – чтение, поиск, запись, удаление, сортировка, модификация, передача персональных данных (низкий уровень исходной защищенности);

4) по разграничению доступа к персональным данным – доступ имеет определенный приказами руководителя органа ПФР перечень сотрудников (средний уровень исходной защищенности);

5) по наличию соединений с другими базами персональных данных других информационных систем персональных данных – в информационной системе используются только базы данных принадлежащие Пенсионному фонду Российской Федерации (высокий уровень исходной защищенности);

6) по уровню обобщения (обезличивания) персональных данных – предоставляемые пользователю данные не являются обезличенными (низкий уровень исходной защищенности);

7) по объему персональных данных, которые предоставляются сторонним пользователям информационной системы персональных данных – сторонним пользователям предоставляется часть персональных данных (высокий уровень исходной защищенности).

1.2 Модель процесса защиты информационных потоков в ПФР

На рисунке 1.3 представлена диаграмма IDEF0, на которой рассматривается работа криптографических средств защиты в ПФР.

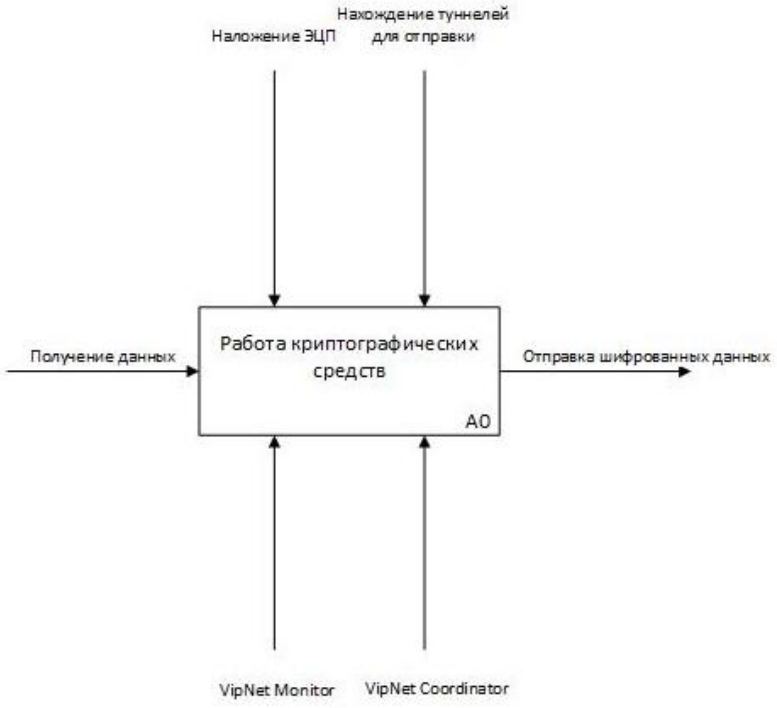

Рисунок 1.3 - IDEF0-диаграмма схемы <AS-IS> работы системы защиты в ПФР

На диаграмме показано, что на вход поступают некоторые данные, которые до отправки шифруются специальными средствами VipNet.

На диаграмме (рисунок 1.4) показано декомпозиция контекстной диаграммы <AS-IS>. На ней находятся:

1) Рабочее место – рабочее место сотрудника, с установленным VipNet Monitor, с помощью которого происходит отправка данных. Установлено в территориальном органе (Управлении).
2) VipNet Coordinator – средство шифровки данных. Установлен на обоих концах туннелированного канала. На одном- шифрует данные, на втором – происходит расшифровка.
3) Туннелированный канал – специально проложенный канал, по которому передаются шифрованные данные.
4) Информационная база данных – специальное хранилище данных, установленное в региональном управлении (Отделении).

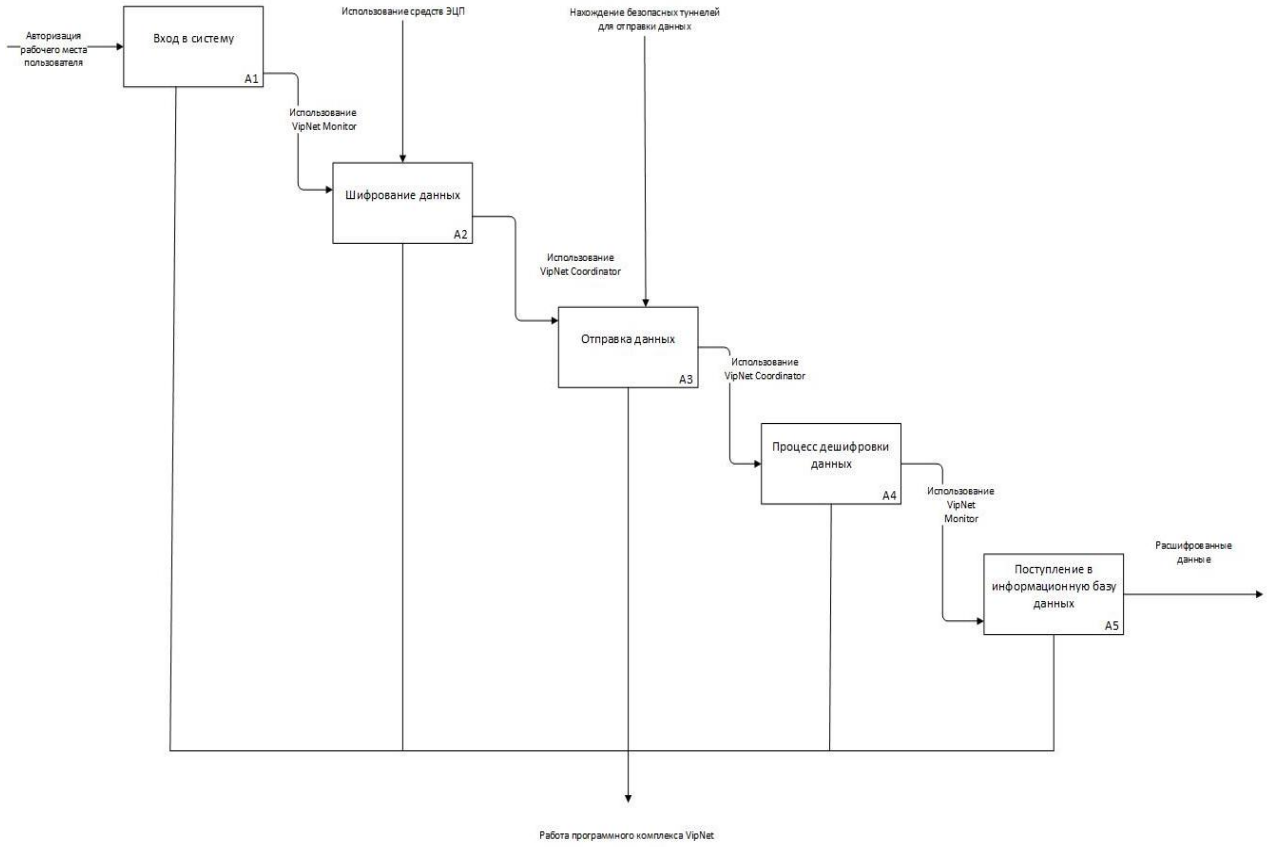

Рисунок 1.4 - Контекстная диаграмма проверки заданий для заочной формы обучения с применением дистанционных технологий «КАК ЕСТЬ» в методологии IDEF0 (1-й уровень)

На данной диаграмме изображены следующие элементы:

- Входные данные: авторизация в системе, после которой следует автоматическое включение VipNet Monitor;
- Выходные данные: переданная информация, занесенная в специальную базу данных.

- Управляющие воздействия: нахождение специальных туннелей передачи данных, использование средств ЭЦП (электронно-цифровой подписи)

1.3 Формирование требований к новой технологии

В данной технологии злоумышленник не сможет напрямую попасть в базу данных, однако существует вероятность нападения на VipNet Coordinator и перехвата зашифрованных данных. Атака производится в точке входа (выхода) с одного из уровней.

В настоящее время для защиты данных от несанкционированного доступа изобретено множество программных продуктов. Однако большинство из них основаны на использовании правил и сигнатур, с помощью которых анализируется вектор входных данных и на основании чего делается вывод о наличии атаки или же её отсутствии. Однако, для успешного нахождения и предотвращения атак бд, сигнатуры и правила требуют постоянного ручного или автоматизированного обновления и , если производится атака, которая не предусмотрена в новых установленных обновлениях, то она пройдет успешно и произойдет вторжение в базу данных. Поэтому из-за большого разнообразия атак в современных системах обнаружения атак используются нейросетевые средства.

С помощью правильно обученной нейронной сети можно забыть о постоянных обновлениях баз, так как если обучить сеть определенным алгоритмам и методам, то а обнаружение сетевых атак будет затрачиваться меньшее количество времени, потому что она способна находить и останавливать атаки по неполным и частично недостоверным исходным данным. Так же сеть способна самообучаться: на основе накопленных правил

и данных об атаках, нейросеть может создавать новые данные, таким образом обнаруживая новые виды атак.

