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

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Исследование вопроса безопасности и приватности конфиденциальных данных в облачных вычислениях»

Студент Д.О. Глеске
(И.О. Фамилия) (личная подпись)

Научный руководитель доцент, Е.А. Ерофеева
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

ОГЛАВЛЕНИЕ

Введение

Актуальность выбранной темы

Многие организации, работающие с конфиденциальной информацией, рассматривают возможность использования облачных вычислений, поскольку они предоставляют ресурсы, которые можно легко масштабировать, наряду со значительными экономическими выгодами в виде снижения эксплуатационных расходов. Тем не менее, сложно правильно обрабатывать конфиденциальные данные в облачных вычислительных средах из-за ряда существующих законов и положений о конфиденциальности. Примером такого законодательства является Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" [28], который требует сохранения конфиденциальности для обработки персонально идентифицируемой информации. В данной диссертации будут рассмотрены проблемы, с которыми сталкиваются организации при хранении персональных данных. Также будет описываться, как облачные вычисления могут использоваться для предоставления инновационных решений, обеспечивающих безопасность конфиденциальной информации.

Основное внимание в этой диссертации уделяется вопросам безопасности и конфиденциальности данных, хранимых или получаемых на предприятии, что требует особенно строгих решений, обеспечивающих конфиденциальность [17]. Например, для высокоточного прогнозирования чего-либо, основываясь на гигантской статистике и не вникая в глубинные причины явлений, используя аналитику больших данных и технологии облачных вычислений. Однако при использовании данных в облаке необходимо учитывать этические и нормативные аспекты, связанные с владением данными. Такие данные должны обрабатываться прозрачно, чтобы личности лиц, «владеющих» данными, не были раскрыты.

Следовательно, облачные решения должны надлежащим образом защищать конфиденциальность данных. Облачные вычисления подняли несколько проблем безопасности, включая многопользовательский режим, потерю контроля и доверия. Следовательно, большинство облачных

провайдеров - в том числе Google, Яндекс и другие, не гарантируют определенные уровни безопасности и конфиденциальности в своих соглашениях об уровне обслуживания (SLA) в рамках договорных условий и положений. между облачными провайдерами и потребителями. Поставщики облачных вычислений виртуализируют и контейнеризируют свои вычислительные платформы, чтобы иметь возможность обмениваться ими между различными пользователями. Под многопользовательским режимом подразумевается совместное использование физических устройств и виртуализированных ресурсов между несколькими независимыми пользователями или организациями. [16]

Потеря контроля — это еще одно потенциальное нарушение безопасности, которое может возникнуть, когда данные, приложения и ресурсы потребителей размещаются в принадлежащем облачному провайдеру помещении. Если пользователи не имеют явного контроля над своими данными, это позволяет облачным провайдерам выполнять интеллектуальный анализ данных пользователей, что может привести к проблемам безопасности. Кроме того, когда облачные провайдеры выполняют резервное копирование данных в различных центрах обработки данных, потребители не могут быть уверены, что их данные будут полностью удалены везде, когда они удаляют свои данные. Это может привести к неправильному использованию стертых данных. В таких ситуациях, когда потребители теряют контроль над своими данными, они видят в облачном провайдере черный ящик, в котором они не могут напрямую осуществлять прозрачный мониторинг ресурсов. Доверие играет важную роль в привлечении большего количества потребителей, обеспечивая поставщиков облачных услуг. Проблемы безопасности в облачных вычислениях приводят к ряду проблем с конфиденциальностью, потому что конфиденциальность - это сложная тема, которая имеет различные толкования в зависимости от контекста, культуры и сообщества. Кроме того, конфиденциальность и безопасность являются двумя различными темами, хотя безопасность, как правило, необходима для обеспечения конфиденциальности

[11]. Юристы, философы, исследователи, психологи и социологи предприняли несколько попыток осмыслить конфиденциальность, чтобы дать нам лучшее понимание конфиденциальности - например, исследование Алана Вестина в 1960 году считается первой значительной работой по проблеме конфиденциальность данных потребителей и защита данных. Вестин [21] определил конфиденциальность следующим образом. "Конфиденциальность - это требование отдельных лиц, групп или учреждений самим определять, каким образом и каким образом информация о них сообщается другим лицам. "

Исходя из этого тема защиты данных в облаке является актуальной.

Объект исследования: ИС облачных вычислений, где взаимодействуют клиент и поставщик облачных сервисов.

Предмет исследования: модели и методы проверок информационной безопасности в ИС облачных вычислений.

Цель исследования: нахождение способа оценить степень угрозы похищения данных в ИС облачных вычислений.

Задачи исследования:

1. Выяснить какие виды нарушений могут быть в системе облачной безопасности, также понять, что может являться источником угроз. Реализовать модель угрозы ИБ, принимая во внимание отличительные черты системы облачных вычислений.

2. Изучить нормативные документы о защите информации в облаке, выполнить разработку метода частной политики безопасности системы облачных вычислений.

3. Применяя численную оценку вероятности возникновения угрозы нарушения информационной безопасности, в которую внедрена искусственная нейросеть, реализовать метод проверки ИБ в облаке.

4. Реализовать программу целью которой будет автоматизация проведения проверок информационной безопасности системы облачных вычислений. Выполнить тестирование данной программы, применяя вычислительные исследования.

В данной работе будут применены следующие методы исследования: теория искусственный нейросетей, моделирование IDEF0, теория нечетких когнитивных карт.

Научная новизна:

1. Благодаря, применению нечетких когнитивных карт, появляется возможность увидеть, как происходит увеличение угроз и их источников в облаке.

2. Предложенный в данной работе способ разграничения доступов для ролей, что приводит к исключению роли пользователя с максимальными доступами, и убирает его вероятность прямого использования потоков данных клиента и устранение возможности распоряжения конфигурационными файлами облака. Стоит отметить, что способ применяется при разработке методики частной политики.

3. Следующий метод, предложенный в данной работе – проведение проверок ИБ облака, основываясь на получении численной оценки оперативного значения вероятности возникновения угрозы нарушения ИБ, применяя искусственную нейросеть. Что приведет к тому, что поставщик сможет адекватно реагировать на вероятные происшествия незамедлительно и аргументировать свои действия.

4. Реализация программы позволит определять прогнозируемое и оперативное значение вероятности возникновения угрозы нарушения ИБ. Первое значение применяется на стадии проектирования защиты информации в облаке, а второе для определения вероятности возникновения в настоящее время, учитывая возможность возникновения сложной атаки.

Публикации:

Основные публикации по теме магистерской диссертации отражены в 2 статьях, представленных на научно-практических конференциях и индексируемых РИНЦ [4, 5].

Теоретическая значимость работы:

1. Испытанный на практике метод проверки информационной безопасности в системе облачных вычислений, применялся при решении проблемы оперативного значения вероятности возникновения угрозы нарушения ИБ.

2. Реализованная модель ИБ частной политики в облаке, при должном соблюдении требований приведет к уменьшению нарушений, исключит роль пользователя со всеми правами и также различных лиц из доступа к системе. Следовательно, данные действия приведут к улучшению доверия клиентов.

Практической значимостью работы является: проведение модернизации системы, установка различных средств защиты системы облачных вычислений, а также выбор варианта реагирования на угрозу.

Результатом работы является совокупность теоретической и практической деятельности по направлению «Прикладная информатика», выполненная в процессе обучения.

В структуру работы входят: введение, 4 главы, заключение, список используемой литературы и 1 приложение.

Работа изложена на 103 страницах и включает 29 рисунков, 12 таблиц, 33 источников.

Глава 1 Исследование ИС, в основе которой лежат облачные технологии, как объекта защиты

1.1. Анализ типов облачных услуг и моделей облачного размещения, которые имеются на данный момент

Облачные вычисления предлагают перспективу гибких вычислений по требованию, предоставляемых в качестве сервисных услуг, и революционизируют многие области вычислений. По сравнению с более ранними методами обработки данных, среды облачных вычислений обеспечивают значительные преимущества, такие как доступность автоматизированных инструментов для сборки, подключения, настройки и настройки виртуальных ресурсов по требованию. Это делает их более легкими по отношению к организационным целям и организациям. [19]

Облачный клиент и облачный сервер - две составляющие облачной системы.

Внутри ИС имеются средства для вычисления, которые применяются в облаках. Данные средства необходимы для получения одной\нескольких облачных услуг. Такие средства вычислительной техники и есть - облачный клиент.

Облачным сервером считается виртуальный сервер, который обрабатывает запросы и производит хранение данных потребителей (клиентов) облачных сервисов. Также на таком сервере, различные приложения клиентов имеют возможность работать одновременно. Такое действие возможно благодаря виртуальному разделению ресурсов, которые в свою очередь, дают возможность формирования сетевых доменов. Также виртуальное разделение ресурсов позволяет разграничить уровни доступа, для разных групп потребителей в целях обработки конфиденциальной информации.

Для улучшения современного бизнеса могут применяться облачные сервисы, так как это дает возможность быстрой адаптации различным предприятиям, по причине того, что облачные вычисления стали практически невидимыми для клиентов ИТ-инфраструктуры.

За последние несколько лет крупные поставщики (такие как Amazon, Microsoft и Google) предоставили виртуальные машины через свои облака, которые клиенты могли арендовать. Эти облака используют аппаратные ресурсы и поддерживают динамическую миграцию виртуальных машин в дополнение к динамической балансировке нагрузки и подготовке по требованию. Это означает, что, арендуя виртуальные машины через облако, весь центр обработки данных современного предприятия может быть уменьшен с тысяч физических серверов до нескольких сотен (или даже десятков) хостов виртуализации.

В данное время имеется огромное множество моделей облачного размещения и видов услуг, которые предоставляют облачные вычисления. Для того чтобы понять какая облачная среда подходит БП (бизнес-процессам) компании-потребителя облачных услуг, следует изучить разницу среди существующих облачных сред.

Облачные вычисления предоставляют в качестве сервисов: ПО, инфраструктуру и платформы, основанных на моделях с оплатой по мере использования. Модели облачных сервисов, такие как Software-as-a-Service (SaaS), PaaS и Infrastructureas-a-Service (IaaS), могут быть развернуты для хранения по требованию и вычислительной мощности. [30,31]

Модели облачных сервисов можно обобщить следующим образом [22].

• SaaS позволяет потребителям запускать приложения путем виртуализации оборудования на облачных провайдерах, например, Salesforce Customer Relationship Management (CRM) 1 или Oracle Sales Cloud.

• PaaS позволяет развертывать пользовательские приложения с их зависимостями в среде, называемой контейнером. Контейнеры обеспечивают изоляцию и управление ресурсами в средах Linux. Контейнер ОС изолирует процесс от остальной части системы. Google App Engine2, Oracle Java Cloud3, Heroku4, OpenShift5, dotCloud6 и Cloud Foundry7 являются примерами PaaS облаков.

• IaaS предоставляет аппаратную платформу (например: виртуальные машины, обработку, хранение, сети и службы баз данных) в качестве службы, такой как Amazon Elastic Compute Cloud (EC2) 8, Google Compute Engine или Oracle Compute Service.

Облачные сервисы предоставляются клиентам при помощи различных моделей развертывания облака: частного, общественного, публичного и гибридного облака.

• Приватное облако: в частном облаке предоставляется облачная инфраструктура в интернете организации. Оно может принадлежать и эксплуатироваться организацией или сторонними партнерами на территории организации. [25]

• Общественное облако: инфраструктура облака, которой может использоваться несколькими организациями совместно, имея общие проблемы, например: задачи, требования безопасности, политики и соответствие нормативным требованиям.

• Публичное облако: облачная инфраструктура создана для открытого использования через общедоступный Интернет и доставляется потребителям по подписке. Публичным облаком может управлять бизнес, академическая или правительственная организация или их комбинация.

• Гибридное облако: облачная инфраструктура гибридного облака создается из двух или более облаков других типов (то есть частных, общественных или общедоступных облаков). Гибридные облака позволяют совместно использовать ресурсы и поддерживать переносимость данных и приложений.

Такие модели облачного развертывания обычно создаются в центрах обработки данных для облачных вычислений, которые принадлежат одной или нескольким организациям, где в зависимости от модели развертывания могут иметься относительно однородные или гетерогенные программные и аппаратные платформы. Центр обработки данных или компьютерный центр — это средство, используемое для размещения компьютерных систем и связанных с ними компонентов, таких как системы хранения и сети.

Как правило, он включает в себя резервные или резервные блоки питания, резервные сетевые подключения, кондиционирование воздуха и средства пожарной безопасности. В облачных дата-центрах используется небольшое количество очень больших приложений, где рабочие нагрузки облачных вычислений спроектированы так, чтобы изящно допускать большое количество сбоев компонентов, практически не влияя на производительность и доступность уровня обслуживания. Эталонная архитектура облачных вычислений на рисунке 2 определяет пять основных участников облачной сферы: пользователи\поставщики облачных услуг, облачные аудиторы и компании, управляющие облачными сервисами. Каждый из этих действующих лиц является субъектом (человеком или организацией), которая участвует в выполнении задач в облачных вычислениях [19].

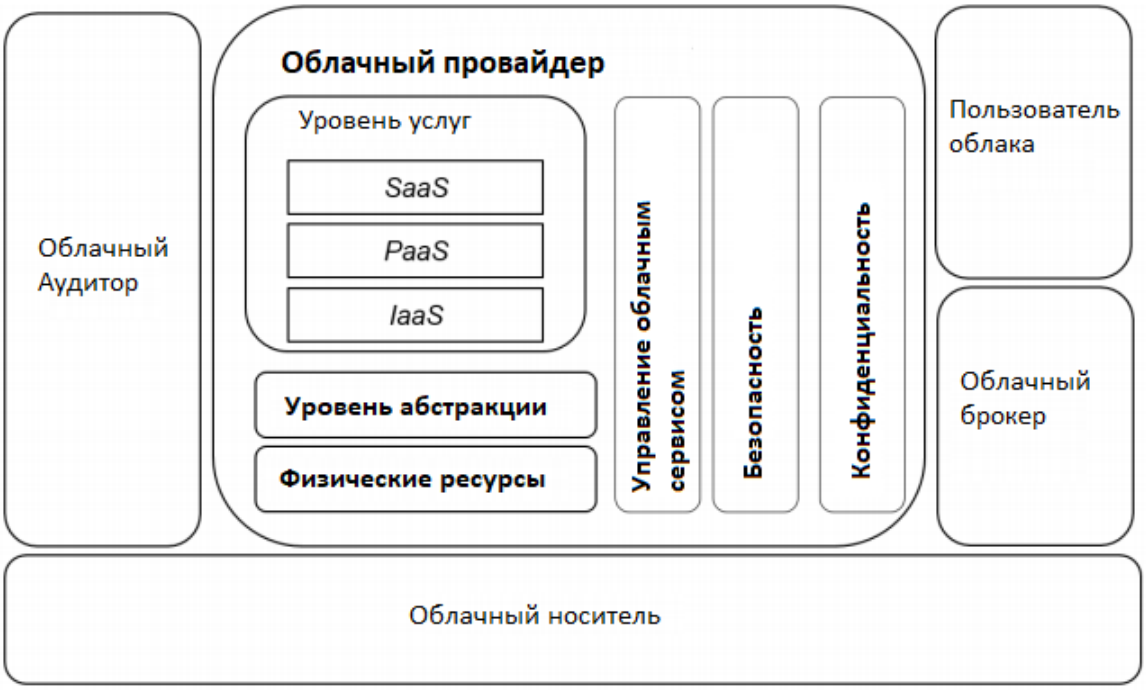


Рисунок 1.1 - Эталонная архитектура облачных вычислений

Пользователь облака (клиент) — это человек или организация, использующий услуги облачных провайдеров в целях деловых отношений.

Основная задача облачного провайдера - поддержание облачных сервисов доступными для клиентов.

Задачей аудитора (проверяющего) - проведение независимых оценок для облачных сервисов. Проверки так же проходят различные операции, производительность и безопасность при облачном развертывании.

Облачный брокер выполняет следующие функции: управление использованием, производительностью и доставкой облачных услуг, также устанавливает отношения между поставщиками\потребителями облачных услуг.

Облачный оператор следит за подключением и передачей облачных услуг от облачных провайдеров к облачным клиентам через базовую сеть.

Хотя облачные вычисления практичны и рентабельны, при использовании систем, которые не предоставляются собственными силами, могут возникнуть проблемы с безопасностью. Чтобы изучить их и найти подходящие решения, необходимо понять несколько ключевых концепций и технологий, широко используемых в облачных вычислениях, таких как механизмы виртуализации, разновидности облачных сервисов и «контейнерные» технологии.

1.2 Анализ источников из литературы, в которых рассматриваются проблемы облачных вычислений

На данный момент одно из важнейших направлений IT-технологий — это облачные вычисления, которые в свою очередь считаются одним из лучших решением с целью поддержки ИС для различных предприятий, из-за того, что имеют огромное количество очевидных положительных сторон, в отличии от стандартных средств хранения информации. Уже сейчас многие приложения, ПО, которые предназначены для обработки данных, базируются на облачных сервисах. [1]

Но у облачных вычислений имеются свои проблемы, которые в свою очередь затрудняют использование ими.

Основная проблема - безопасность и сохранение данных приватными. Большое количество экспертов не дают 100% гарантии, что конфиденциальные данные, хранящиеся в облаке, будут полностью защищены от атак. Чтобы

решить данную задачу "о сохранении данных в облаке конфиденциальными", необходимо реализовать стандарты безопасности.

На сегодняшний день существует следующая проблема в РФ, связанная с сохранением данных в облаке конфиденциальными - отсутствие законов\стандартов для ИБ в облаках. Данная ситуация усложняет конкурентную борьбу среди поставщиков облачных сервисов. Также у них пропадает возможность стремительно совершенствоваться, что в следствии приводит к тому, что рынок данных услуг становится дороже из-за непрозрачности. [15]

Еще одна из проблем облачных вычислений - доверие потребителя. Большое количество потребителей облачных услуг опасаются за сохранность конфиденциальной информации и ее защиту.

Следующая проблема, связанная с ИБ в облаках - центры обработки данных могут иметь возможность размещения в разных странах. Любая страна имеет право получить конфиденциальную информацию, которая храниться в данном центре.

1.3 Исследование имеющихся стандартов и нормативных правовых документов в сфере ИБ облачных сред

Для того чтобы производить какую-либо деятельность по защите конфиденциальных данных в облаке, необходимо опираться на действующие нормативно-правовые документы. На данный момент на стадии разработки находятся документы, которые позволят вести разработку и эксплуатировать облачные сервисы и сохранять информацию конфиденциальной.

Сейчас в нашей стране был разработан стандарт о защите информации в облаке - ГОСТ 56938 «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации», разработанный федеральным автономным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" дата введения: 1 июня 2017г. Данный ГОСТ обращает внимание на

то, что угрозы ИБ могут возникнуть из-за использования технологий виртуализации, примерами таких угроз являются: атаки на ВМ, виртуальное сетевое оборудование и устройства, гипервизор и так далее.

Также в РФ существует следующий проект ГОСТа "Защита информации. Требования по защите информации, обрабатываемой с использованием технологий "Облачных вычислений"", данный проект еще находится на стадии разработки, и носит исключительно информационный характер.

Также в РФ существует методический документ, созданный федеральной службой по тех. и экспортному контролю, утвержден от 11 февраля 2014года: «Меры защиты в государственных информационных системах». В данном документе описаны требования для защиты данных, хранящихся в облаке, от несанкционированного доступа. Также в нем описаны различные термины, касающиеся облачных вычислений, приведены примеры видов облачных услуг, список объектов, для защиты в облаке, и угрозы ИБ.

Требования о защите конфиденциальных данных в облаке, которые изложены в данном документе, адресованы поставщику облачных сервисов. Также в данном документе описаны объекты, которые следует защищать, примеры объектов: копии данных, хранящиеся в облаке, информационные носители\ресурсы, прикладное ПО, информация с ВМ (виртуальных машин) и так далее.

Данный методический документ обладает и негативными моментами, например: нет точных требований о защите конфиденциальных данных, которые могут храниться в облаке.

Также в мае 2014 года был создан законопроект «О внесении изменений в отдельные законодательные акты РФ в части использования облачных вычислений». Законопроектом предлагается внести изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» в изменении определений понятий, которые применяются в формировании и предоставлении облачных сервисов, также условия применений данных сервисов, и методов их предоставления и так далее.

Рассмотрев данный законопроект, было проанализировано положение, которое находится в нем. Данное приложение включает в себя требование о финансовой устойчивости и степень профессиональной обученности поставщика для защиты информации.

Для того, чтобы предоставить защиту персональных данных в облаке, имеется следующее предложение о внесение изменений в закон "О персональных данных".

Полагаясь на вышеперечисленное, можно сделать вывод, что в РФ большое число нормативно-правовых документов о сохранении конфиденциальности данных облачных сервисах не покрывают всех аспектов защиты информации в облаках или находятся на стадии проектирования. Выполнив анализ требований к законам, о защите данных в облачных вычислениях, других стран, можно понять, что их законы реализованы и более требовательны. [24]

Например, National Institute of Standards and Technology − Национальный Институт стандартов и технологий США, разработал стандарт архитектуры облачных вычислений. Понятие облачной системы, здесь описано следующим образом: коллекция источников (ресурсов) , которая доступна при помощи сети для клиентов облачных сервисов. Цель данного стандарта - раздробление системы облака на 5 основных вопросов, которые вызывают дискуссионные ситуации. Чтобы избежать споров, были разработаны утверждения:

– Облачный сервис не является исправным для клиента, если сеть не безопасна, другими словами, любой клиент должен иметь надежный сетевой доступ.

– Не только поставщик, но и каждый потребитель облачных услуг обязан обеспечивать безопасность облаку, а именно, самостоятельно поддерживать, контролировать и сопровождать его.

– Поставщик облачных сервисов обязан без обращений к клиентам, выполнять деление нагрузки между ВМ, данное действие должно выполнятся с целью продуктивного управления сферами облака.

– В одно время в общей локальной сети и общем облаке, могут быть произведены несколько вычислительных процессов разных клиентов, но угроза хищения конфиденциальных данных клиента, если ПО или политика безопасности имеет незащищенность или малейшую уязвимость.

– Проблема пропускной способности сети появляется по причине того, что клиенты, выполняют загрузку\выгрузку какой-то информации, превышающие скорость информации в сети, в связи с эти происходят сетевые задержки, являющиеся проблемой.

– Также в данном стандарте есть описание 4-х моделей развертывания, о которых было ранее подробное описание:

– Приватное облако;

– общественное облако;

– Гибридное облако;

– Публичное облако.

Периметр безопасности, который необходим для размещения любой модели развертывания, напрямую выполняет контроль - клиент. И как результат, он же дает контроль подписчикам над информацией, которая храниться в облаке.

В одном из штатов США был основан "Альянс облачной безопасности " (CSA). Данная организация является одним из лучших специалистом в области обеспечения безопасности в облачных вычислениях. Специалисты данной организации реализовали методическое пособие, в котором имеются рекомендации по оценки угроз в облаке. Также эксперты, работающие, на эту организацию установили следующие мнение: угроз ИБ в облачных вычислениях всего семь разновидностей. Примерами данных разновидностей являются:

– Несанкционированный доступ к облаку;

– Незащищенные API;

– Ошибки при работе специалистов на стороне поставщика;

– Уязвимости в общей среде;

– Потеря или утечка информации, данных пользователей, учетных записей;

– Угрозы, о которых изначально не было известно.

– Сервисы IaaS и PaaS, являются самыми ненадежными, по мнению специалистов CSA. Чтобы избежать атак на данные сервисы, они рекомендуют:

– Производить слежку за информацией платежных систем и публичных черных списков IP-адресов;

– Отслеживать сетевой трафик;

– Создать жесткие правила для первоначальной регистрации

Зачастую поставщики услуг дорабатывают прикладные программы с целью предоставления дополнительных сервисов, но это влечет к угрозам безопасности системы. Эксперты рекомендуют выполнять следующие действия:

– Обеспечить строгую аутентификацию;

– Шифрование трафика;

– Контролировать доступ;

– анализировать цепочки зависимостей, которые имеют отношение к интерфейсам прикладного программирования.

Также угрозу безопасности связана с тем, что множества ИТ-сервисов, работают под одним управлением в интересах различных заказчиков. Существует вероятность того, что поставщик услуг имеет полный доступ к данным и ресурсам, что создает возможность несанкционированного доступа, и обнаружить это практически невозможно. Данная проблема касается всех видов облачных сервисов, SaaS, IaaS и PaaS не исключения.

Иногда для несанкционированного доступа мошенники похищают учетные данные. Это происходит с помощью вредоносного ПО, фишинга и неполной защищенности оборудования. Чтобы избежать таких ситуаций необходимо запретить использование общих учетных записей, ввести

использование многофакторной аутентификации, соблюдать все нормы политики безопасности и анализировать их у поставщика, также следует мониторить несанкционированной активность. Данная проблема может возникнуть в следствии того, что получатель облачных услуг не имеет полного представления о рисах ИБ в облачной среде.

Trusted Computing Group (TCG) — это еще один пример организации, которая беспокоится о безопасности в облаке. Данная организация разрабатывает универсальный стандарт переносимости и управления облачными сервисами.

Проведя анализ нормативно-правовых документов и стандартов в области безопасности облачных услуг, можно сделать вывод, что российские стандарты находятся на стадии разработки или их не существует во все. В то время как зарубежные стандарты и нормативно-правовые документы, которые разработаны для ИБ облаков давно используются в различных странах, но в России данные стандарты не могут быть использованы.

1.4 Анализ вопросов предоставления ИБ в облачных средах

На сегодняшний день, как было уже замечено ранее, облачные вычисления очень быстро развиваются, но проблема защиты данных в облаке не решена, ведь очень часто появляются новости о том, что конфиденциальную информацию похитили из облака. Это с тем, что возможности информационных систем увеличиваются и совершенствуются, тоже самое происходит с информационными угрозами.

Очень часто эксперты обращают внимание, что не стоит полностью доверять поставщикам облачных услуг в сохранении данных конфиденциальными. Существует суждение, сохранение данных конфиденциальными - реализует поставщик облачных сервисов, соответственно, клиент получает уровень защиты данных, который устанавливается поставщиком.

Хранимая в облачной среде конфиденциальная информация, защищается поставщиком. Для сохранения данных защищенными, ему необходимо делать

независимую экспертную проверку - аудит. Который в свою очередь считается одним из обязательных требований международных стандартов для правильного существования жизненного цикла ИС.

Проблема "о сохранении данных облаке защищенными" имеется не только в России, но и в других странах.

В Соединенных штатах Америки CSA выпустил еще один документ "Матрица управления облаком" (CCM). В этом документе предложен реестр технологий ИБ, существующих на сегодняшний день, с целью применения их в облачных вычислениях. Некоторые эксперты из CSA высказывают такую точку зрения: сейчас существуют такие стандарты: "ISO 27001" и "ISO 27002", для обеспечения ИБ данных, при построении SaaS облака, но следует разработать новые нормативно-правовые документы для облачных сервисов.

Стоит обратить внимание на то, закон "о защите конфиденциальной информации» у каждого государства разработан свой. Облачные хранилища могут находится удаленно друг от друга и быть в разных странах. Поэтому провайдеры облачных услуг должны разворачивать хранилища, не нарушая законы других стран. [32]

Для того чтобы уменьшить затраты на инфраструктуру облака и сделать масштабируемой всю систему, приходит на помощь средства виртуализации в облачных вычислениях. Но данный способ дает возможность появлению новых угроз ИБ. Виртуальные машины из-за того, что могут существовать параллельно, находятся в опасности заражения вредоносным кодом, также оно может произойти в выключенном состоянии виртуальной машины (VM), через интернет-сеть. [12]

Также стоит обратить внимание на проблему изменчивости виртуальной машины, то есть она может перемещаться между физическими серверами.

У поставщиков и потребителей облачных услуг могут возникать проблемы с авторизацией, это связанно с тем, что передача данных происходит с одного узла на другой, из-за нескольких серверов.

Следующая проблема - в облачные виртуальные среды внедряется ПО антивируса. То есть требуется большое количество вычислительных ресурсов, оперативной память, чтобы позволить правильно работать антивирусному ПО.

Необходимо обратить внимание, на то, что специальные средства для обеспечения ИБ в ИС, влияют на скорость обработки данных в облаке в худшую сторону и уменьшают продуктивность. Федеральная служба по техническому и экспортному контролю и Федеральная служба безопасности на данный момент не сертифицировали ни один из продуктов ИБ для защиты облака.

Клиент, использующий облачные сервисы, не обладает следующей информацией:

- Местоположение обработки данных
- Полной информацией о среде
- Инфраструктуре облака
- Место обработке критичной информации
- Информация о вероятности возникновения угроз и ИБ системы

Из этого можно сделать следующий вывод: потребителю облачных услуг необходимо заключать договор с поставщиком таких услуг, запросив вышеперечисленную информацию. Но поставщик может отказать, это может нанести вред другим пользователям облачных услуг. Для того чтобы придти компромиссу можно внедрить средства для мониторинга событий и угроз, это дает возможность получить вероятность возникновения угроз ИБ облачных сервисов.