Выводы к главе 1

В данной главе была рассмотрена организационная структура ПФР, рассмотрена существующая модель защиты и возможные пути атаки на конфиденциальную информацию.

Было предложено рассмотрение применения нейронных сетей для анализа наличия угроз и их предотвращения. Главное требование к алгоритму – его быстродействие и гибкость.

Были обнаружены слабые и поддающиеся места для атаки в системе, например, возможная атака на координатор. Анализ поведения системы при такой ситуации рассмотрен в главе 3.

Глава 2. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Существует ряд таких задач, с которыми удобнее всего пользоваться системами на основе нейронных сетей. Во второй главе будут рассмотрены типы нейронных сетей, обоснование выбора одной из них и применимость сетей в информационной безопасности.

2.1 Выбор архитектуры нейронной сети

В зависимости от поставленной задачи могут использоваться разные нейронные сети. Задачи могут быть совершенно разного характера: задача кластеризации, распознавания образов, анализа данных, прогнозирования и т.д.

Для нахождения наиболее подходящей архитектуры нейронной сети с целью решения проблем безопасности данных стоит определить, какую именно задачу нужно решить.

В рассматриваемом контексте - это задача анализа данных.

2.1.1 Однослойный персептрон

Однослойный персептрон состоит из одного входного слоя (S), одного скрытого слоя (A) и одного выходного слоя (R).

A – элементы называют ассоциативными, так как одному такому элементу соответствует определенный набор S элементов. A – элементы активируются как только количество сигналов S превысило определенное количество. Далее, сигналы от A-элемента передаются в определенный сумматор R, каждый из таких сигналов имеет свой определенный вес.

Если вес положительный, то соответствующий ему синапс – возбуждающий, если отрицательный – тормозящий. Если суммарный импульс превышает порог активации, то нейрон возбуждается и выдает на выходе 1, иначе 0.

$$a\ x\ = \varphi \sum_{j=1}^{n} w_j x^j - w_0\ \ , \qquad (2.1)$$

Где w_0 – порог активации;

φ – функция активации;

w_j – веса нейронов;

x^j – определенны элемент входного вектора (рисунок 2.5).

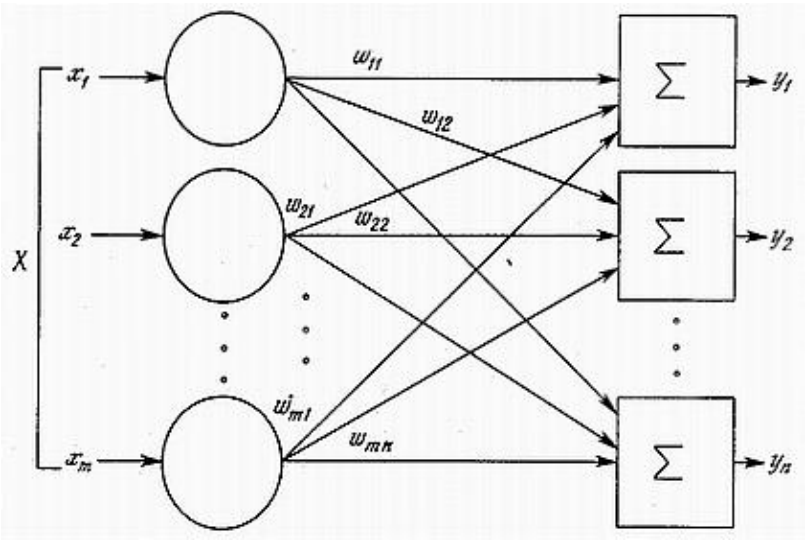

Рисунок 2.5 – Однослойный персептрон

Обучение однослойного персептрона подразумевает, что имеется такая пара векторов (X^S, D^S), в которой значения X – это входной вектор, а D – это правильный выходной вектор при данном значении входного. Значения вектора D – эталоны и поэтому, реальные выходные значения Y сравниваются с ними. Зная их разницу, можно ввести коррекцию для весовых коэффициентов и пороговых уровней:

1) если $d^s - y^s = 0$, то ответ сети считается правильным и веса нейронов не корректируются.
2) если $d^s - y^s < 0$, то ответ сети считается меньше правильного и веса нейрона увеличивают.
3) если $d^s - y^s > 0$, то ответ сети считается больше правильного и веса нейрона уменьшают [14].

2.1.2 Многослойный персептрон

Многослойный персептрон характерен тем, что входной сигнал распространяется напрямую от слоя к слою. Многослойный персептрон состоит из: входного слой, состоящего из некоторого множества нейронов, подаваемых на вход; некоторого множества скрытых слоев и выходного слоя (рисунок 2.6).

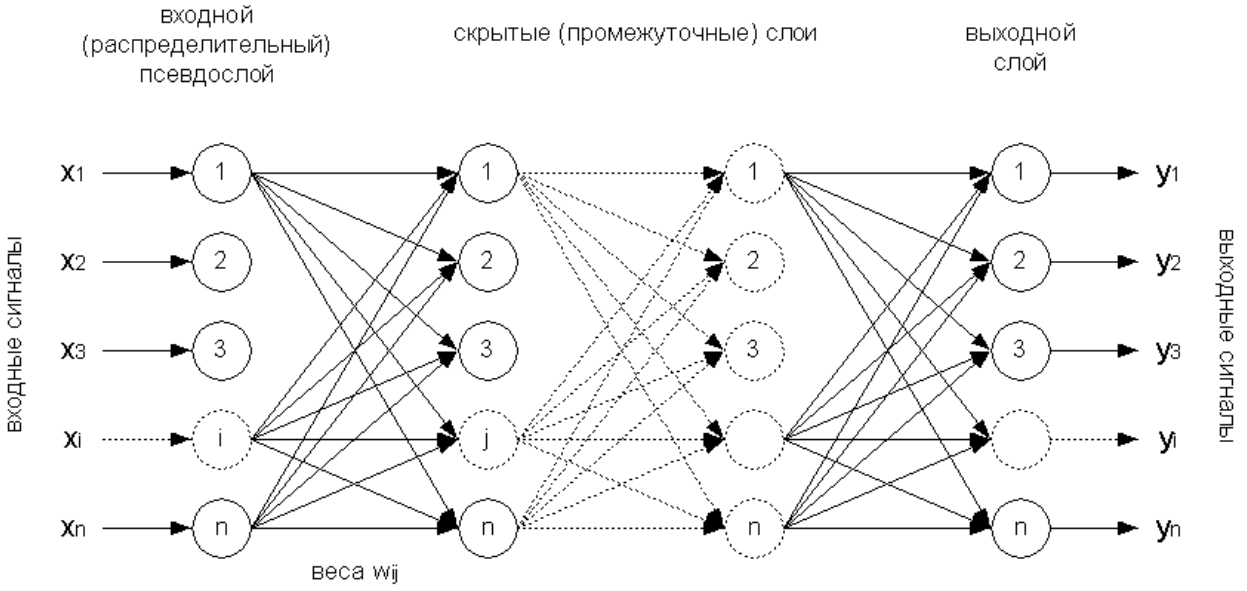

Рисунок 2.6 – Модель многослойного персептрона

От выбора количества слоев и типа активационной функции будет зависеть какие задачи сеть в дальнейшем способна будет решать. К примеру, однослойная сеть способна решать только задачи, связанные с формированием линейных разделяющих поверхностей. Однако сама линейная модель является точкой отсчета для сравнения эффективности разнообразных многослойных сетей с нелинейными функциями активации.

Необходимо подобрать такие значения весов w_{ij}, чтобы при заданном векторе x получить на выходе такие значения y, которые будут совпадать с требуемой точностью со значениями вектора ожидаемых сигналов d_i, для $i = 1, 2, \dots, N$.

Сигнал скрытого слоя у многослойного персептрона рассчитывается по формуле:

$$v_j = f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_j\right) \qquad (2.2)$$

А выходной нейрон рассчитывается по формуле:

$$y_k = f\left(\sum_{i=0}^{K} w_{ij}^{(2)} v_i\right) = f\left(\sum_{i=0}^{K} w_{ki}^{(2)} f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_j\right)\right), \qquad (2.3)$$

где $w_{ij}^{(1)}$- вес входного сигнала;

$w_{ij}^{(2)}$ – вес сигнала скрытого слоя;

x_j – сигналы входного слоя;

v_j – выходные сигналы скрытого слоя.

Исходя из формул видна зависимость значения выходного сигнала от весов всех слоев, однако сигналы, которые вырабатываются в скрытом слое, не зависят от весов выходного слоя.