Проведя анализ ИБ в облаке, можно сделать вывод, что безопасность должна быть соблюдена у поставщика и потребителя облачных услуг, также у коммуникаций, связывающий их. Как поставщику, так и потребителю облачных услуг, необходимо проявить заботу о политике безопасности. Потребитель должен указать в своей политике безопасности: исключение передачи прав доступа сторонним лицам, а поставщик должен обеспечить

потребителям защиту их пользовательских мест. Также нужно с обоих сторон: определить уровень подходов и средств защиты для обеспечения нормального БП (бизнес-процесса) потребителя, и определить критичность облачных сервисов. [29]

Проанализировав текущую ситуацию в облачных средах, был выявлен ряд следующих проблем:

– В России отсутствуют стандарты и нормативно-правовые документы, которые могли бы обеспечить информационную безопасность в облаках [6]

– Угрозы ИБ, которые могу возникнуть для любой информационной системы, также угрозы, связанные с особенностями облаков

– При использование современных средств для обеспечения ИБ, снижается эффективность и скорость обработки информации потребителя в облачных сервисах.

– Федеральная служба по техническому и экспортному контролю (ФСТЭК) и Федеральная служба безопасности (ФСБ) на данный момент не сертифицировали продукты ИБ для защиты облака.

Имеется общепринятое мнение: от поставщика облачных сервисов полностью зависит безопасность в облаках. Данное мнение является ошибочным, так как защита информации в системе облачных технологий должна быть гарантирована на всей цепочки, а именно, и поставщик, и потребитель, должны поддерживать защиту данных, и на средствах связи, которые соединяют их.

В момент заключения договора с поставщиком, будущий потребитель облачных сервисов обязан выполнить запрос на мониторинг событий и управление инцидентами. Цель данного действия заключается в том, что это позволит ему оценивать угрозы нарушения ИБ информационной системы облачных технологий, и отслеживать путь распространения угрозы от определенного потребителя к конкретному критическому объекту. [33]

Проверки независимыми специалистами в области обеспечения ИБ в облаке должны выполняться для каждой системы облачных вычислений. Такие проверки должны соответствовать международным стандартам.

1.5 Выводы по первой главе

1. Изучение нормативно-правовых документов и стандартов в области защиты информации в облачных средах дает возможность сделать вывод о том, что исследование и разработка методов и инструментов для проведения проверки информационной безопасности информационной системы облачных технологий многообещающий. На сегодняшний день, основываясь на анализ нормативно-правовых документов, который был выполнен в данной работе, можно сделать вывод, что в России такие документы, которые связаны с облачными вычислениями, разработаны, но не покрывают всех аспектов, либо находятся на стадии проекта. В результате: отсутствие конкретных решений для проведения проверок в облаке. Опираясь на вышеизложенное, следует, что в условиях отсутствия нормативно-правовой базы, необходимо спроектировать и реализовать решение для проверок, целью которого является: оценка степени угроз информационной безопасности в облаке.

2. Как показало изучение стандартов, приказов, требуется реализация модели угроз, которая учитывающая все особенности инфраструктуры облака, это нужно с целью успешного прохождения проверок информационной безопасности с использованием численных методов получения вероятности возникновения угрозы с последующим выбором верным вариантом реагирования на опасные события. Для реализации модели угроз, опираться на политику частную безопасности для облаков, и следует расширить список угроз и их источников. На сегодняшний день достаточно проблематично найти исследования, задача которых выявление самих угроз и их источников в облачных средах. Для ИС облачных технологий подходы по созданию моделей угроз -отсутствуют.

3. Для получения объективных результатов проверок системы защиты облаков, следует обратить внимание на вероятность возникновения угрозы при

ее проявлении, по определенному пути, также не забывать про вероятность возникновения угрозы нарушения информационной безопасности с учетом всего перечня потенциальных угроз, согласно нормативным документам. Но методов, которые могли бы получить вероятность возникновения угрозы, полагаясь на сенсоры и датчики опасных событий, еще не разработаны.

Глава 2 Исследование вопроса выполнения аудита ИС, в основе которой лежат процессы облачных вычислений

2.1. Анализ источников литературы, которые посвящены аудиту ИБ

Рассмотрим понятие «проверка» - независимый аудит каждой отдельной области на предприятии, который может быть двух видов: внешний и внутренний.

Внешний аудит - является обязательным требованием во многих акционерных обществах и организациях. Обычно аудит проводится регулярно по инициативе руководства или акционеров.

Внутренний аудит - постоянная деятельность подразделения внутреннего аудита, которое в свою очередь оценивает вероятность возникновения угроз, повышает рентабельность и так далее.

Также существует понятие «аудит безопасности ИС». Целью такого аудита является проверка безопасности информационной системы, анализ угроз и вероятности возникновения угроз, оценка уровня защиты и соответствия стандартам информационной безопасности, разработка рекомендаций по защите конфиденциальных данных. Данный аудит является очень важным этапом при построении ИС защиты данных на любом предприятии. Для того чтобы получить полное понимание о состоянии информационной безопасности на предприятиях проводится комплексная аудиторская проверка. Такая проверка позволяет узнать слабые и незащищенные места, локализировать существующие проблемы, и создать программу построения полностью защищенной информационной системы на предприятии. На рисунке 2.1 наглядно показано, что включает в себя термин «аудит безопасности ИС».

Рисунок 2.1 - Аудит безопасности ИС

На рисунке 2.2 показаны шаги работ по проведению проверки безопасности ИС.

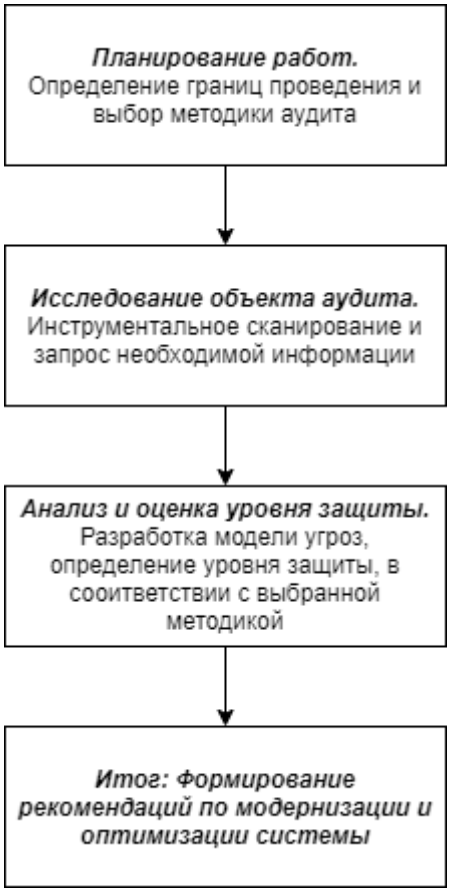


Рисунок 2.2 - Шаги работ по проведению проверки безопасности ИС

В настоящее время существует всего два способа для проведения проверок безопасности информационной системы.

Первый способ - анализ вероятности возникновения угрозы нарушения ИБ. Такой способ является очень трудозатратным. Аудитор устанавливает для исследуемой информационной системы специальную последовательность требований безопасности, основываясь на анализе вероятности возникновения

угрозы, учитывая особенности и уязвимые места этой информационной системы. Но как отмечают эксперты на сегодняшний день такой способ отсутствует для ИС, построенных на основе облачных технологий.

Второй способ - внедрение эталонов в сфере ИБ. С помощью эталонов вводится стандартированный набор условий с целью обеспечения защиты для нескольких информационных систем, которые были созданы в следствии международной практики. Эталоны устанавливают различные наборы требований для сохранения данных конфиденциальными, в зависимости от степени защищенности информационной системы. Способ является очень простым, надежным, и малозатратным, по этой причине, на практике является одним из популярным для проведения внешних проверок, с целью вывода о состоянии информационной системы. Основным минусом данного способа является: некоторое количество эталонные условия не учитывают специфику исследуемого объекта проверки.

Зачастую предприятия сталкиваются с проблемой оценки инвестиций в ИБ, полагаясь на мнения ученых. Также основываясь на их утверждениях, необходимо делать не только оценку на пригодность эталонам, но и регулярно проводить анализ вероятности возникновения угрозы, главной целью данных действий является: подбор наилучшего вида защиты конфиденциальных данных, и поможет снизить затраты на ИБ.

Для проведения проверок ИС основе облачных технологий, лучшим способом проверок является оценка вероятности возникновения угрозы нарушения ИБ, как было установлено во время анализа нормативно-правовых документов РФ [4]

2.2 Исследование нормативно-правовых документов, которые существуют на сегодняшний день, в области проверок ИБ

В данном разделе рассматривается исследование нормативно-правовых документов ИБ, которые представляются важными и перспективными при применении, с целью проведения проверок защиты ИС облачных технологий.

В настоящее время имеются несколько разработанных стандартов, которые рассматривают вероятность возникновения угрозы ИБ:

1. Американский стандарт - NIST SP 800-30:2002 «Risk Management Guide for Information Technology Systems».
2. Британский стандарт - BS 7799-3:2006 «Information security management systems. Guidelines for information security risk management»
3. Международные стандарты - ISO 17799 «Code of practice for information security management» и ISO 15408 «The Common Criteria for Information Technology Security Evaluation»
4. Спецификация по требованиям стандарта SysTrust - стандарт, разработанный Американским Институтом Сертифицированных Публичных Бухгалтеров (AICPA) и Канадским Институтом Общественных Бухгалтеров (CICA) для проведения IT - аудита.
5. Российский стандарт - ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
6. Российский стандарт - ГОСТ Р ИСО/МЭК 27007 – 2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»
7. Российский стандарт ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»

Изучив данные стандарты, можно сделать вывод, что в американском и британском стандарте оценка вероятности возникновения угрозы, а также

анализ - идентичны. Также международный стандарт ISO 17799 - копия британского стандарта. Международные стандарты, о которых писалось ранее являются фундаментом с целью аудита или проверок работ в области ИБ. Если рассмотреть подробно международный стандарт ISO 15408, который устанавливает подробные требования для защиты конфиденциальной информации, то международный стандарт ISO 17799 больше направлен на вопросы управления и организации безопасности.

Проанализировав российский стандарт ГОСТ Р ИСО/МЭК 27005-2010, можно сделать следующее заключение: данный стандарт является руководством по менеджменту угроз ИБ на предприятиях. Каждое нарушение способно нанести ущерб определенному активу или их группе, данное действие считается - угрозой ИБ. Такие действия всегда сказываются на предприятии. Для начала необходимо реализовать анализ угрозы, и какие последствия она может вызвать, прежде чем сделать вывод о том, что необходимо сделать для снижения вероятности возникновения угроз ИБ. Также исходя из описания стандарта, можно отметить, что процесс менеджмента может быть итеративным для видов деятельности как обработка угроз и оценка вероятности возникновения угроз. Что в свою очередь дает возможность для детальной оценки и углубления при каждой итерации. Но не стоит забывать, что оценку вероятности возникновения угроз необходимо проводить, зная БП предприятия.

Проанализировав следующий российский стандарт - ГОСТ Р ИСО/МЭК 27007 – 2014, то можно сделать вывод, что он необходим для предприятий, которые нуждаются в разъяснение или проведение аудитов (внутренний и внешний), также применение программы аудита ИБ. Для проведения корректного аудита необходимо разработать программу проверок, согласно данному стандарту. В основе этой программы лежит ситуация, которая взаимосвязана с угрозой ИБ на данном предприятии. Стоит также отметить, что программа аудита информационной безопасности - комплекс мероприятий по аудиту, согласно которому будут выполнены задачи для достижения

определенной цели в определенные сроки. В данном стандарте описана пошаговая деятельность по аудиту в области ИБ:

1. Начало аудита. Настройка связи с объектом аудита.
2. Подготовительные работы для начала аудиторской деятельности, то есть подготовка плана аудита и моделирование угрозы ИБ
3. Аудиторская деятельность. Сбор и проверка информации, анализ безопасности системы.
4. Отчет о сделанной работе.
5. Конец аудита. Выполнение действий по результатам аудита.

Также рассмотрев еще один российский стандарт ГОСТ Р ИСО/МЭК 31010-2011, можно отметить, что здесь имеются рекомендации по выбору и применению методов оценки вероятности возникновения угроз и факторы, которые влияют на выбор метода оценки вероятности возникновения угроз, например:

- ресурсы, которые необходимы (время, информация и так далее);
- сложность проблемы;
- оценка данных, которые получаются на выходе;

В таблице 2.1 представлены методы их описание, плюсы и минусы из данного стандарта.

Таблица2.1 - методы и описание оценки вероятности возникновения угроз

Название метода	Данные поступающие на вход\выход	Положительные стороны способа	Негативные стороны способа
Анализ вероятности возникновения угроз и критические контрольные точки (ХАССП(HACCP))	Данные на вход: технологические карты или блок-схемы процесса и сбора информации об опасных событиях. Данные на выход: карта анализа, возможные предупреждающие действия для каждой опасности.	Предоставляется документированное свидетельство качества идентификации опасности, управления и снижения вероятности возникновения угроз	Требуется чтобы угроза была распознана и идентифицирована и вероятность возникновения угроз был определена

Продолжение таблицы2.1 - методы и описание оценки вероятности возникновения угроз

Анализ уровня надежности средств защиты (LOPA)	Входные данные: основная информация о вероятности возникновения угроз, включая опасности, причины и последствия, частота причинных событий, оценки вероятности отказа барьеров защиты, оценки последствий и допустимого уровня вероятности возникновения угроз; частота инициирующих причин, оценки вероятности отказа барьеров защиты, оценки последствий и допустимого уровня вероятности возникновения угроз. Выходные данные: рекомендации относительно дальнейшего применения средств управления и их эффективности для снижения вероятности возникновения угроз.	Помогает идентифицировать наиболее критичные барьеры защиты и обеспечить их ресурсами, помогает идентифицировать операции, системы и процессы с недостаточным уровнем защитных мер.	Неизвестен метод нахождения исходных данных.