Многослойный персептрон обучают с помощью алгоритма обратного распространения ошибки, который представляет собой целевую функцию, сформулированную в виде квадратичной суммы разностей между имеющимся и ожидаемым значениями выходных сигналов [12].

$$E(w) = \frac{1}{2}\sum_{k=1}^{M} (y_k - d_k)^2 \qquad (2.4)$$

Однако, если выборок больше, чем 1, то целевая сумма становится суммой по всем выборкам:

$$E(w) = \frac{1}{2}\sum_{j=1}^{P}\sum_{k=1}^{M} (y_k^{(j)} - d_k^{(j)})^2 \qquad (2.5)$$

Полноценная формула для обучения многослойного персептрона алгоритмом обратного распространения ошибки будет выглядеть следующим образом:

$$E = \frac{1}{2}\sum_{k=1}^{M} f\left(\sum_{i=0}^{K} w_{ki}^{(2)} f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_i\right) - d_k\right)^2 \quad (2.6)$$

В корректировке весов нуждаются как выходной слои, так и скрытые. Для вычисления значений, используются разные формулы. Возьмем нейроны p – из него выходит синаптический вес, а q – нейрон, в который он входит.

Для вычисления значений выходного слоя:

$$\delta_q = OUT_q\ (1 - OUT_q)\ (T_q - OUT_q)\ , \quad (2.7)$$

где δ_q- величина, которая показывает разность между требуемым и реальным выходами, умноженную на производную логической активации.

Веса выходного слоя будут равны:

$$w_{p-q}\ (i+1) = w_{p-q}\ (i) + \mu\delta_q OUT_p, \quad (2.8)$$

где i- номер текущей итерации;

μ – коэффициент скорости обучения;

w_{p-q} – величина синаптического импульса между нейронами p и q.

Для вычисления значений скрытых слоев:

$$\delta_q = OUT_q\ (1 - OUT_q) \sum_{k=1}^{N} \delta_k w_{q-k} \quad (2.9)$$

Веса скрытых слоев после коррекции:

$$w_{p-q}\ (i+1) = w_{p-q}\ (i) + \mu\delta_q OUT_p \quad (2.10)$$

Таблица 2.1 – Сравнение характеристик нейронных сетей на основе персептронов

Критерий	Однослойный персептрон	Многослойный персептрон
Быстрота	+	-
Точность	+	+
Эффективность	+	+

Продолжение таблицы 2.1 - Сравнение характеристик нейронных сетей на основе персептронов

Малое количество итераций	+	-
Итого	4	2

2.2 Основные типы атак

Атаки отказ в обслуживании (DoS атаки) или распределенный атаки отказа в обслуживании (DDoS-атака) являются попыткой сделать компьютерный ресурс недоступным для предполагаемых пользователей, хотя это не обязательно обеспечивается при помощи вредоносных программ . Эти атаки обычно реализуются хакерами. Хотя средства для выполнения, мотивы и целевые атаки DoS могут изменяться, они обычно состоят из совместных усилий лица или лиц, с целью предотвращения доступности интернет-сайта или веб-сервиса, временно или на неопределенный срок. Основной целью для атак DoS, как правило, являются целевые сайты или сервисы, содержащие информационные ресурсы банков, служб управления кредитных карт, платежных шлюзов и т.д.

Одним из инструментов, которые хакеры используют для запуска DDoS-атаки, является LOIC (Low Orbit Ion Cannon) .

Общий метод атаки состоит в насыщении целевого сервера-мишени (потерпевшего) внешними запросами, таким образом, что он не может ответить на легитимный трафик, или реагирует так медленно, чтобы его работа была либо неэффективна, либо он полностью недоступен. В общих чертах, DoS-атаки осуществляются с целью загрузить ресурсы целевого компьютера таким образом, чтобы он больше не был способен обеспечивать свои сервисы нужными ресурсами.

Remote to Local Attack (R2L). Атаки удаленного пользователя – это атаки в которой пользователь отправляет пакеты на сервер через Интернет, с

целью поиска уязвимостей сервера использование которых позволит получить права супер пользователя.

User to Root Attack (U2R). Эти атаки используют представляют собой атаку при которой хакер начинает работу в системе с правами обычного пользователя с целью получения привилегии супер пользователя

Probe (Зондирование). Зондирование это атака, в которой хакер сканирует машину или сетевое устройство для того, чтобы выяснить слабые места или уязвимости, которые могут быть впоследствии, эксплуатироваться с целью обхода системы ее безопасности [10].

2.3 Использование нейронных сетей в информационной безопасности

Существует огромный ряд преимуществ использования нейронных сетей для построения систем защиты информации:

- Высокая скорость обработки данных – позволяет работать системе в режиме реального времени.
- Способность анализировать данные из сети, включая неполные и искаженные данные.
- Возможность анализа и изучения таких элементов атак, которые ранее не встречались.

Однако, у таких систем есть и недостатки, которые являются продолжением достоинств:

- Для обучения нейронной сети необходимо на первоначальном этапе создать невероятно большое количество разнообразных вариаций атак.
- Точное описание поведения системы в целом невозможно, так как присутствует неопределенность в экстремальных ситуациях.
- Трудность с формированием модели, подходящей под все случаи.
- В связи с быстрым развитием информационных технологий необходимо пересматривать концепции уже существующих СЗИ.

2.4 Вычисление выходного сигнала нейрона

Пример 1.

Разберем пример получения выходного сигнала. Для этого нам понадобиться однослойный персептрон (рисунок 2.7).

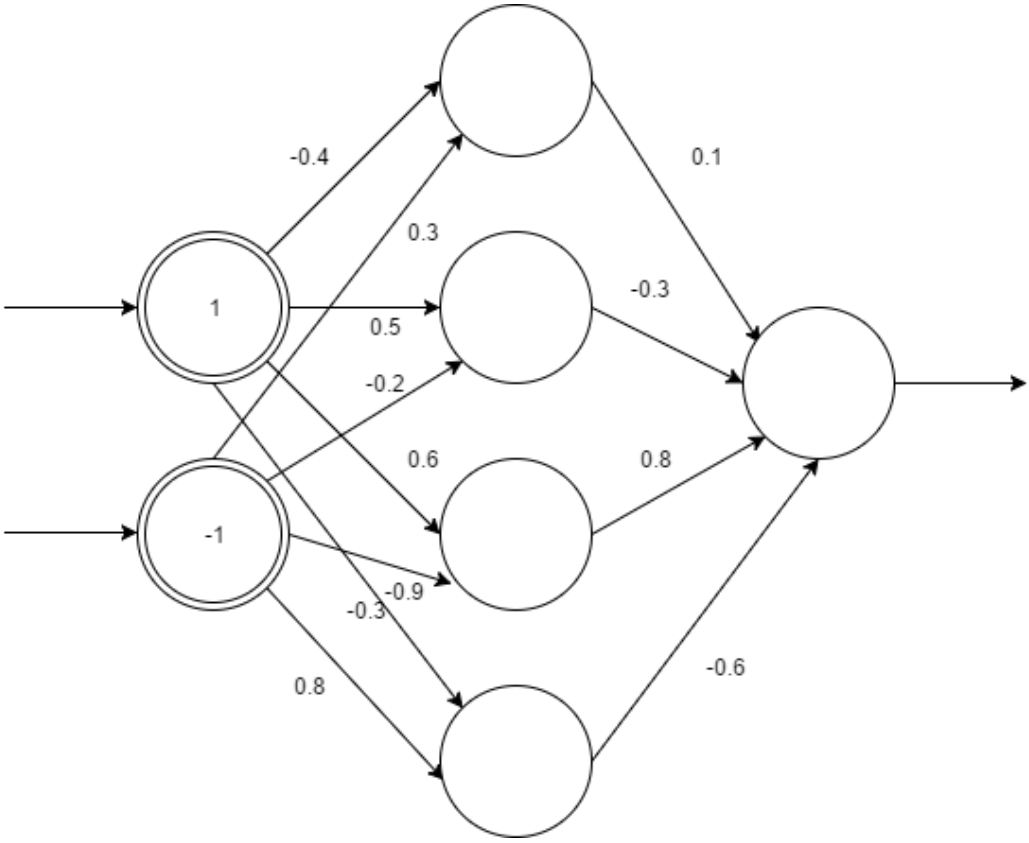

Рисунок 2.7 – Пример однослойного персептрона

Весовые коэффициенты отобразим в матричном виде для наглядности и удобства.

$$w_1 = \begin{matrix} -0.4 & 0.5 & 0.6 & -0.3 \\ 0.3 & -0.2 & -0.9 & 0.8 \end{matrix},$$

$$w_2 = \begin{matrix} 0.1 \\ -0.3 \\ 0.8 \\ -0.6 \end{matrix}$$

Для расчета результата работы сети понадобиться

1) комбинирование входа:

$$NET = c = \sum_{i=1}^{n} x_i w_{ij} \qquad (2.11)$$

2) функция активации:

$$f\ x\ = \frac{e^{NET} - e^{-NET}}{e^{NET} + e^{-NET}} \quad (2.12)$$

Теперь найдем работу от входного слоя к скрытому.

$$c_{11} = -0.4 + \ -0.3\ = -0.7,$$

$$f\ -0.7\ = \frac{0.49 - 2.01}{0.49 + 2.01} = \frac{-1.52}{2.5} = -0.608;$$

$$c_{12} = 0.5 + 0.2 = 0.7,$$

$$f\ 0.7\ = 0.608;$$

$$c_{13} = 0.6 + 0.9 = 1.5,$$

$$f\ 1.5\ = \frac{4.48 - 0.22}{4.48 + 0.22} = \frac{4.26}{4.7} = 0.906;$$

$$c_{14} = -0.3 - 0.8 = \ -1.1,$$

$$f\ -1.1\ = \frac{0.33 - 3.004}{0.33 + 3.004} = \frac{-2.674}{3.334} = -0.802$$

Далее произведем расчет конечной работы сети. Для этого понадобится другая формула активации, так как сеть определяет является ли входная информация атакой через анализ бинарной классификации. То есть, если значение будет +1, то атака совершена не была, если -1, то была.

$$f\ x\ = \begin{matrix} +1, & c > 0 \\ -1, & c \leq 0 \end{matrix}, \quad (2.13)$$

где t- порог.

$$c_{11} = -0.608 * 0.1 + 0.608 * \ -0.3\ + 0.906 * 0.8 + 0.802 * 0.6 = 0.4156$$

$$f\ x\ = +1$$

Исходя из полученного значения, видно, что атаки не было.

Пример 2.

Входные данные:

Известен ли источник получения информации $(0/1)$
Время передачи сигнала (сек)
Конфиденциальность информации $(1-10)$
Защищена ли информация паролем $(0/1)$

Допустим, установим такие значения: 0, 0.15, 3, 1. Веса установим, как степень важности параметра: 5, 1, 4, 4. Установим порог t = 20.

$$f\ x\ = \begin{matrix} +1, & t > 20 \\ -1, & t \leq 20 \end{matrix}$$

Теперь перемножаем соответствующие значения с весами.

$$c = 0 * 5 + 0.15 * 1 + 3 * 4 + 1 * 4 = 16.15$$

$$f\ 16.15\ = -1$$

Таким образом, видно, что атака была совершена на систему.

2.5 Разработка алгоритма анализа информационных угроз на основе нейронной сети

В качестве алгоритма был выбран регрессивный алгоритм, подразумевающий прогнозирование одной или нескольких числовых переменных на основе других, уже имеющихся, атрибутов.

На вход вектора x поступают оцифрованные данные, которые приходят с различных источников (такие как, МФЦ, ПТ КС и т.д.).

Далее, после работы нейронной сети мы получаем выходной нейрон, который сравнивается с определенными имеющимися диапазонами. Если полученное значение лежит в корректном диапазоне то считается, что данные были “чистые”. Если полученное значение принадлежит диапазону, содержащему значения атак, то такие данные считаются угрозой системы.

Диапазон может варьироваться, т. е. задаваться произвольно, таким образом, диапазон правильных источников информации и диапазон возможных угроз могут, как увеличиваться, так и уменьшаться. Так же значения могут быть разбиты по количеству значений после запятой и другим признакам (рисунок 2.8).

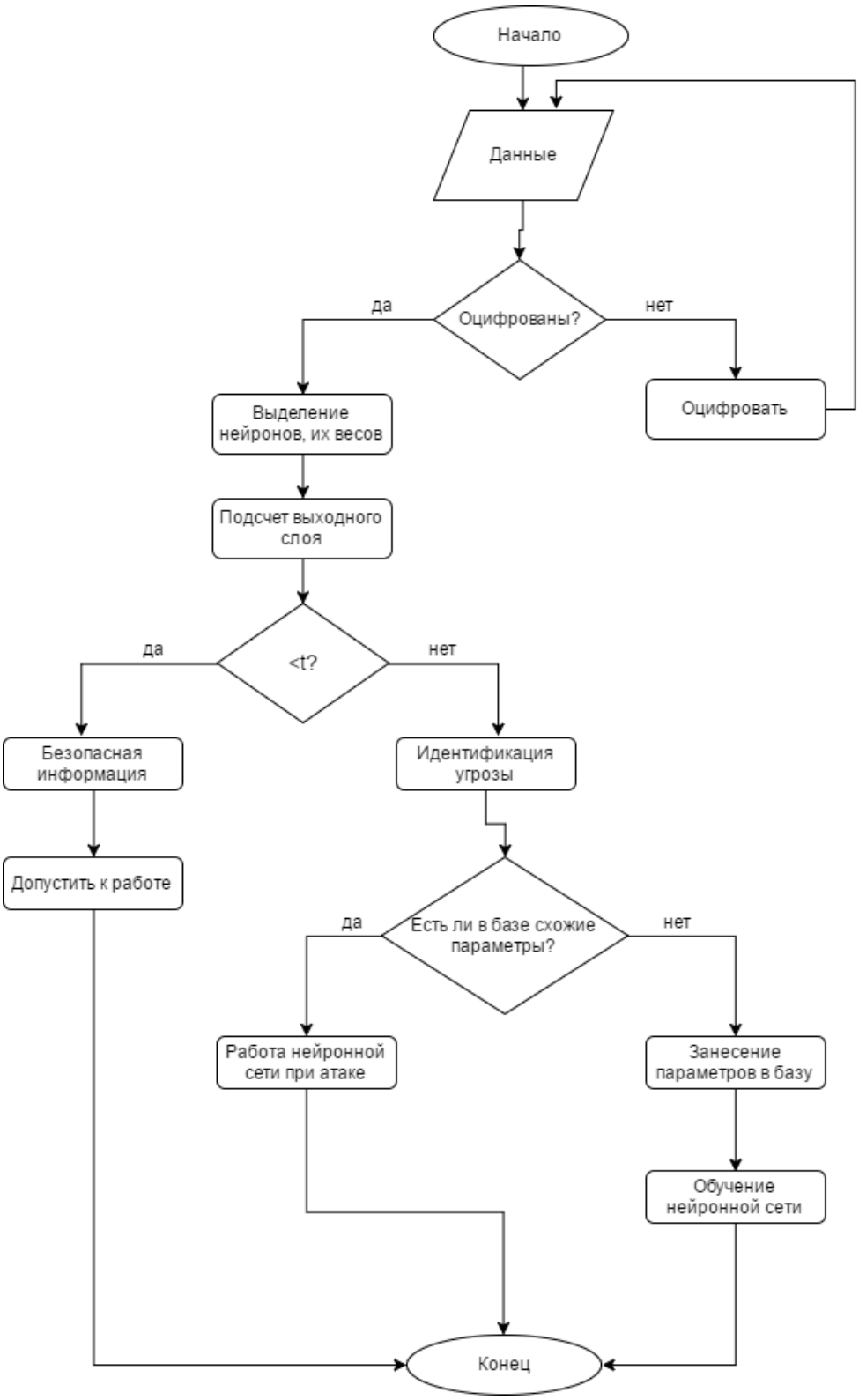

Рисунок 2.8 – Блок-схема алгоритма работы системы

Выводы к главе 2

В данной главе были рассмотрены две архитектуры нейронной сети и выбран однослойный персептрон для дальнейшей работы, так как он

наиболее быстро сможет определить характер возможной угрозы, за счёт меньшего количества слоёв сможет разделить поступившую на вход оцифрованную информацию на определенное количество параметров, тем самым увеличивая точность и эффективность работы сети.

Был составлен алгоритм анализа информационных угроз, на основе которого выстроена дальнейшая модель поведения системы.

Глава 3. МОДЕЛИРОВАНИЕ КОМПОНЕНТОВ СИСТЕМЫ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ

3.1 Основные требования к разрабатываемой комплексной системе защиты информации

Для идентификации объектов доступа, при создании правил разграничения доступа, используются соответственно имена объектов доступа и маски, для внешних устройств (накопителей) – их идентификация, включая серийные номера конкретных устройств.

При этом конкретная реализация процедуры идентификации и аутентификации включает ограничения:

− длина пароля, наличие букв разных регистров, наличие цифровых комбинаций или специальных символов;

− определение конечного (максимального) числа попыток ввода пароля до блокировки ;

− блокировка учетной записи или программно-технического устройства;

− возможное автоматическое генерирование пароля, с требуемыми ограничениями;

− разрешение или запрет входа пользователя в безопасном режиме работы рабочей станции.

Средством защиты информации (СЗИ) реализовывается также идентификация и аутентификация пользователя при запросах на доступ к объектам удаленной системы (разделяемым ресурсам).

В качестве объектов доступа в комплексной системе защиты информации выступают:

− файловые объекты, как локальные, так и распределенные в сети – файлы, каталоги, подкаталоги, диски;

− файловые объекты на внешних носителях информации;

− объекты системного реестра операционной системы;

− локальные и сетевые принтеры;

− сетевые адаптеры;

− любые иные устройства, являющиеся внешними по отношению к системе.