Продолжение таблицы2.1 - методы и описание оценки вероятности возникновения угроз

Предварительный анализ безопасности (PHA)	Входные данные: информация об оцениваемой системе, доступные и относящиеся к делу детали проекта системы. Выходные данные: перечень опасностей и соответствующей вероятности возникновения угроз, рекомендации по принятию вероятности возникновения угроз, рекомендуемые средства управления, требования к конструкции или запрос на выполнение более детальной оценки.	Дается возможность исследовать вероятность возникновения угроз на самых ранних стадиях жизненного цикла системы.	Не является всесторонним методом и не может обеспечить подробную информацию об опасных событиях и способах их предотвращения

Продолжение таблицы2.1 - методы и описание оценки вероятности возникновения угроз

Причинно-следственный анализ	Входные данные: опыт рабочей группы, ранее разработанные модели. Выходные данные: схемы и диаграммы, на которых изображены причины угроз	Структурированный анализ; результаты отображаются в простой форме в виде диаграмм и схем, которые легки для восприятия;	Аудиторы могут быть недостаточно компетентны, данный метод подходит только для анализа первопричины.

Исходя из вышеперечисленного, можно сделать вывод, что ни один из нормативно-правовых документов не покрывает полностью все факторы, которые, в свою очередь, оказывают воздействия на метод оценки вероятности возникновения угроз.

2.3 Изучение способов, популярных на сегодняшний день, для автоматизации проверок ИБ.

Средства для автоматизирования проверок ИБ необходимы:

- Для оценки степени защищенности ИБ на предприятии,
- Для обнаружения вероятности возникновения угроз нарушения ИБ, которые уже имеются в системе,
- Для оценки выбора рационального набора средств защиты информации.
- ПО, которое на сегодняшний день предлагает рынок делится на два вида:
- ПО, которое предусматривает базовый уровень ИБ

– Программное обеспечение, которое предусматривает полный анализ вероятности возникновения угроз.

Данные ПО дают возможность уменьшить трудозатраты на анализ вероятности возникновения угроз и разработки контрмеры для защиты ИБ, но применение их необязательное требование к предприятию.

2.3.1ПО, которое предусматривает базовый уровень ИБ

Сегодня на рынке есть небольшое количество программ, которые позволяют сделать анализ вероятности возникновения угроз на базовом уровне ИБ. Например: Программный продукт - Consultative Objective and Bi-Functional Risk Analysis (COBRA), используется для аудита ИБ или для работ служб, которые ответственные за сохранение информации конфиденциальной. Данное программное обеспечение было разработано в Британии, компанией Risk Associates. Также необходимо отметить COBRA соответствует Британскому стандарту - BS 7799. Для количественной оценки вероятности возникновения угроз - применяется данное ПО. Так как в нем имеется стандарт, как база требований, появляется возможность проверки ИБ на требования стандарту. Плюсы программы:

– Простота в области применения
– Соответствие международному стандарту.
– Минусы программы:
– Отсутствие возможности установки требований безопасности при расчете значения вероятности возникновения угроз юзером,
– Отсутствие стабильного запуска отчета для Win2000 и выше,
– Отсутствие выбора языка ПО.

Следующий метод, предусматривающий базовый уровень ИБ - RA Software Tool. Огромный плюс данного метода в том, что он соответствует сразу нескольким международным стандартам. Минусы этого метода:

– Отсутствует возможность оценки вероятности возникновения угроз

– Система проверяется только на соответствие стандартам

– Нет возможности сменить язык программы

2.3.2 Программное обеспечение, которое предусматривает полный анализ вероятности возникновения угроз.

На сегодняшний день существуют ПО и методы системного анализа, которые позволяют сделать полный анализ вероятности возникновения угроз. Например, универсальный инструмент CRAMM, который решает аудиторские задачи, а также производит анализ вероятности возникновения угроз. Но у данного программного продукта есть ряд своих минусов:

– Данный метод требует высокой квалификации аудитора информационной безопасности

– Требуются большие трудозатраты на работу аудитора

– Подходит только для существующих информационных систем, которые уже используются

– Не вся документация в отчете приносит пользу

– Отсутствует возможность внесения возможность адаптации к определенному предприятию

Еще одним примером ПО для полного анализа вероятности возникновения угроз является RiskWatch. Основной плюс данной программы - проведение различных видов аудитов ИБ. Минусами этого ПО является:

– ПО подходит только для предприятий, на котором ведется документация по происшествиям в сфере ИБ

– Возникает необходимость в найме специалиста, который сможет определить объем потерь от угрозы ИБ

– Вероятности возникновения угрозы информационной и физической безопасности просматриваются вместе

Для проведения анализа вероятности возникновения угроз путем анализа модели информационных потоков и анализа модели угроз и уязвимостей можно

при помощи универсального инструмента ГРИФ2006, который имеет 2 метода анализа вероятности возникновения угроз.

Первый метод: Оценка вероятности возникновения угроз информационной системы в данном методе происходит путем моделирования угроз и уязвимостей, конфиденциальность любого ресурса определяется после анализа угроз и уязвимостей, которые действуют на него. У данного метода есть следующие минусы:

– Отсутствует возможность сравнивать отчеты на разных стадиях внедрения

– Добавление требований политики безопасности компании невозможно.

– Второй метод: здесь анализ вероятности возникновения угроз нарушения ИБ, происходит при помощи построения модели ИБ предприятия. Данный метод имеет ряд следующих минусов:

– Учет одного из двух наличия\отсутствия преград на пути распространения угроз

– СрЗ не оказывает влияние на величину вероятности возникновения угроз нарушения ИБ

– Учет атак, которые происходят от пользователей, не рассматривается

Еще один программный комплекс, который тоже делает оценку вероятности возникновения угроз нарушения ИБ - RiskAnalyzer. К минусам данного комлекса можно отнести ручное строительство моделей угроз в виде нечетких когнитивных карт. Для данного процесса необходима высокая квалификация аудитора информационной безопасности.

Стоит заметить, что у всех рассмотренных методов и ПО имеются схожие недостатки. Например: нет возможности учета тех. характеристик, которые применяются для средств защиты. [5]

2.4 Исследование угроз нарушения ИБ типичных для облаков

В момент создания системы, которая обеспечивает ИБ в облачных вычислениях, нужно обращать внимание на угрозы, которые возникают в следствии нарушения ИБ определенному объекту защиты. Далее представлен список угроз в системах облачных вычислений, в основе которых лежит модель SaaS. Угрозы ИБ делятся на два типа:

- Угрозы ИБ для потребителей облачных услуг
- Угрозы ИБ для поставщика облачных услуг

2.4.1 Угрозы ИБ для потребителей облачных услуг

– Угроза ИБ, которая возникает по причине, того, что клиент и поставщик облачных сервисов не смогли разграничить обязанности. Во избежание данной угрозы, следует: заключить договор с четко прописанными в нем пунктами о безопасности, который будут соблюдать обе стороны [27]

– Угроза ИБ, которая возникает потому, что клиент облачных услуг передает поставщику какую-то часть функций управления своей ИС. Например, поставщику передается управление ОС (операционными системами) и прикладным ПО, при оказании услуги SaaS. Если у клиента отсутствует возможность самостоятельного контроля параметров, которые были заданы им, то это приводит к лишению полноценной защиты конфиденциальных данных, так как админ поставщика имеет доступ к данным клиента.

– Следующая угроза связана с проблемой взаимодоверия. Поставщик применяет программные облачные технологии, к которым у клиента нет доступа, по этой причине, у клиентов нет возможности реально оценить уровень защищенности данных поставщиком. Решением данной проблемы может выступать аудит системы облачных вычислений, с предоставлением результата об гарантии сохранения информации конфиденциальной.

– Угроза ИБ, которая возникает в связи с несанкционированным доступом со стороны потребителей. Из-за того, что облака являются удаленным ресурсом. Здесь угрозы могут возникнуть, так как клиент некачественно

защищает свою сеть. Во избежание таких ситуаций, предлагается введение политике безопасности.

– Облако является общедоступным, поэтому может возникать угроза ИБ.

– Как было описано ранее, облачные сервера могут быть расположены в другом государстве с другими законами о защите информации, следовательно, появляется новая угроза, связанная с управлением облачными данными.

– Причиной возникновения данной угрозой ИБ вседозволенность со стороны клиента. Клиент имеет права устанавливать свое ПО в облаке, которое, возможно, может являться не безопасным, исходя из этого, может быть выполнен взлом доступа.

2.4.2 Угрозы ИБ для поставщика облачных услуг

– Угроза ИБ, которая возникает в связи с нечетким распределением ответственности между провайдером и клиентом облака.

– Угроза ИБ, которая возникает в связи несогласованностью политик безопасности. Так как у поставщиков и потребителей зачастую бывают разные политики безопасностей для одинаковых средств защиты, это может привести к тому, что произойдет утечка конфиденциальных данных.

– Угроза ИБ, которая возникает в связи с модернизацией облачных вычислений. Так как есть возможность поставить на виртуальную машину новое ПО, появляется вероятность возникновения угроз, так как новое программное обеспечение может иметь уязвимости. Чтобы избежать таких инцидентов, необходимо проводить аудит ИБ, с целью определения защищенности системы.

– Данная угроза связана отсутствием подтверждения личности пользователя (аутентификации).

– Виртуализация - одна из угроз для ИБ, так как единая рабочая станция, выступающая сервером, ресурсы которой разделены между виртуальными машинами пользователей.

Также к угрозе, которая актуальна, как для поставщика, так и потребителя можно отнести угрозу технического сбоя. Они могут происходит по двум причинам: сбой коммуникационного оборудования, сбой ПО у поставщика или потребителя облачных услуг.

Проанализировав возможные угрозы ИБ, которые могут произойти у поставщика и потребителя, был составлен список источников угроз, которые могут возникнуть. Данный список представлен ниже в таблице 2.2

Таблица 2.2 - Список источников угроз

Источник угрозы	Описание источника	Причина угрозы	Особенности угроз в системе облачных вычислений
Процесс, запущенный потребителем	Внутренний нарушитель в облаке	Невыполнение требований по ИБ в облачных сервисах. Если пользователь не соблюдает правила описанные в политике безопасности, у нарушителей появляется возможность для несанкционированного доступа к облаку.	Воздействие источника угроз аналогично традиционным ИС

Продолжение таблицы 2.2 - Список источников угроз

Запущенный процесс администратором поставщика облака	Внутренний нарушитель в облаке	Администратор имеет доступ ко всем компонентам системы облачных вычислений. Может организовать несанкционированный доступ к конфиденциальной информации потребителя	Из-за переноса части информации потребителя, появляется возможность у сотрудника-поставщика к этой информации
Процесс, запущенный иным потребителем облака	Внешний нарушитель в облаке	Возможность реализации угрозы по отношению к другим пользователям облачных услуг	Угроза возникает в следствии того, что потребители сами обслуживают себя. Также из-за масштабируемости и консолидацией вычислительных ресурсов
Процесс, запущенный злоумышленником	Внешний нарушитель в облаке	Получения несанкционированного к конфиденциальной информации в облаке производит при помощи сторонних программ, также не является потребителем облачных услуг	Воздействие источника угроз аналогично традиционным ИС

Ниже на рисунке 2.3 показан процесс распространения угроз в системе облачных вычислений. Модель создана согласно полному перечню источников угроз.

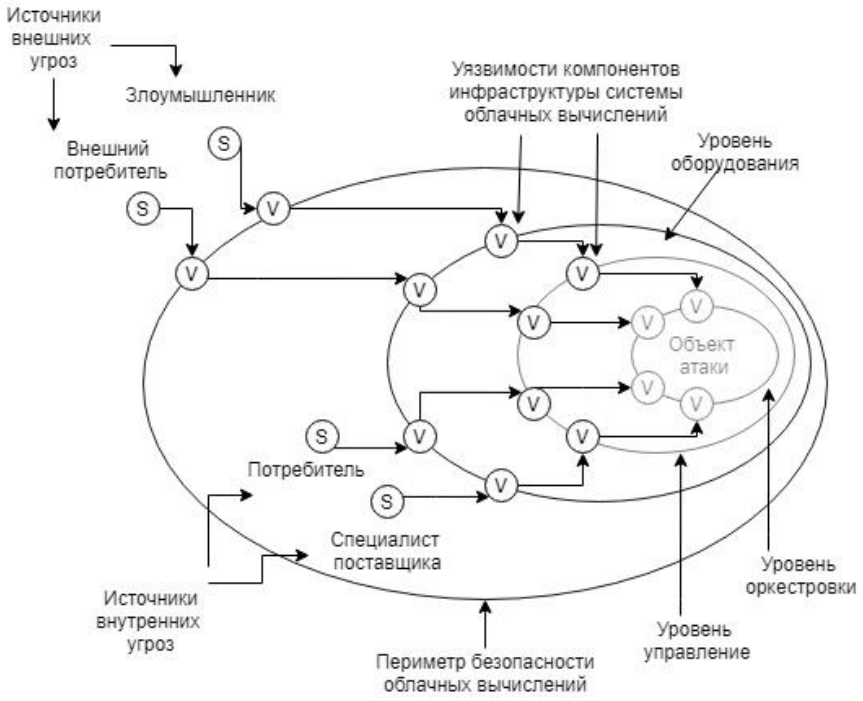


Рисунок 2.3 - Модель распространения угроз

В рамках данной работы под системой облачных вычислений понимается ИС взаимодействия определенного потребителя (клиента) облачных услуг с поставщиком, периметр ИС, в основе которой лежат облачные вычисления. Сеть клиента и поставщика, который обслуживает, конкретного клиента заключается в данном периметре.

Самая важная идея - рассмотрение периметра, как барьера по отношению к различным операциям доступа системы облачных вычислений. Такого рода барьер будет служить для обеспечения защищенности облака. Отношение к облаку делится на 2 вида:

– Субъекты, которые внутри периметра безопасности (внутренние), производят доступ к ресурсам в облаке согласно политике безопасности.

– Такие субъекты находятся за приделами периметра безопасности (внешние). Они не должны получать доступ к ресурсам, так как не обладают правами на данное действие. Но бывают ситуации, когда внешним субъектам

предоставлен доступ к ресурсам, например средствами контроля границ, в основе которых лежат определенные политики доступа.

Уровень оборудования - на данном уровне, он же первый уровень ИС в облачных технологиях, приходят в исполнение функции, обязанности которых лежат на тех.средствах. Примером считается оборудование для коммуникаций клиента и поставщика, сервера и так далее.

Уровень руководства - на данном уровне происходит централизация ресурсов системы облачных вычислений, управление ВМ и виртуальными сетями.

Уровень оркестровки - на данном уровне храниться специализированное программное обеспечение, которое необходимо для управление серверами ИС облачных технологий, ПО для ИБ в облаке, программы который устанавливает сам потребитель облачных услуг.