Система защиты информации в своей работе определяет назначение прав пользователя и прав запускаемых от имени пользователя процессов, определяет необходимость санкционированного доступа к объектам с минимально требуемыми правами.

Обеспечивается контроль по расширению файлов, с целью предотвращения несанкционированного создания, удаления или переименования объектов системы.

Система защиты в обязательном порядке контролирует и обеспечивает разделение полномочий администраторов и пользователей, реализовывающих функционирование информационной системы в соответствии с их должностными обязанностями. А также удаление пользователей, создание временных учетных записей.

Осуществляет контроль неудачных попыток входа и обеспечивает блокировку учетной записи пользователя, как при консольном способе аутентификации, так и по электронному ключу.

В комплексной системе защиты информации должна обеспечиваться регистрация всех событий (вход (выход), а также попытки входа в информационную систему, загрузки (остановки) операционной системы, подключение устройств как внешних, так и внутренних, информационных носителей и т.д.) связанных с обработкой защищаемой информации, а также попытками доступа субъектов к техническим средствам, устройствам.

Для каждого из этих событий должна фиксироваться следующая информация:

− дата и время;

− субъект, осуществляющий регистрируемое действие;

− тип события;

− результат события (обслужен запрос доступа или нет).

При этом должны быть реализованы два режима регистрации событий - оперативный и реального времени, при этом правила регистрации для них должны настраиваться отдельно.

Режим оперативной регистрации событий предполагает формирование журнала аудита (на клиентской части) с возможностью его получения администратором по запросу (с серверной части, на сервере безопасности).

Режим регистрации событий в реальном времени предполагает незамедлительную передачу зарегистрированных событий на сервер аудита.

В функции системы должна входить также защита информации о событиях безопасности, при этом доступ к записям аудита и функциям управления регистрации должен предоставляться только уполномоченным должностным лицам.

Одним их обязательных условий при разработке системы защиты информации являются также требования по обеспечению запрета несанкционированного удаленного доступа и активации устройств и систем связи и передачи информации.

Вариантами реализации данной задачи является предотвращение запуска требуемого приложения, предотвращение подключения требуемых устройств (или контроль за подключением данных устройств в соответствии с правами разграничения доступа), предотвращение взаимодействия через требуемые порты с учетом из номеров.

Система защиты информации должна обеспечивать защиту:

− архивных файлов с параметрами настройки средств защиты информации, программного обеспечения и других данных, не подлежащих изменению в процессе функционирования системы;

− логических границ информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;

− сетевых соединений и их завершение по истечению установленного времени неактивных соединений.

За основу модели комплексной системы защиты информации возьмем реализацию контроля (разграничения прав) доступа субъектов к объектам системы при реализации метода контроля на базе матрицы доступа (рисунок 3.1).

Особенности реализации данной модели защиты состоят в следующем:

− реализуется принудительное управление потоками информации – только администратор может назначить правила доступа к объектам (пользователь исключен из схемы администрирования);

− права доступа назначаются как для субъектов в разграничительной политике, а не устанавливаются в виде атрибутов;

− матрица доступа (правила доступа) хранятся в виде таблиц в отдельном файле.

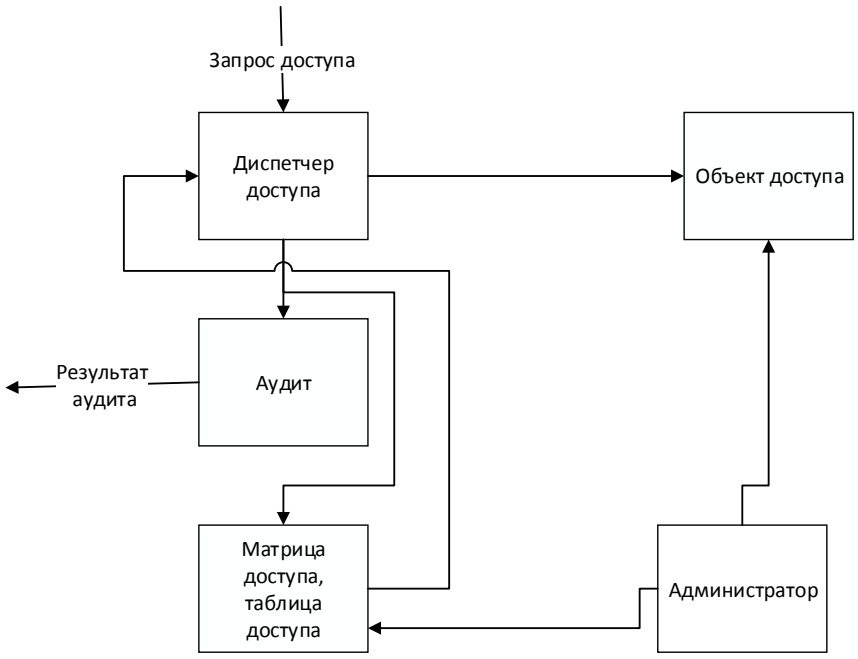

Рисунок 3.9 - Модель контроля доступа

При построении такой модели защиты кроме упрощения задачи администрирования (разграничения прав для субъектов) возможно решение задачи по обеспечению прав доступа к вновь создаваемым объектам (для которых могут быть не установлены права доступа).

3.2 Возможности различных групп пользователей системы

Система защиты информации должна разграничивать права доступа пользователей к объектам системы, с целью предотвращения несанкционированного доступа и защиты информации, содержащейся в различных объектах.

Существует несколько групп пользователей:

- Системный администратор
- Начальник управления – обладает правами на подключение к рабочим станциям сотрудника и начальника отдела. Имеет права на read/write.
- Начальник отдела – обладает правами на подключение к рабочей станции сотрудника, находящегося в непосредственном подчинении. Имеет права на read/write.
- Специалист.

На рисунке 3.10 изображена диаграмма классов зависимости групп пользователей.

Как следует из диаграммы, пользователь администраторской группы обладает правами на просмотр информации с рабочих мест других пользователей, включая начальника управления. Каждое нижестоящее звено обладает всё менее значимыми правами.

У начальника управления нет непосредственной возможности перехода на рабочую станцию сотрудника. Он может попасть туда только через начальника отдела. Администратор системы имеет доступ ко всем рабочим станциям.

Таким образом, есть возможность атаки на различные группы пользователей, степень опасности которых является прямо пропорциональной иерархии групп.

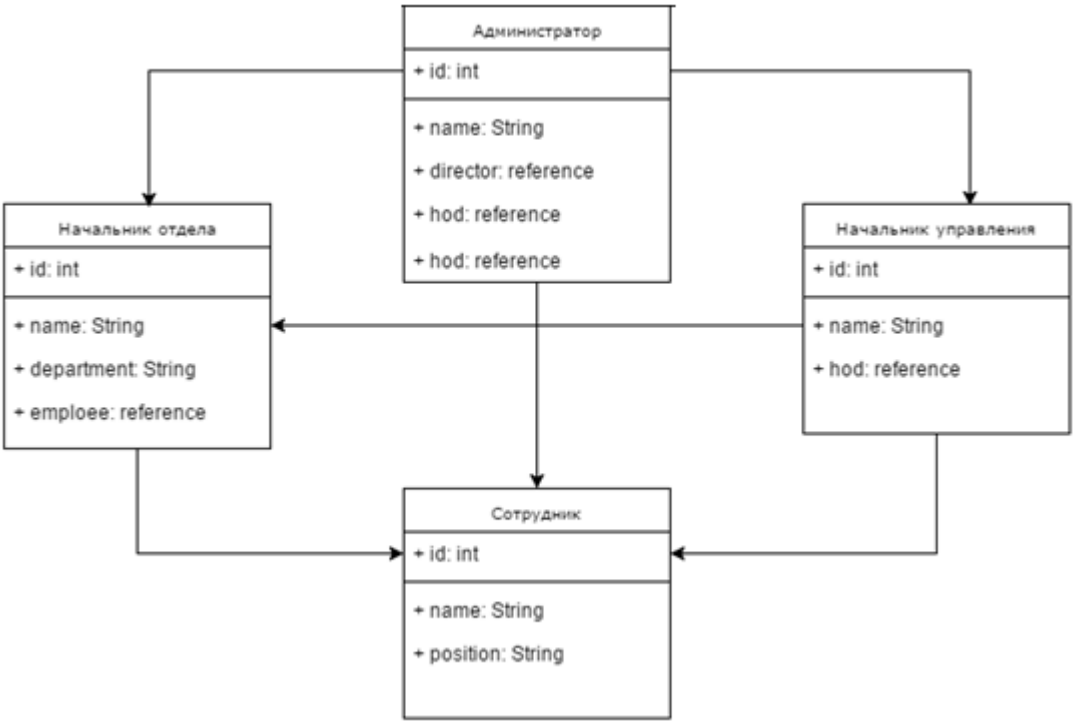

Рисунок 3.10 – Зависимость групп (hod – head of department)

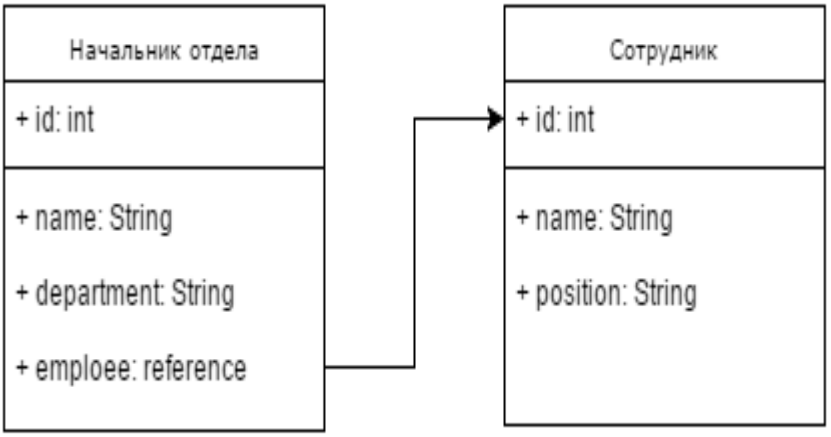

Рисунок 3.11 – Отношение вышестоящего к нижестоящему.