2.5 Формализованное описание системы защиты информации системы облачных вычислений на основе абстрактно-алгебраического подхода

На защиту процесс защиты конфиденциальных данных влияет множество факторов. Для того чтобы выявить такие факторы, зачастую используется математическое описание. Проблема защиты конфиденциальных данных имеет отношение к слабоструктурированных и слабоформализуемых проблемам.

На сегодняшний день имеется несколько способов к описанию качественных и количественных проблем при помощи математических формул, такое действие дает возможность найти разумный способ действий, который в свою очередь опирается на количественные оценки. Математическая модель требуется для анализа объекта и процесса, которые в свою очередь представляются как математические действия. [13]

Также необходимы модели, которые показывают важные характеристики моделируемого явления, с целью описания защиты конфиденциальных данных в облаке, применяя символические системы.

Абстрактно-алгебраический подход к описанию систем будет рассмотрен в данной работе для формализации системы защиты конфиденциальных

данных в системе облачных вычислений. Системы защиты конфиденциальных - объединение исполнителей, органов и техники для защиты объектов информации.

$A = \{Q, R, B, Z, K, T_a, M, Y\}$ - множество элементов системы защиты конфиденциальных данных

где Q – элемент информационных ресурсов, таких как: ВМ и приложения пользователя, объекты облачного хранилища, экземпляр БД, и так далее. Также данный элемент является объектом атаки.

R – элемент, который является частью механизма системы облачных вычислений;

B – элемент, способный обеспечить защиту информации и сервисов безопасности системы облачных вычислений;

Z – элемент, в который включены стандарты, приказы и другие документы о защите информации, в том числе частная политика безопасности;

K – в основе данного элемента лежат источники угроз. Например: субъект-нарушитель, который может являться, и может не являться потребителем облачных сервисов, то есть, работник или сторонний злоумышлений.

T_a– элемент, в котором может произойти активизация источников угроз;

M –элемент в котором хранятся состояния облака;

Y – в данном элементе происходит смена состояния облака с опасного в надежное и с надежного в опасное.

Набор существенных свойств в определенный момент времени - элемент возможность активирования угроз $t_a \in T_a$и $k \in K$ - элемент источников угроз нарушения безопасности в облаке

Операционные свойства системы - элементы информационных ресурсов $q \in Q$и элементы частей механизма облака $r \in R$.

Чтобы выполнить анализ ИБ для всех состояний системы необходимо сделать ввод 4-х атрибутов, для определения пространства активации источника угроз:

$t_a^{зл}$ – возможность того, что источником угрозы будет являться - злоумышленник.

$t_a^{адм}$ – возможность активизации сотрудника поставщика облачных услуг.

$t_a^{внш}$ – возможность активизации иного нарушителя, который является иным потребителем облачных услуг;

$t_a^{кл}$ – возможность активизации сотрудника-нарушителя компании потребителя облачных услуг.

$$t_a^{зл}, t_a^{адм}, t_a^{внш}, t_a^{кл} \in [0,1]$$

Состояние системы облачных вычислений, при котором ($t_a^{зл}, t_a^{адм}$, $t_a^{внш}, t_a^{кл}) = (0,0,0,0)$ – данное состояние называется безопасным, иначе состояние можно считать небезопасным.

Исходя из этого пространство состояний, которые являются безопасными записывается следующим соотношением.

$$M^+ = \{m \in M | (\ t_a^{зл}, t_a^{адм}, t_a^{внш}, t_a^{кл}) = (0,0,0,0)\}$$

Как было изложено ранее, если один из атрибутов будет отличен от 0, то он считается небезопасным, описание соотношения:

$$M^- = \{m \in M | \exists \forall m \in \{\ t_a^{зл}, t_a^{адм}, t_a^{внш}, t_a^{кл}\}, m \neq 0\}$$

$M^- \cup M^+ = M$ – таким соотношением описывается пространство состояний системы облачных вычислений.

H^- – описывается переход системы облачных вычислений из безопасного в небезопасное состояние.

$$H^- = y | y \in Y, y: M^+ \to M^-$$

H+ – описывается переход системы в состояние противоположное H^-

$$H^- = y | y \in Y, y: M^- \to M^+$$

Переход состояния, который описан в H^- , может привести к повышению нарушений ИБ L. Для системы защиты данных необходимы создаваться следующие условия, с целью снижения уровня вероятности возникновения угроз, в таком случае, уменьшится вероятность перехода состояния H^-. Также позволительно, чтобы уровень вероятности возникновения угроз опускался до допустимого.

$$A \Leftrightarrow (L \to 0) \coloneqq l: M^+ | l: M^- \to M^+$$

$W = \{Q, R, K, C, D\}$ - множество элементов угроза ИБ системы облачных вычислений на основании алгебраического метода

где C – элементы, относящиеся к уязвимым частям механизма облака

D – элементы, которые лежат в основе реализации угроз.

Место, которое является слабым местом в барьере либо его отсутствие для распространения атаки называется- незащищенность системы облачных вычислений $c \in C$. Если такая незащищенность существует, то может повлечь за собой осуществление атаки на ресурс ИС облачных вычислений:

$$C = \{c | c = b \wedge m | k \wedge m \Rightarrow H^-\}$$

Пространство угроз нарушения ИБ – комплекс объектов и субъектов атаки, при котором система облачных вычислений переходит из безопасного в небезопасное состояния:

$$W = \{w \epsilon d | w = 0 \wedge m | k \wedge m \Rightarrow M^-\}$$

Различие традиционных ИС и облачных заключается в том, что элементы Q, R, K, T_aмогут расширяться в облачных ИС. Иными словами, математическая модель, которая предложена в данной работе может применяться и к традиционным ИС. Если рассматривать облачные ИС, то при расширении элементов элементы Q, R, K, T_a, будут изменены и следующие элементы: C, D. Исходя из этого, можно сделать вывод, что при увеличении ИС угрозы нарушения ИБ, тоже увеличатся.

Если нарушитель(злоумышленник) определенное действие, которое связано с проведением атаки, то ему необходимо использовать незащищенность периметра, либо он может активизировать атаки.

Любое действие злоумышленника связано с достижением частных целей, но для проведения атаки им нужно активировать или использовать уязвимости в компонентах системы облачных вычислений, стоит отметить случай, когда злоумышленник, имеет доступ к периметру безопасности облачных вычислений. Чтобы избежать таких угроз необходимо выполнить реализацию политики безопасности для облака, чтобы избежать преднамеренных угроз.

2.6 Выводы по второй главе

1. Так как имеется необходимость проведения проверок ИБ, целесообразно разработать программу, реализующую результаты исследований, для уменьшения времени проверок ИБ. Так как некоторое количество компаний приходит к тому, что облачные технологии, могут применяться в ведении бизнеса. В результате этого, нужно обратить внимание на сложные сценарии нарушения безопасности в системе облачных вычислений, при реализации программы. Одним из примеров, который способен выполнять данные функции – искусственная нейросеть.

2. Разработана архитектура системы облачных вычислений для общественного облака и концепция вычислительного облака для предоставления услуги SaaS, которая учитывает требования к типичной ИС облачных вычислений и требования архитектуры сетевой безопасности.

3. Алгебраический метод, который сформулирован в диссертации, представлен перечень потенциальных угроз для системы облачных вычислений и их источников с учетом облака, предложено описание защиты информации системы облачных вычислений.

Глава 3 Разработка метода частной политики ИБ в облаке

Поддержка степени защищенности конфиденциальной информации в облаке целиком выполняется только поставщиком облачных сервисом, такое мнение высказывают некоторые специалисты. Но, также необходимо предусмотреть защиту для пользователей в системе. Для этого следует выполнить реализацию политики безопасности для облака в целом.

Термин "политика ИБ предприятия" имеет такое значение: комплект рекомендаций, который разработан для защиты конфиденциальной информации на предприятии. В данный комплект могут быть включены различные практики, правила, оценка вероятности возникновения угроз и так далее. Для каждого предприятия необходимо разрабатывать индивидуальную политику безопасности, по причине того, что процесс обработки активов и потоков, применяемых в ИС, различается. Также следует обращать внимание на тип предоставляемой услуги клиенту (примеры услуг: SaaS, PaaS, IaaS) и принцип развертки облака (примеры: частное облако, публичное облако и другие типы облака). Также как отмечается, в момент создания политики для каждой информационной системы, она разбивается на более мелкие политики безопасности, с целью углубления в конкретные нюансы ИБ системы.[3]

3.1 Моделирование политики ИБ предприятия в системе облачных вычислений

Как было изложено ранее, разработка политики ИБ на предприятии необходимо, для детального анализа и управления ИБ в системе, с целью обеспечения защиты данных в облаке. При разработке частной политики необходимо учитывать действия, которые связывают поставщика и клиента использующих облачные технологии.

Верно, реализованная частная политика ИБ приведет к тому, что произойдет рост надежности системы, будет применяться верная поддержка и управление ею, следовательно, вероятность возникновения возможности нарушения ИБ будет уменьшена, а также возрастет доверие клиентов облачных

сервисов. Но также стоит помнить, о том, что поставщик и клиент обязаны соблюдать данную политику.

При моделировании частной политики ИБ, был в основу взять проект международного стандарта «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения». В соответствии с данным стандартом будет применена услуга SaaS. Так как данная услуга требует огромного внимания, были разработаны следующие требования, которые изображены на рисунке в виде модели политики ИБ.

Соблюдение дополнительных требований к политике ИБ системы облачных вычислений, которые были предложены в данной работе, приведет к тому, что будет возможно избежать кражу конфиденциальных данных при использовании облачных вычислений как поставщиком, так и клиентом облачных сервисов, следовательно, это повлияет на доверие клиентов в лучшую сторону.

3.1.1 Применение технологии при создании политики ИБ в облаке

В данной работе предлагается применение технологии разработки политики ИБ с использованием формальной модели, основанной на математической модели управления доступом на основе ролей для системы облачных вычислений. Данная модель способствует тому, что формирование политики безопасности происходит, опираясь на роли для юзеров. Другими словами, каждому пользователю в системе облачных вычислений будет выдаваться определенная роль с конкретными правами. Такая модель позволит облегчить управление облаком в целом, и убирает возможность появления нарушений ИБ, связанных с отсутствием четкого распределения обязанностей. [9]

Применяя данную технологию, стоит отметить, что у поставщика и клиента могут возникнуть расхождения о представлении по проблемам, связанных с разделением обязательств и ролей. Чтобы избежать возможных

конфликтов, поставщик должен разработать иерархии ролей для администраторов и для обычных пользователей.

У каждой роли имеются свои определенные обязанности в облаке. То есть, каждый клиент имеет свою определенную роль, которая имеет конкретные права и обязательства. Но стоит отметить, что роли задаются не навсегда, они могут изменяться, например, по причине, подключений новых приложений, в таком случае у некоторых клиентов, обязанности могут увечится, соответственно, расшириться доступ на них.

В мат. модели управления доступом ролей применяются следующие составляющие:

U – Юзеры.

R – Роли.

P – Права доступа к объектам облака.

S – Сессии пользователей внутри облака.

L – решетка уровней защиты данных.

$PA: R \rightarrow 2^P$– с помощью данной функции происходит установка ролям определенной совокупности правил доступа, где для любого $p \in P$ имеется $r \in R$, такая, что $p \in PA(r)$.

$UA: R \rightarrow 2^R$– с помощью данной функции происходит установка каждому юзеру определенное количество ролей, где для каждой роли требуется аутентификация в системе облачных вычислений.

Следующая функция $user: S \rightarrow U$ необходима для определения логина (имени) юзера для каждой сессии внутри облака, и

$roles: U \rightarrow 2^R$ – применяя данную функцию, можно установить определенное количество ролей для каждого юзера, который имеется в облачной сессии, где в любой временной интервал для каждого $s \in S$ выполняется условие $\mathrm{roles(s)} \subseteq \mathrm{UA(user(s))}$.

c: U $\rightarrow$ L – функция уровня доступа юзера.

c: O $\rightarrow$ L– функция уровня защиты объекта облака.

A $= \{read, write\}$ – возможный вид доступа.

AR – Административные роли ($AR \cap R = \emptyset$) .

AP – Административные права доступа к объектам облака($AP \cap P = \emptyset$) .

Применяя функцию $ARA: AR \rightarrow 2^{AP}$ можно выявить определенные права администратора доступа для любой роли администратора, где для каждого $p \in AP$ имеется $r \in R$ такая, что $p \in ARA(r)$.

$AUA: U \rightarrow 2^{AR}$ – помощью данной функции задается определение для любого юзера определенное количество административных ролей.

$roles: S \rightarrow 2^R \cup 2^{AR}$ – помощью данной функции происходит определение ролей для юзера в определенной сессии в облаке. Стоит отметить в любой временной интервал для каждого $s \in S$ выполняется следующее условие $roles(s) \subseteq UA(user(s)) \cup UA(user(s))$.

$can - assign \subseteq ARxCRx2^R$ - модель отношения, с помощью которого происходит контроль ролей.

Отношение $can - assign\ (x, y, \{a, b, c\})$ можно интерпретировать следующим образом: обладатель роли администратора x или обладатель более старшей роли, имеет право назначать пользователей, если, в настоящий момент, их роль соответствует необходимым требованиям, а также является членом постоянных ролей a, b или c.

Для реализации модели ролевого доступа в облаке, следует определить уровни безопасности информации и установить множество объектов доступа для определенных систем облачных вычислений. Также необходимо реализовать множество субъектов доступа, которые возможны. Для объектов системы облачных вычислений определены такие уровни защиты:

- Информация открытая (ИО)
- Информация закрытая (ИЗ)
- Строго конфиденциальная информация (СКИ)

В таблице 3.1 представлен результат исследований, в рамках которых продемонстрированы множество доступов объектов информации для облаков.

Таблица 3.1 – Объекты, к которым необходим доступ в облаке

Обозначение	Наименование	Уровень защиты
1	Веб-сайт поставщика облачных сервисов.	ИО
2	Личные логины\пароли работников клиента облачных сервисов	ИЗ
3	Образы ВМ потребителя облачных сервисов	СКИ
4	Информационные ресурсы, которые имеются в облачном хранилище	СКИ
5	Файлы системы облачных вычислений, которые относятся к конфигурированию собственных ВМ конкретным потребителем облачных сервисов.	СКИ
6	1. Файлы системы облачных вычислений, которые имеют отношение к управлению пространством внутри облака поставщика. 2. Файлы системы облачных вычислений, которые имеют отношении к сервисам безопасности поставщика.	СКИ
7	Различные данные в облаке. Например: объем хранилища данных, текущее время сервера и так далее.	ИЗ
8	Информация, хранимая в общем пуле облачного сервиса, о фактическом распределении доступа.	СКИ
9	Объем услуг, который в свою очередь был оказан потребителю.	ИЗ
10	Данные по проекту, которые были активизированы в физической операционной среде (в кластере облачного поставщика).	СКИ
11	Информационные ресурсы по проекту, которые находятся на стороне потребителя облачных сервисов	ИЗ

В таблице 3.2 ниже представлены субъекты доступа (роли), которые были реализованы в результате исследований.