Как видно из примера, в БД начальника отдела хранятся сведения по работнику его отдела, которое представляет собой ссылку на самого

работника, вычисляемую по id из базы данных сотрудника. Таким образом, переходя по данным ссылкам, можно выйти на рабочую станцию сотрудника.

3.3 Описание поведения системы при атаке

Как уже было сказано раннее, степень сложности защиты при атаке зависит от расположения в иерархии групп пользователя, на которого была совершена данная атака. Таким образом, мы имеем несколько уровней сложности защиты.

Уровень № 1 (рисунок 3.12).

Идентификация угрозы на координаторе.

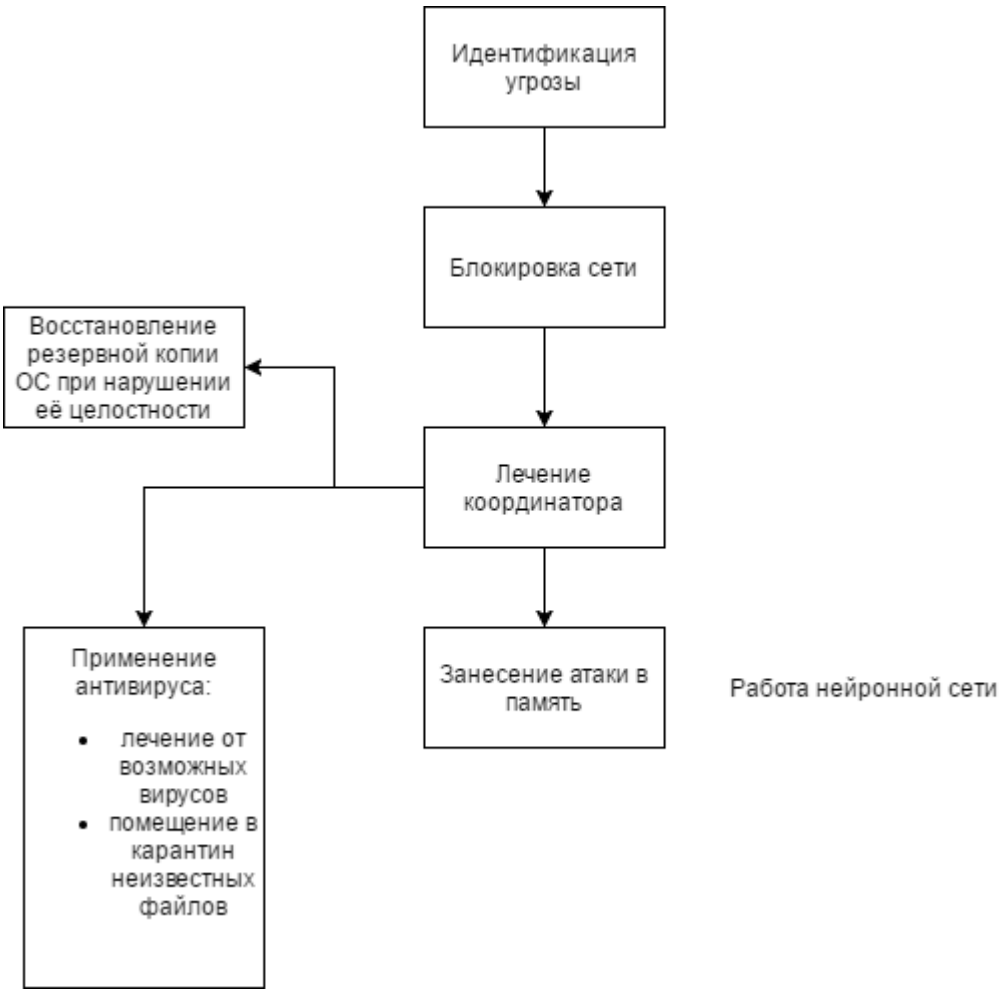

Рисунок 3.12– Схема угрозы 1-го уровня

Уровень № 2 (рисунок 3.12).

Атака на рабочую станцию сотрудника.

Данная ситуация может произойти в нескольких случаях:

1) Атака произведена непосредственно координатор – сотрудник

2) Атака произведена координатор – начальник отдела – сотрудник

3) Атака произведена координатор – начальник управления – сотрудник

4) Атака произведена координатор – начальник управления – начальник отдела – сотрудник

Случаи, 2-4 наиболее вредоносны, так как получив более высокий доступ, можно добраться до гораздо большего количества конфиденциальной информации. Во всех 4 случаях производится лечение координатора, отключение рабочей станции от сети, перемещение её в карантин, лечение канала передачи.

Уровень № 3.

Атака произведена на пользователя с правами администратора.

Наиболее вероятная и опасная модель атаки, так как при попытке взлома пострадает абсолютно вся система.

Для начала стоит разобрать случаи взлома учетной записи администратора (таблица 3.13):

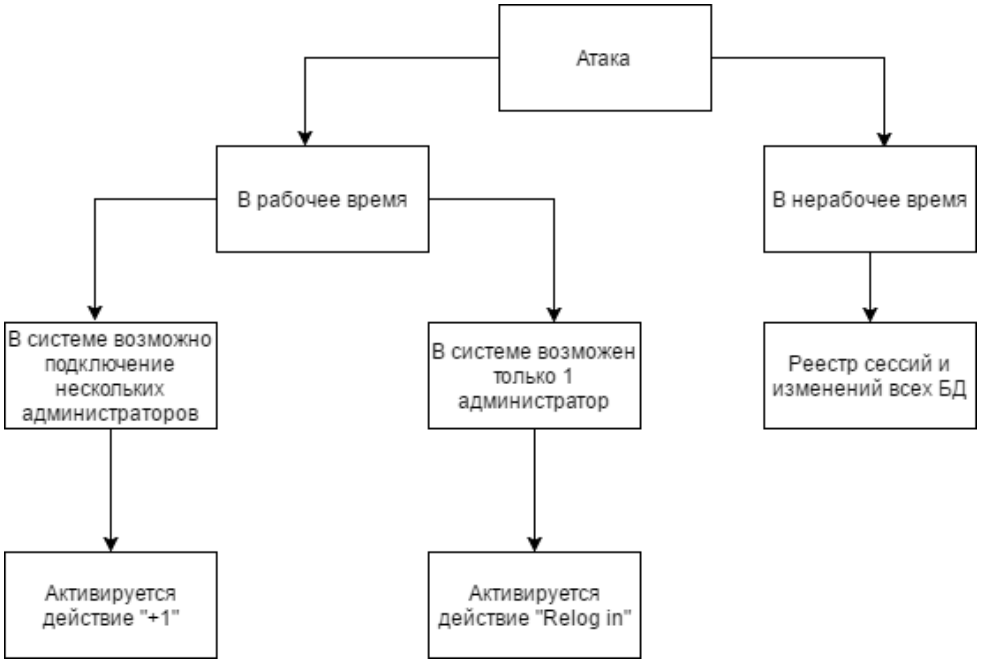

Рисунок 3.13 – Схема угрозы 3-го уровня

Таблица 3.2 – Описание активационных действий системы

Название	Действие
Действие “+1”	1.Current_user = Current_user + 1 2. Отображение нового пользователя в системе.
Действие “Relog in”	1. Current_user =admin 2. Current_user = Current_user + 1 3. Принудительный выход из системы
Реестр сессий и изменений БД	Происходит сохранение всех действий, произведенных над БД. После каждого входа в систему производится снятие резервных копий с имеющихся БД.

3.4 Описание работы нейронной сети в системе

Нейронная сеть включает в себя определенную базу знаний, в которую входят все предыдущие типы атак. Таким образом, в системе безопасности данных на основе нейронной сети будет срабатывать два вызова функции (рисунок 3.14).

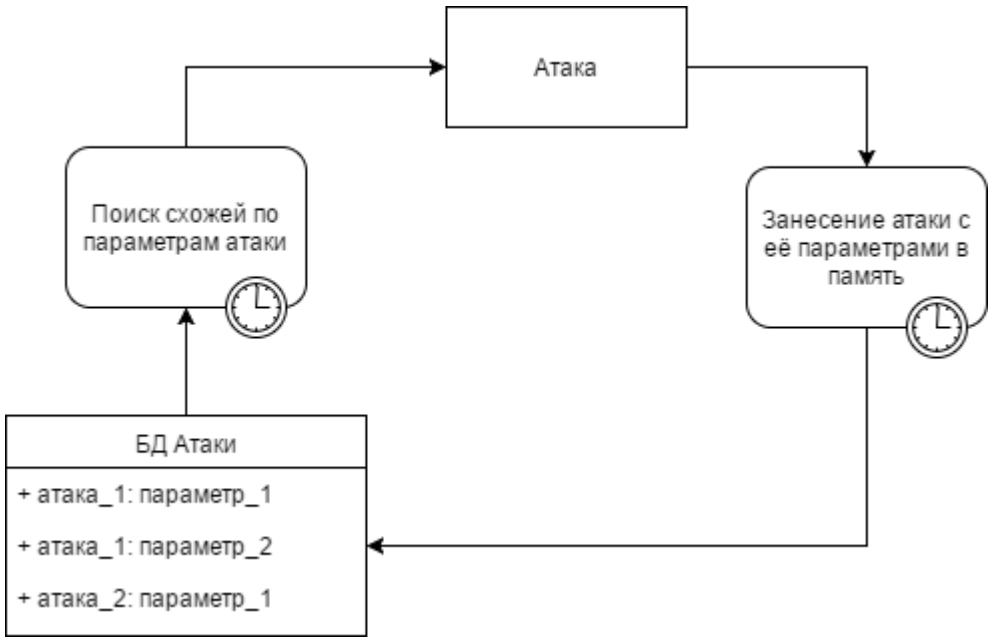

Рисунок 3.14 – Работа нейронной сети в системе

В базе нейронная сеть раскладывает имеющиеся после обучения атаки на составляющие – параметры и при получении на вход новой атаки, совпадающей хотя бы по одной характеристике, производит защиту от вторжения.

Так же немаловажно обучить нейронную сеть просчитывать интервалы между запросами – если интервал очень мал, то скорее всего происходит атака машиной.

Так как система подразделяется на 2 направления, то соответственно и тестирование будет двунаправленным.

3.4 Разработка тест-кейсов

Для начала рассмотрим тестирование некоторых частей основного функционала системы (таблица 3.2)

Таблица 3.3 - Тест-кейс №1. Авторизация в системе

Действие	Ожидаемый результат
Войдите в систему как пользователь любой из групп. (Введите корректные логин - пароль)	Вход должен быть осуществлен.
Нажмите на кнопку закрытия системы.	Должно быть предложено действие на закрытие сессии. Должно появиться сообщение “Вы хотите выйти из системы. Закрыть данную сессию?”
Нажмите кнопку “Нет”	Окно с предупреждением должно закрыться.
Повторите действие из шага №2	
Нажмите кнопку “Да”	Должен быть произведен выход из системы.

Таблица 3.4 - Тест-кейс № 2. Регистрация пользователя в системе

Действие	Ожидаемый результат
Войдите в систему как системный администратор.	Вход должен быть осуществлен.
Зайдите Меню -> Пользователи -> Добавить нового пользователя	Окно для выбора группы доступа для нового сотрудника должно быть открыто.
Выберите необходимую группу пользователей. Нажмите “Далее”	Окно для ввода необходимых данных должно быть открыто.
Введите данные в систему. Нажмите “Создать”	Новый пользователь должен быть создан в системе.

Таблица 3.5 - Тест-кейс № 3. Проверка одиночного нахождения сотрудника в системе

Действие	Ожидаемый результат
Войдите в систему как пользователь.	Система должна заработать с соответствующими правами.
Откройте систему ещё раз.	Должна открыться стартовая страница системы с сохранением введенных настроек. (Вы не должны “вылететь” из системы)
На другом компьютере введите те же пароль/логин.	Должно появиться сообщение, что “Вход в систему уже произведен. Вы не можете авторизоваться дважды.”

Таблица 3.6 - Тест-кейс № 4. Проверка возможности администратора находится в системе через несколько аккаунтов.

Действие	Ожидаемый результат
Зайдите в систему сначала под одним администратором.	Вход должен быть произведен.

Продолжение таблицы 3.6 - Тест-кейс № 4.

На другой машине зайдите в систему под другим аккаунтом администратора.	Вход должен быть произведен.
	На первом администраторском аккаунте в правом верхнем углу должно появиться “+1 активный аккаунт администратора”
Зайдите Меню -> Пользователи -> Группы -> Администратор -> Активные пользователи.	Должно быть открыто окно с активными пользователями, наделёнными правами администратора.

Для прохождения данного кейса необходимо иметь двух пользователей с одинаковыми правами администратора.

Теперь обратим внимание на второе направление тестирование системы – тестирование интегрированности нейронной сети в среду.

Для этого до начала тестирования необходимо иметь хорошо обученную нейронную сеть (>100 вида атак), несколько старых видов атак, пару абсолютно новых и атаки, не все параметры которых известны системе.

Таблица 3.7 - Тест-кейс № 5. Атака 1-го уровня

Действие	Ожидаемый результат
Спровоцируйте атаку на координатор.	
Зарегистрируйтесь в системе как администратор.	Вход должен быть произведен. Сообщение об атаке.
Зайдите Меню -> Защита -> Действия -> Координатор	Должно открыться окно с выбором возможных действий на систему.

Продолжение таблицы 3.7 - Тест-кейс № 5.

Выберите: блокировка локальной сети, лечение координатора, блокировка связи с регионом (туннелированная связь). Нажмите “Ок”	Должно начать экстренное лечение координатора, он должен быть помещен в карантин, локальная сеть должна быть изолирована.
	Должно появится сообщение “Лечение окончено. Все функции системы в безопасности и включены”
Нажмите “Ок”.	Система должна заработать автоматически.
Зайдите Меню -> Защита -> Нейронная сеть	Должно открыться окно с историей внесения изменений в базу нейронных сетей.

Таблица 3.8 - Тест-кейс № 6. Атака 2-го уровня (координатор - сотрудник)

Действие	Ожидаемый результат
Спровоцируйте атаку на рабочую станцию сотрудника.	
Зарегистрируйтесь в системе как администратор.	Вход должен быть произведен. Должно появиться окно о том, что система подверглась атаке.
Зайдите Меню -> Защита -> Действия -> Рабочая станция	Должно открыться окно с выбором возможных действий на систему.
Выберите: помещение в карантин рабочей станции №…. Нажмите “Ок”	Координатор автоматически помещается в карантин, лечится, блокируется локальная сеть и связь с регионом.

Продолжение таблицы 3.8 - Тест-кейс № 6.

	Должно появиться сообщение “Лечение окончено. Все функции системы в безопасности и включены”
Нажмите “Ок”.	Система должна заработать автоматически.
Перейдите Меню -> Защита -> Нейронная сеть	Должно открыться окно с историей внесения изменений в базу нейронных сетей.

Для вариантов координатор – начальник управления – сотрудник, координатор – начальник управления – начальник отдела – сотрудник, координатор – начальник отдела – сотрудник, шаги тест-кейса № 6 будут идентичными, за исключением того, что в меню “Действия” надо выбрать пункт “Цепь” и в появившемся окне выбрать подходящий вариант. Далее появятся окна для заполнения информацией.

Таблица 3.9 - Тест-кейс № 7. Атака 3-го уровня (похищение/удаление/замена данных в нерабочее время)

Перед завершением работы система обязательно сохранит резервную копию данных.

Действие	Ожидаемый результат
Спровоцируйте атаку на координатор.	
Зарегистрируйтесь в системе как администратор.	Вход должен быть произведен. Сообщение об атаке
Зайдите Меню -> Защита -> Действия -> История	Должно открыться окно с историей действия с системой.

Продолжение таблицы 3.9 - Тест-кейс № 7.

После появления сообщение “Поиск/сортировка завершен” нажмите “Ок”.	Должны быть показаны варианты поиска.
Справа от найденного варианта нажмите знак вопроса.	Должно появиться сообщение о всех изменениях и действиях, произведенных в течении этой сессии.
Справа от найденного варианта нажмите на знак крестика.	Должно появиться сообщение: “Вы действительно хотите пролечить систему после данной сессии?”
Нажмите “Ок”	Система должна уйти на перезагрузку и автоматически обновиться. Появится окно для повторной авторизации в системе.
Зайдите Меню -> Память -> Резервные копии БД. В сплывшем окне выберите дату, от которой необходимо восстановить данные. Нажмите “Ок”	Данные должны восстановиться
Зайдите Меню -> Защита -> Нейронная сеть	Должно открыться окно с историей внесения изменений в базу нейронных сетей.