Таблица 3.2 - Субъекты, к которым необходим доступ в облаке

Обозначение	Наименование	Уровень защиты
L1	Директор по тех. вопросам у поставщика облачных сервисов.	СКИ
$LT1-3$	Работники тех. поддержки у поставщика облачных сервисов: 1. Работник L1 2. Работник L2 3. Работник L3	ИЗ
S1	Начальник службы автоматизации ИС облачных технологий.	СКИ
S2	Ответственный специалист по ИС облачных технологий.	СКИ
S3	Администратор инфраструктуры ИС облачных технологий.	ИЗ
S4	Ведущий специалист в области виртуализации в облачных вычислениях.	ИЗ
InfoSec 1	Управляющий службы безопасности поставщика облачных сервисов.	СКИ
InfoSec2	Эксперт по защите ПО и платформ услуги SaaS, на стороне поставщика	ИЗ
InfoSec 3	Эксперт по защите виртуальной инфраструктуры облака услуги SaaS, на стороне поставщика	ИЗ
InfoSec 4	Эксперт по защите кластера физических серверов поставщика.	ИЗ
$A1$	Руководитель службы ИБ и автоматизации потребителя.	СКИ
$A2$	Администратор ИБ потребителя облачных сервисов.	СКИ
$A3$	Специалист, который отвечает за интеграцию и сопровождение SaaS ИС облачных вычислений.	СКИ
$A4$	Администратор штатных средств защиты потребителя.	ИЗ
$P1$	Директор по тех. вопросам облачных сервисов на стороне клиента	СКИ
$P2_i$	Руководящие лица, эксплуатирующие облако в соответствии с БП, на стороне клиента.	СКИ
$P3_i$	Работники на стороне клиента, эксплуатируют облако в соответствии с БП предприятия на определенном проекте, например проект А.	ИЗ

Продолжение таблицы 3.2 - Субъекты, к которым необходим доступ в облаке

$P4_i$	Работники на стороне клиента, эксплуатируют облако в соответствии с БП предприятия на определенном проекте, например, проект Б.	ИЗ
$P5_i$	Работники на стороне клиента, принимающие участие в работе на проектах А и Б, но без прав на использование облака в соответствии с БП предприятия.	ИО
$P6_i$	Работники на стороне клиента, не принимающие участие в работе на проектах А и Б , и без прав на использование облака в соответствии с БП предприятия.	ИО

Так как в облаке происходит совместная работа между клиентом и поставщиком, предлагается сделать внедрение не единственной максимальной роли, а использовать две такие роли, как для поставщика ($L1$), так и для потребителя облачных сервисов ($P1$).

Иерархия ролей для юзеров имеет несколько уровней, пример представлен ниже на рисунке 3.1. Также на этом рисунке продемонстрировано, что потребитель имеет 2 отдела, которые производят эксплуатацию системы облачных вычислений, отвечая всем БП. Каждый специалист облачных сервисов, не имеющий прав на использование системы облачных вычислений - обладает минимальной ролью ($P5_i, P6_i$). Максимальной ролью обладают начальники отделов и руководители отделов, у которых есть все доступы и права на использование системы облачных вычислений ($P2_i$). Важное уточнение, 2 отдела потребителя облачных сервисов, имеют возможность на одновременное исполнение работы в системе облачных вычислений над разными проектами в соответствие с БП, у которых в свою очередь, отсутствуют единые или пересекающиеся средства и активы. Исходя из вышеперечисленного можно сделать вывод, что у работников разных отделов нет доступа к одним и тем же информационным средствам и активам системы облачных вычислений.

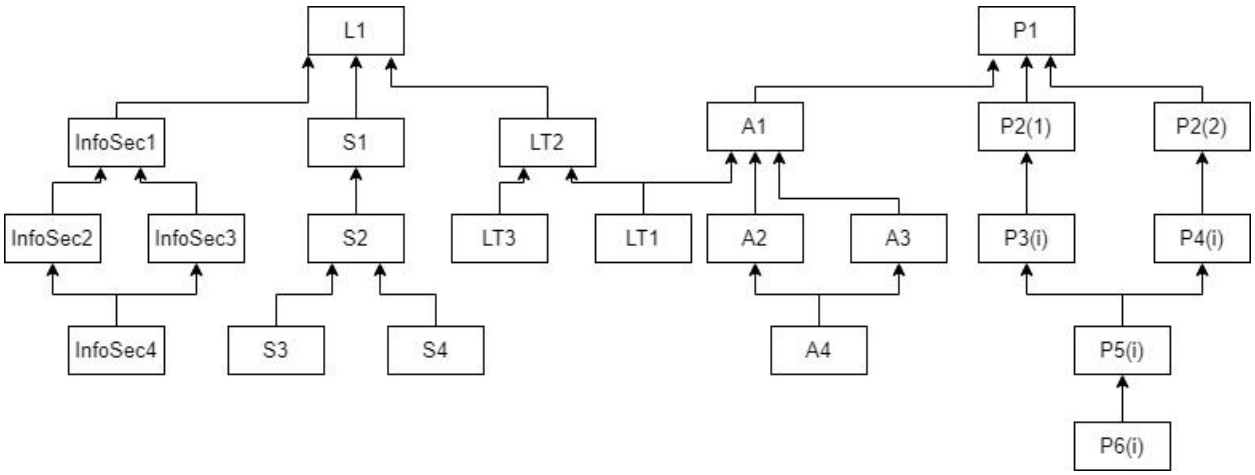


Рисунок 3.1 - Пример иерархии ролей

Кроме 2х отделов, которые выполняют работу на своих проектах в иерархии, существует еще один отдел, который несет ответственность за ИБ на предприятии. Вся ответственность за данный отдел лежит на руководителе службы ИБ и автоматизации потребителя ($A1$), также он владеет максимальной ролью. Минимальная роль приходится на администратора штатных средств защиты потребителя ($A4$), данный специалист выполняет работу по принятию мер защиты для систем безопасности, которые не находятся в облаке.

Одну из важнейших ролей на стороне поставщика облачных сервисов занимает - директор по тех. вопросам у поставщика облачных сервисов ($L1$), в его обязанности входит контроль над тремя отделами тех. поддержки у поставщика облачных сервисов ($\mathrm{LT1}-3$). Данные отделы на прямую контактируют с клиентами, которые используют облачные сервисы и при помощи этих отделов происходит решение вопросов, которые возникают у потребителей. Во время исследований было выявлено 3 отдела тех. поддержки облачных сервисов:

- Работник $L1$ - данный специалист анализирует и ликвидирует сбои, которые мешают или блокируют работу клиентам облачных сервисов. не имеет высокого доступа к системе облачных вычислений.
- Работник $L2$ - данный специалист является работником профиля уже чем, работник $L1$, имеет больше доступа к системе облачных вычислений.

Также обладает знаниями для решений вопросов, связанных с сервисами облака.

- Работник $L3$ - специалист по разработке облака.

Отдел автоматизации облачных вычислений занимается разработкой и внедрением решений облачных вычислений в SaaS на стороне потребителя услуг. Работники данного отдела специализируются на оптимальном управление облачными сервисами в контексте сетевых ограничений, которые имеются у потребителя облачных сервисов. Одна из важных ролей находится у начальника отдела автоматизации ИС облачных технологий. ($S1$), в то время как самыми минимальными ролями владеют: Администратор инфраструктуры ИС облачных технологий (S3), ведущий специалист в области виртуализации в облачных вычислениях(S4).

Существуют 3 роли для защиты облака (InfoSec $2-4$). Одна из важнейших и ответственных ролей, которая контролирует роли (InfoSec 2, InfoSec 3, InfoSec 4) - Руководитель службы ИБ у облачного поставщика (InfoSec 1). Также, стоит отметить, что роль InfoSec4 – обладает наименьшими правами при защите облака.

Роли пользователей в системе облачных вычислений определяется на множестве R отношение частичного порядка «≤», далее выполняется следующее условие: для $u \in U$, если $r_i, r_j \in R, r_j \in UA(u)$ и $r_i \leq r_j$, то $r_i \in UA(u)$. Но для $r_i \leq r_j$ должно выполняться хотя бы одно условие из 2х:

1. $r_i = x_i\_read,\ r_j = x_j\_read, x_i \leq x_j$;
2. $r_i = x_i\_write,\ r_j = x_j\_write, x_j \leq x_i$.

Для ролей пользователей в системе облачных вычислений имеется ряд следующий ограничений:

- ограничение UA функции - для любого клиента $u \in U$ роль $x\_read = \bigoplus (UA(u) \cap \{y\_read | y \in L\}\ UA(u)$ (здесь $x = c(u)$)и $x\_write = \bigoplus \{y\_write | y \in L\} \in UA(u)$(здесь $x = \bigoplus L$).

- ограничение $roles$ функции - для любой сессии $S \in s$ множество ролей roles(s) $=$ {x_read, x_write}.
- ограничения функции PA:
    - для всех $x \in L$ доступ $(o, read) \in PA(x\_read)$, только тогда, когда доступ $(o, write) \in PA(x\_write)$.
    - для всех доступов $(o, read)$ имеется только одна единственная роль x_read: $(o, read) \in PA(x\_read)$ (здесь $x = c(o)$).

Стоит отметить, что поставщик не должен иметь доступ к информации и устройствам, которую обрабатывает клиент облачных сервисов, это является основным параметром. Примером информации и устройств являются: ВМ, информационные ресурсы и так далее. Также специалисты поставщика, которые обладают правами администратора ИБ в облаке, должны уметь самостоятельно настраивать ВМ и файлы, которые будут незаметны для других специалистов поставщика и будут относится только к определенному клиенту. Для обеспечения защиты конфиденциальных данных каждого определенного клиента, поставщик может настраивать и управлять пространством в облаке. Это позволяет защищать данные не только от злоумышленников, но и от остальных клиентов, использующих облако.

Чтобы вносить корректировки в настройки файлов, образы ВМ, предлагается применять роли администратора и менеджера ИС на стороне клиента облачных услуг. К ролям, которые имеют права и доступ ресурсам проектор своего предприятия, можно отнести такие роли на стороне клиента: тех. директор и руководитель службы ИБ.

К ресурсам, которые хранятся в облачном хранилище у клиента, имеется доступ и права у начальника отдела и специалистам, работающим на стороне потребителя и тех.директору клиента облачных сервисов. Данные специалисты производят использование системы облачных вычислений на своих проектах согласно БП предприятия. Также данные специалисты имеют права и доступ к

файлам, которые относятся к конфигурированию своих ВМ и определенным потребителям облачных сервисов.

Правами на чтение логинов\паролей юзера, обладают специалисты по защите ПО и платформ клиента. Но правами на внесение изменений в логины\пароли от личных кабинетов на стороне клиента имеют в своем распоряжении только начальники отделов автоматизации и безопасности и тех. директор. Каждый юзер имеет права на чтение сайта поставщика облачных сервисов. Для работников на стороне поставщика тоже есть доступ на чтение сайта, но данный доступ дан только некоторым сотрудникам, а именно: ведущему специалисту в области виртуализации, специалисту по защите облака, специалистам L1 и L3 тех.подержки, админу ИС облачных технологий, работнику по защите ПО, руководителю ИБ. Внести изменения на сайт могут тоже ограниченное число специалистов, например, такие как: работники L2, тех. директор поставщика облачных услуг, ведущий специалист ИС облачных технологий. Начальникам отделов потребителей, специалистам L1 и тех. директору доступна информация об объеме услуг, которые предоставляет поставщик, но они имеют доступ только к прочтению. Но права на изменение данной инфомации есть только у L2, начальник службы автоматизации и тех. директор поставщика.

К информации о различных данных в облаке (серверное время, скорости обработки данных, объем хранилища данных и так далее) имеется доступ к прочтению у начальников отделов, администраторам ИБ потребителя и специалистам защиты облака, ведущему специалисту по виртуализации со стороны поставщика. Права на внесение изменений есть у менеджера ИС системы облачных технологий, начальника ИБ потребителя облачных сервисов, тех. директор потребителя и работник L1 и L2, тех. директор поставщика и начальник автоматизации облака.

Информацию о фактическом распределении доступа в едином пуле облака могут читать специалисты со стороны поставщика, такие как работник в сфере защиты инфраструктуры облака, руководитель безопасности, ведущий

специалист по виртуализации. Изменять и читать данную информацию могут: начальник и работник в отделе автоматизации, работники L1 и L2 тех.поддержки и начальник отдела автоматизации у потребителя.

Файлы, которые отвечают за конфигурацию внутри облака и ресурсы, которые используются для защиты поставщика, необходимо скрывать от всех специалистов, работающих у потребителя облачных сервисов. Данные фалы доступны для чтения специалистам: защиты ПО, начальник отдела безопасности. Для изменения доступны: L2, специалист по защите ПО и начальник отдела безопасности.

Опираясь на все изложенные выше условия, была разработана матрица с доступом ролей в системе облачных вычислений. Данная матрица представлена на рисунке 3.2 в виде таблицы, где r-read (доступ чтение), w-write (доступ на внесение изменений)

Субъекты, к которым необходим доступ в облаке	Объекты, к которым необходим доступ в облаке											
	1	2	3	4	5	6(1)	6(2)	7	8	9	10	11
L1	rw	w				rw	rw	rw	rw			
LT1	rw	w				rw		rw	rw			
LT2	r							rw	rw			
LT3	r					w						
S1	rw					rw		rw	rw			
S2	rw					rw		r	rw			
S3	r					rw		r				
S4	r					r		r	r			
InfoSec 1	r	w				r	wr	r	r			
InfoSec 2	r	w					rw					
InfoSec 3	r						rw	r	r			
InfoSec 4	r						rw					
A1	r	rw	rw	rw	rw			rw	rw		rw	rw
A2	r	rw			rw			rw	rw		rw	rw
A3	r	rw						r			w	w
A4	r	rw						r			w	w
P1	r	rw	rw	rw	rw			rw		r	rw	rw
P2(i)	r	rw	r	rw				r			rw	rw
P3(i)	r	r	r	rw							rw	rw
P4(i)	r	rw										
P5(i)	r											

Рисунок 3.2 - Матрица ограничений доступа

Результаты матрицы ограничений доступа, которые были получены во время разработки политики безопасности в облаке, могут применяться во время настройки контроля доступами и распределения обязанностей у пользователей. Каждая учетная запись пользователя в системе облачных вычислений связана с

индивидуальным IPадресом. В момент, когда происходит запуск ВМ, всем IPадресам даются определенные атрибуты, при помощи которых можно понять, какие из записей могут запускать определенную ВМ. Ниже в таблице 3.3 показано реализованное множество административных ролей в системе облачных вычислений.