Выводы к главе 3

В данной главе были выявлены три типа атак на систему, а также рассмотрена работа нейронной сети, когда встает вопрос об её нахождении в уже имеющейся базе. Составлены тест-кейсы, по которым пользователь может проверить готовность и работу системы, как в целом, так и по модулям. Тестирование позволяет подтвердить верную работу алгоритма и обнаружить недочеты, которые устранятся в последующих версиях продукта.

ЗАКЛЮЧЕНИЕ

В ходе бакалаврской работы была спроектирована начальная версия системы защиты информации на основе нейронной сети. Путем сравнения была выбрана определенная архитектура нейронной сети – многослойный персептрон.

Проектирование системы заключалось в разграничении прав пользователей, а так же рассмотрении поведения системы при атаке. Так же было рассмотрено применение нейронной сети с информационной безопасности.

Подготовка к тестированию включила в себя проработку тестовых сценариев для дальнейшей работы с системой. С их помощь заказчику будет легче разобраться в ходе работы системы, а так же увидеть ожидаемый результат и сравнить его с имеющимся, полученным в ходе тестирования результатом.

В ходе бакалаврской работы, были выявлены несомненные преимущества использования нейронных систем в данной сфере.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

Научная и методическая литература

1. Гончаров В.А., Пржегорлинский В.Н. Метод обнаружения сетевых атак, основанный на кластерном анализе взаимодействия узлов вычислительной сети // Вестник Рязанского государственного радиотехнического университета. 2011. № 36. С. 3-10.

2. Злобин В.К., Ручкин В.Н., Нейросети и нейрокомпьютеры//БХВ-Петербург. 2011

3. Мустафаев А.Г. Применение искусственных нейронных сетей для ранней диагностики заболевания сахарным диабетом // Кибернетика и программирование. 2016. № 2. С. 1-7. DOI: 10.7256/2306-4196.2016.2.17904.

4. Осовский С. Нейронные сети для обработки информации. М.: Финансы и статистика, 2012. 344 с.

5. Саймон Хайкин, Нейронные сети. Полный курс// Вильямс. 2016.

6. Тархов Д. А., Нейросетевые модели и алгоритмы. Справочник// Радиотехника. 2014.

Электронные ресурсы

7. Сайт пенсионного фонда РФ[Электронный ресурс]. – Режим доступа: http://www.pfrf.ru (дата обращения 01.06.2017).

8. Тестирование программного обеспечения. [Электронный ресурс]. - Режим доступа: http://www.protesting.ru (дата обращения 01.06.2017).

9. Лекции по теории и приложениям искусственных нейронных сетей. [Электронный ресурс]. – Режим доступа: http://alife.narod.ru/lectures/neural (дата обращения 01.06.2017).

10. Интуит – Национальный Открытый институт. [Электронный ресурс]. - Режим доступа: http://www.intuit.ru/studies/courses/17846/1242/lecture/27501

11. Tproger [Электронный ресурс].- Режим доступа: https://tproger.ru/translations/learning-neural-networks/ (дата обращения 01.06.2017).

12. BaseGroup Labs/ Технологии анализа данных [Электронный ресурс]. – Режим доступа: https://basegroup.ru/ (дата обращения 01.06.2017).

13. Портал искусственного интеллекта. [Электронный ресурс]. – Режим доступа: http://www.aiportal.ru/ (дата обращения 01.06.2017).

14. neurones.ru [Электронный ресурс]. - Режим доступа: http://neurones.ru (дата обращения 01.06.2017).

Литература на иностранном языке

15. Dennis A. System Analysis and Design/ A. Dennis, B. H. Wixom, R. M. Roth. // Wiley. – 2014. – 6th Edition

16. Jeff Heaton. Artificial Intelligence for Humans, Volume 3: Deep Learning and Neural Networks/ Jeff Heaton // Heaton Research Inc. – 2015. – 1st Edition

17. Jeff Heaton. Introduction to the Math of Neural Networks / Jeff Heaton // Heaton Research Inc. – 2012.

18. John W. Foreman. Data Smart: Using Data Science to Transform Information into Insight / John W. Foreman/ Wiley. – 2013. - 1st Edition

19. Martin T Hagan, Howard B Demuth, Mark H Beale, Orlando De Jesús. Neural Network Design (2nd Edition)/ Martin T Hagan, Howard B Demuth, Mark H Beale, Orlando De Jesús// Martin Hagan. – 2014. – 2nd Edition

20. Yoav Goldberg. Neural Network Methods in Natural Language Processing (Synthesis Lectures on Human Language Technologies)/ Yoav Goldberg, Graeme Hirst.// Morgan & Claypool Publishers. – 2017.

ПРИЛОЖЕНИЕ А

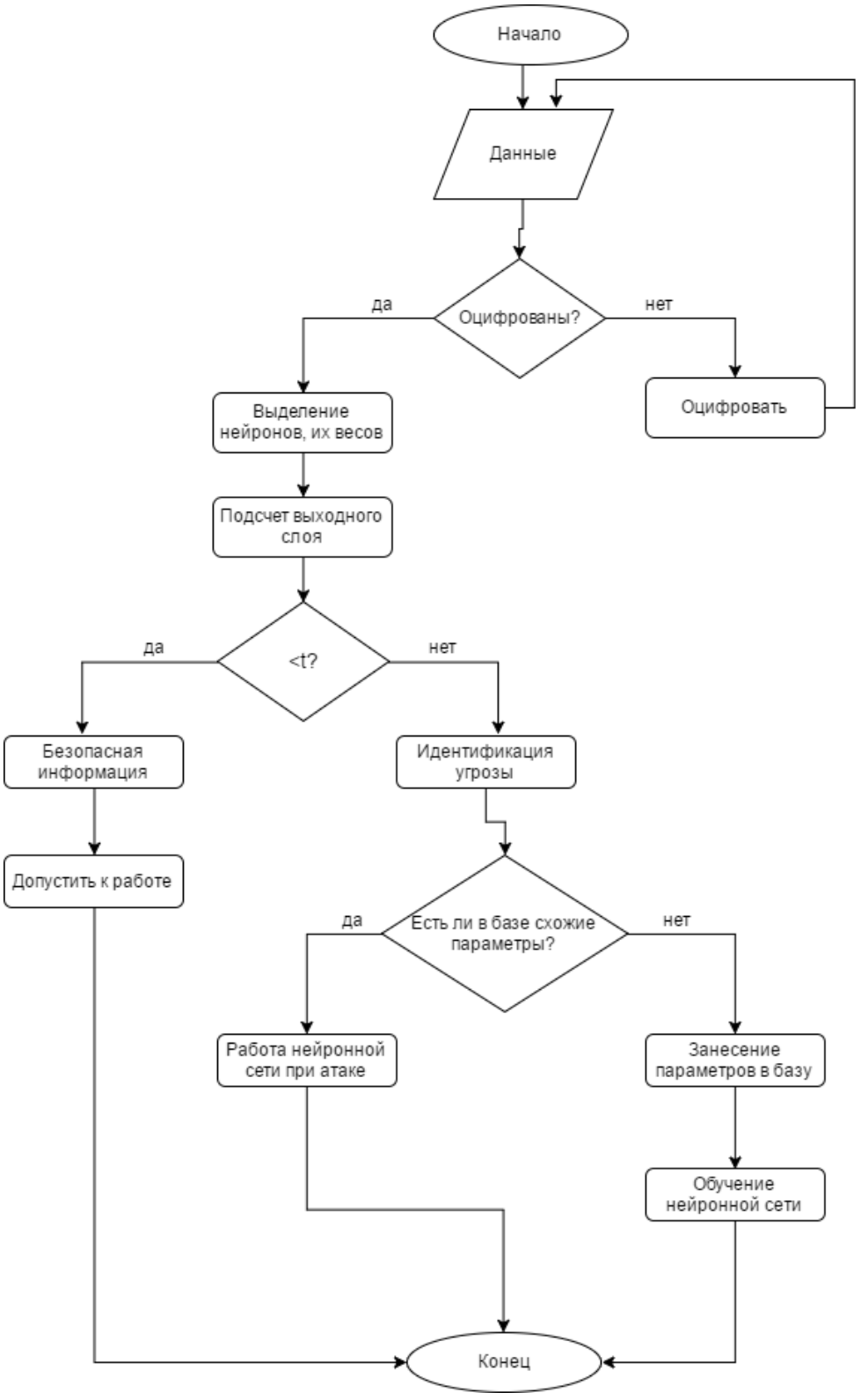

Рисунок А.1 – Алгоритм анализа нейронной сетью данных на наличие угрозы