Таблица 3.3 - Множество административных ролей в системе облачных вычислений

Обозначение	Наименование
v_aRole1	Модератор сервера в облаке
v_aRole2	Специалист ИБ на сервере в облаке
v_aRole3	Модератор системы облачных технологий
v_aRole4	Специалист по автоматизации облака
v_aRole5	Специалист по тех. поддержки облака
c_aRole1	Модератор облачного клиента
c_aRole2	Специалист ИБ облачного клиента
c_aRole3	Специалист по файлам конфигурации проекта А
c_aRole4	Специалист по файлам конфигурации проекта Б

В ходе исследования были выявлены следующие результаты: реализация административных ролей, в которых объединены роли потребителя и поставщика - невозможно. По причине того, что при создании объединенных ролей, появляются пользователи, которые имеют доступ к потоку данных потребителя. Исходя из этого в данной работе были реализованы 2 иерархии на административные роли, пример представлен на рисунке 3.3.

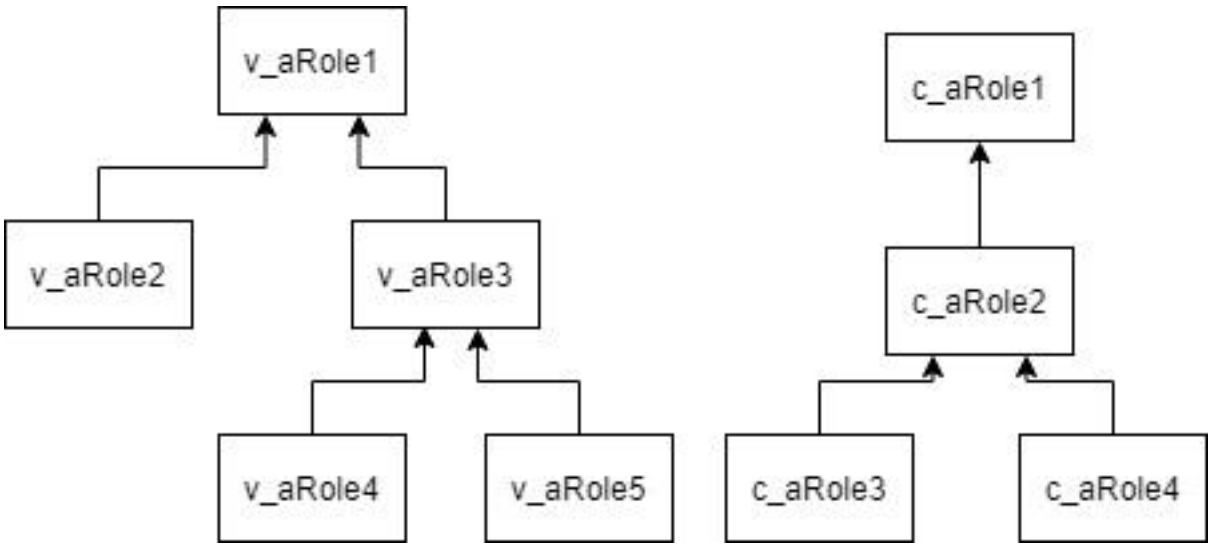


Рисунок 3.3 - Иерархия ролей для администраторов

Ниже описаны заданные функции для управления множествами пользователей, которые находятся в системе:

- Функция $can - assign(): AR \rightarrow CR \times 2R$ – выполняет определение других ролей юзеров, которые идентифицировались и вошли в систему, используя роль администратора. Данные роли представлены ниже в таблице 3.4.

Таблица 3.4 - Роли пользователей идентифицировавшихся в системе

Обозначение	Предварительное условие	Роли функции
v_aRole1	$InfoSec, S$	$L1$
v_aRole2	$InfoSec\ and\ (not\ S1)\ and\ (not\ LT(L2))$ $InfoSec$	$InfoSec1$ $InfoSec2, InfoSec3,$ $InfoSec4$
v_aRole3	$S\ and\ (not\ LT(L2))$ $LT\ and\ not\ (S1)$	$S1$ $LT(L2)$
v_aRole4	S	$S2, S3, S4$
v_aRole5	LT	$LT(L3), LT(L1)$
c_aRole1	$A\ and\ (not\ P2_i)$ $P6_i$	$A1$ P

Продолжение таблицы 3.4 - Роли пользователей идентифицировавшихся в системе

c_aRole2	A $P6_i\ and\ (not\ (A1\ or\ P2_i))$ $P6_i\ and\ (not\ \ (A1\ or\ P2_i))$	$A2, A3, A4$ $P2_i$ $P2_i$
c_aRole3	$P5_i$	$P3_i, P5_i$
c_aRole4	$P5_i$	$P4_iP5_i$

- Функция $can-revoke(): AR \rightarrow 2R$ – выполняет поиск и ролей юзеров, которые можно исключить, используя роль администратора. Данные роли представлены ниже в таблице 3.5.

Таблица 3.5 - Роли пользователей вышедших из системы

Обозначение	Роли функции
v_aRole1	$L1$
v_aRole2	$[InfoSec1 \dots InfoSec4], L1$
v_aRole3	$S1, LT2, L1$
v_aRole4	$[S1..S4]$
v_aRole5	$LT(L3), LT(L1)$
c_aRole1	$[LT(L1) \dots LT(L3)]$
c_aRole2	$[A1 \dots A4], P2_i$
c_aRole3	$P3_i, P5_i$
c_aRole4	$P4_iP5_i$

Применяя мат. модель ролевого доступа, при разработке частной политики ИБ облака, исключается возможность появления юзера, у которого в роли будут все права, благодаря которым он будет влиять на файлы настроек и потоки данных. В данной работе предложено ввести 2 роли, у которых будет иметься самое большое число прав. Это роль тех. директоров для обоих сторон в системе облачных вычислений, это позволит отвечать бизнес-процессам

облаков. Если данные требования будут соблюдены, то это даст возможность увеличить доверие новых потребителей ИС облачных технологий.

3.2 Применение нечетких когнитивных карт при реализации модели угроз в облаке, с учетом инфраструктуры объекта защиты

Для того чтобы исследовать модель угроз в системе облачных вычислений, была построена модель в основе которых лежат нечеткие когнитивные карты. Нечёткие когнитивные карты - нечёткий ориентированный граф, узлы которого являются нечёткими множествами. Термин "нечеткие" имеет значение, что причинные связи имеют значение действительных чисел. Данный метод позволяет перевести ситуацию, в которой имеются проблемы, в математический язык. Стоит отметить, что такая модель является простой для понимания. [23, 26]

Ниже на рисунке 3.3 изображена модель угроз в системе облачных вычислений в виде НКК, где показаны все уязвимости компонентов в облаке, также продемонстрировано распространение атаки.

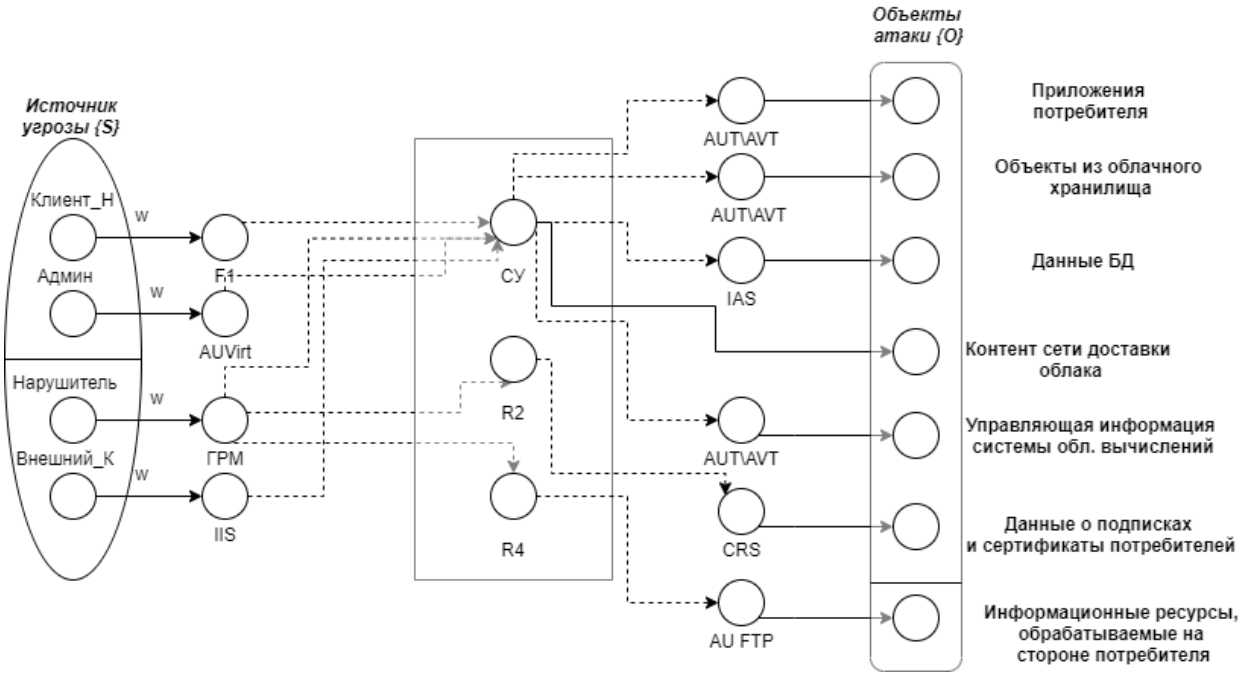


Рисунок 3.3 – Модель угроз в облаке

На данном рисунке имеется ряд следующих обозначений:

- Клиет_Н- субъект доступа: сотрудник, нарушающий установленные компанией потребителя услуг облачных вычислений распределение доступа по ролям;
- Админ – субъект доступа: сотрудник, выступающий от поставщика услуг облачных вычислений;
- Внешний_К – субъект доступа: субъект, не являющийся сотрудником компании потребителя или компании поставщика, однако пользующийся услугами облачных вычислений компании потребителя;
- Нарушитель – субъект доступа: субъект, являющийся нарушителем, не пользующийся услугами облачных вычислений компании потребителя;
- w − уровни уязвимости каждого из компонентов инфраструктуры системы облачных вычислений;
- R – маршрутизатор; IIS – пограничный сервер;
- AUVirt, AUT, AVT, IAS – серверы аутентификации облака;
- FTP – файловый сервер;
- СУ – управляющий сервер.
- Оценки каждого из уровней уязвимостей были взяты путем использования метода CVSS, а также международной БД уязвимостей (NVD) [79].

Для того чтобы создать такую модель необходимо владеть информацией о незащищенных местах в сети, которые имеются в системе облачных технологий. Из БД National Vulnerability Database [79] была взята информация о незащищенности компонентов в инфраструктуре облака. Далее определив незащищенные данные, источники и объекты атак, слудует выявлять пути реализации угроз.

НКК дает возможность увидеть угрозы, которые может нанести нарушитель, проанализировать данную информацию, то есть показать, какой объект - цель атаки, место, откуда может появиться угроза и т.д. Также при

построении модели угроз с помощью НКК, можно учесть структуру потребителя\поставщика, и незащищенность пограничных серверов, хранилища данных в облаке.

3.3 Реализация схем и методов для проведения проверок ИБ в облаке.

Система, в которой взаимодействует поставщик и клиент облачных сервисов — это система облачных вычислений. Как было описано ранее в такой системе происходят проблемы связанные с угрозами ИБ.

Благодаря аудиту ИБ, который стал популярным на сегодняшний день можно изучить ИС не только в облачные, но и традиционные. Проверка ИБ состоит из 3х образующих элементов:

- Алгоритм действия при проведении проверок, который включает в себя средства, модели и различные методы проведения проверок.
- Заключение о проведение проверок (результат может быть качественный или количественный).
- Система обеспечения безопасности, являющееся эталоном с которой сравниваются результаты проверки информационной системы.

Пример таких составляющих приведен на рисунке 3.4:

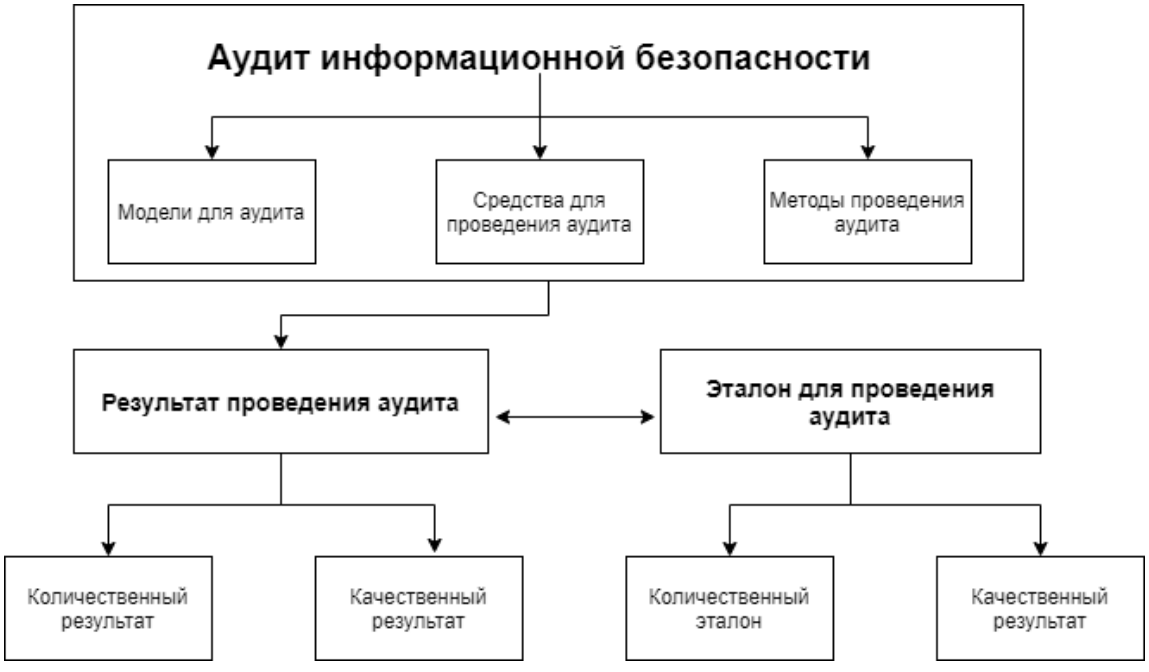


Рисунок 3.4 – пример составляющих аудита

Важно чтобы во время проведения аудита, исходные данные являлись целостными и достоверными, так как именно они влияют на качество проводимой проверки. В такие данные обычно входит техническая документация о ИБ, данные о ПО и средствах защиты.

Аудит информационной безопасности бывает инструментальный (активный) и экспертный:

- инструментальный (активный) - аудит, в котором происходят автоматические проверки ПО. Результатом является вывод рекомендаций по модернизации системы защиты. Недостатком является то, что зачастую данные рекомендации не полные, в связи с этим создать полную защиту информации невозможно.
- экспертный - аудит, в котором проверка опирается на соответствие стандартам, с целью исследования защиты системы. Огромным недостатком такой проверки является отсутствие стандартов, на основании которых аудитор должен проводить исследование системы.

Ранее было описано, что на данный момент в нашей стране нормативные документы и стандарты по защите информации в облаке - отсутствуют. В данной работе предложен вариант проведения проверок системы облачных вычислений при помощи искусственных нейронных сетей.

Искусственная нейронная сеть (ИНС) — информационная система, использующая ресурсы для самообучения, которая создает сеть ассоциативных понятий (нейронов) для распараллеленного поиска решений используя метод тренировки на данных обучающей выборки. Результатом тренировки будет являться математическая модель, функции которой зависимы между собой входными и выходными сигналами нейронной сети.

Искусственный нейрон – это элементарный элемент нейронной сети, имеющий некоторое неотрицательное число входов, на которые попадают сигналы (входные данные). Действия нейрона происходят в два шага: на первом, в нейрон от соседних нейронов поступает некоторое количество

сигналов, которые обрабатываются и передаются на выходной сигнал, переходя к следующему нейрону, на втором общее количество сигналов проходит через функцию преобразования, в результате которой будет создан итоговый выходной сигнал нейрона.

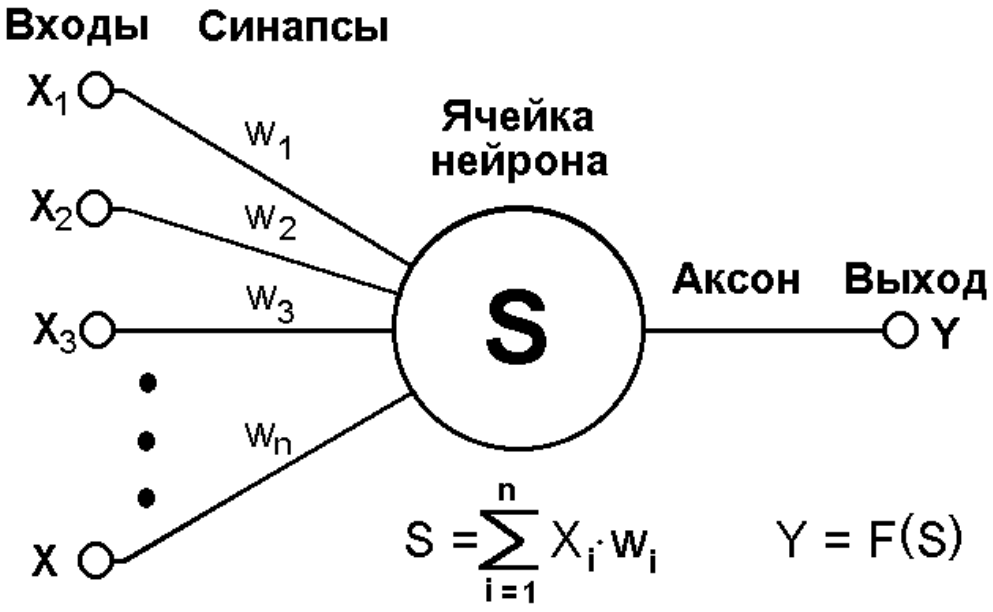


Рисунок 3.5 – схематичное представление нейрона

Синапс — это место соединения 2х нейронов, в котором происходит передача.

Аксон – это отросток нейрона, с которой выходной сигнал поступает на синапсы. Такой отросток может быть только один.

Главное преимущество нейронных сетей - поиск закономерностей в массивах данных. Также расширение диапазона задач с помощью нейронных сетей. Благодаря матричным преобразованиям процесс решения задач проходит точно и быстро, в сравнении с другими системами. В данной сети в отличии от в индуктивных и абдуктивных систем происходит имитация параллельного процесса прохода по нейронной сети. Для решения задач с помощью нейронных сетей можно создать программный модуль. В связи с этим в работе была нейронная сеть, как инструмент для реализации экспертного аудит информационной безопасности.

Чтобы оценить проблему нарушения безопасности информации в облаке, необходимо использовать 2 подхода для установления вероятности возникновения угроз:

- степень вероятности возникновения угроз нарушения информационной безопасности - оперативный подход
- оценка прогнозируемого значения - прогнозируемый подход

Стратегия безопасности, должна разрабатываться для системы облачных вычислений заранее, так как это связано с оценкой прогнозируемого значения. Далее происходит отслеживание системы безопасности, если была замечена атака в облаке, необходимо переходить к тактическим действиям.

Тактические действия - результат совместной работы отслеживания и управления безопасностью в сети.

Степень вероятности возникновения угроз нарушения ИБ помогает в определении мер, необходимых для применения в конкретный момент времени.

Итоговые данные, полученные после проведения процесса расчета значений вероятности возникновения угроз, следует использовать как множество данных для обучающей выборки нейронной сети. Это позволит проверяющему специалисту вычислить степени вероятности возникновения конкретной угрозы в реальном времени. Экспертная проверка включает себя:

- построение модели угроз в виде нечеткой когнитивной карты;
- вычисление прогнозируемых значений уровня вероятности возникновения угроз проверяемого нарушения информационной безопасности;
- создание обучающей выборки для тренировки нейронной сети путем формирования множества данных, а также настройка и тренировка ИНС;
- вычисление оперативного значения уровня вероятности возникновения угроз проверяющим сотрудником в реальном масштабе времени, используя полученную информацию с датчиков событий;

- создание отчета проверяющим сотрудником, используя полученные значения уровня вероятности возникновения угроз.

На рисунке 3.6 продемонстрирован метод проверки, используемый при получении оперативного значения уровня вероятности возникновения угроз нарушения ИБ.

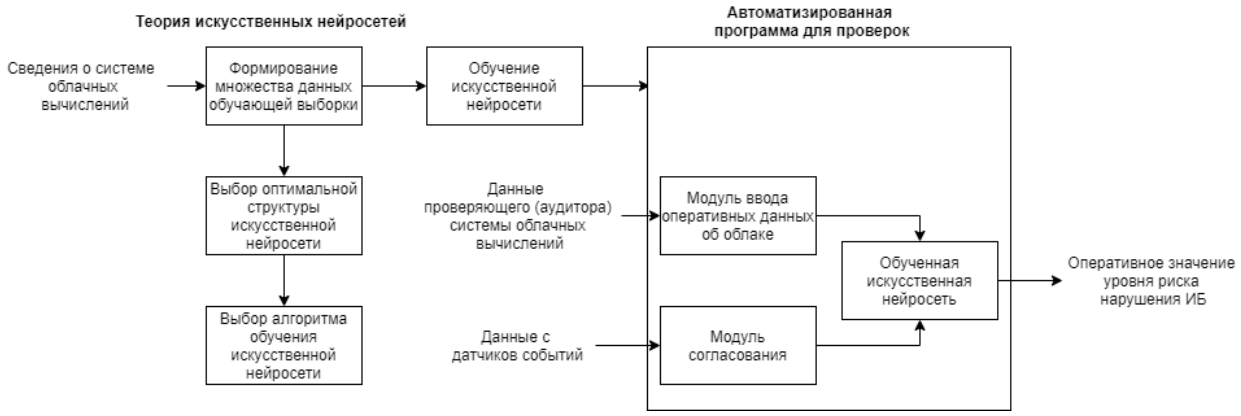


Рисунок 3.6 - метод проверки, используемый при получении оперативного значения уровня вероятности возникновения угроз нарушения ИБ

В следствии того, как нейронная сеть была обучена, это позволит определять степень вероятности возникновения угроз нарушения ИБ с учетом актуальных данных. Полученная информация с выхода модуля "оперативных данных о системе облачных вычислений" и с модуля, в котором согласуются данные попадают на вход в нейронную сеть. В модуле "согласование данных" выявляется источник угрозы на основе оперативных данных, например антивирусы, сенсоры системы вторжения и так далее. После этого на выходе из ПО аудитора реализуется результат расчетов вероятности возникновения угроз нарушения информационной безопасности в облаке. Данный результат поставщик может применять для обеспечения защиты конфиденциальной информации клиента. Оценка вероятности возникновения угроз нарушения информационной безопасности позволяет сделать верный вариант реагирования на различные ситуации, которые могут возникнуть в облаке. [14]

3.4 Анализ и решение проблемы, связанной сформированием обучающего множества

Формирование множества данных обучающей выборки - основная проблема нейронных сетей. Для того чтобы научить нейронную сеть необходимо создавать различные примеры для обучения и обширно раскрывать задачу, с которой связана нейронная сеть.

Для обеспечения характерности выборки при составлении множества данных для обучения, необходимо реализовать нужное число примеров для входных\выходных данных, которые демонстрируют закономерности и правила, которые в свою очередь будет должна определить нейронная сеть в ходе обучения. Подробный пример представлен на рисунке 3.7.

Рисунок 3.7 – Характерности обучающей выборки нейросети

Обучающая выборка должна выполнять 3 основных условия:

- Количество примеров должно быть оптимальным.
- Примеры, переданные в качестве обучающей выборки, должны быть в одинаковом количестве и с одинаковым шагом дискреции.
- Комбинации на вход и выход должны быть разнообразные в обучающих примерах.

Основываясь на алгебраическом подходе, реализованы условия достаточности множества данных обучающей выборки для обучения искусственной нейронной сети.

- В выборку должно попадать ограниченное количество примеров, которые показывают соответствие между X, Y пространствами, для обученного состояния W.

$$W = \{X(x_1 \dots x_n) \leftrightarrow Y(y_1 \dots y_m)$$

- Выборка должна быть оптимальной для обучения и представлена следующим образом, где D - пространство примеров для обучения, T - пространство тестовых наборов и K - контрольный пример, который не входит в множество для обучения.

$$W = \{D(X,Y), T(X,Y) | K(X,Y)\}$$

- Чтобы уменьшить количество итераций и упростить обучение, необходимо ввести примеры, которые будут подходить под следующее условие:

$$w = \{w \in W | (w_1 \dots w_n) \propto (w_1 \dots w_n) | y_{qw} = const\}$$

где: n - количество примеров обучающей выборки,

y_{qw}- шаг дискретизации обучающей выборки

- Пороговые значения должны включаться в выборку на практике, и также должны включаться промежуточные значения с необходимым шагом дискреции. [18] Комбинации на вход\выход необходимо задавать разнообразными для обучения:

$$W = \{w_1, w_n \big| (w_2 \dots w_n) \approx \left(w_2 \dots y_{qw}\right) \dots \left(w_{n-1} + y_{qw}\right) \big| N \gg 1\}$$

Для того чтобы провести обучение нейронной сети успешно, необходимо прибегнуть к применению множеству данных обучающей выборки, исходя из данных условий. В результате, для проведения проверок ИБ системы облачных вычислений при помощи нейросетей, следует сформировать обучающее множество, которое будет выполнять все требования, которые были

перечислены выше. Стоит обратить внимание, на то, что при построении обучающей выборки необходимо работать только с числовыми входными данными, что и применяется в данной работе для обучения.

После оценки вероятности возникновения угроз происходит вычисление угроз ИБ активам инфраструктуры вендора и пользователя услуг облачного вычисления, исходя из общей ценности обрабатываемой информации, а также оценки значимости угроз из различных источников по сегментам по следующей схеме:

- значения уровней угрозы на путях распространения от одного источника до одной цели атаки определяются, как произведение вероятности активации угрозы и величины уязвимости элементов инфраструктуры провайдера и потребителя. Облачные сервисы и барьеры, полученные путем стандартизации, перечислены в международной базе данных:

$$P_j = P_a * W_{z+1} * V_{z+1}$$

где W_{z+1} − значения уязвимостей компонентов облачной инфраструктуры поставщика услуг и барьеров на пути распространения атаки.

V_{z+1}− значения уязвимостей компонентов облачной инфраструктуры потребителя услуг и барьеров на пути распространения атаки.

P_a− вероятность возникновения и срабатывания угрозы.

- Выявление max значения степени угрозы от источника к объекту атаки:

$$P_s^u = \left(K_i \to K_y\right) = max_{j=1}^{J} P_j$$

где J – число путей от одного источника к одному объекту

- Подобные расчеты производятся для всех вероятных источников опасностей для абсолютно всех активов поставщика\потребителя.

- Для расчета результирующего значения уровня угрозы для информационных объектов системы облачных вычислений, применяется следующая формула:

$$P_{\sum}^{u} = 1 - \Pi_s(1 - P_s^u)$$

- Расчеты ведутся для поставщика\потребителя облачных сервисов.
- Значение степени вероятности возникновения угрозы информационной безопасности объектам системы облачных вычислений.

$$\overline{R_n} = \sum_{s=1}^{S} \left[{C_{пост} \atop C_{потр}} \right| C_{пост} + C_{потр} = 1$$

где S – число источников угроз;

$C_{пост}$ – ценность информационных активов поставщика;

$C_{потр}$ – ценность информационных активов потребителя.

- По следующей формуле можно рассчитать значение вероятности возникновения угроз информационной безопасности системы облачных вычислений:

$$\bar{R} = \sum_{n=1}^{N} \overline{R_n}$$

где N – число критичных объектов системы облачных вычислений.

Для худшего случая, когда все возможные источники угрозы активируются в одно время, данный метод позволяет оценить значение уровня вероятности возникновения угроз нарушения информационной безопасности. В таблице 3.7 представлен пример расчета ожидаемого значения вероятности возникновения угроз нарушения ИБ.

Таблица 3.7 - Пример расчета ожидаемого значения риска нарушения ИБ

Сегмент	Ценность	$P_{зл}$	$P_{др\_кл}$	$P_{пост}$	$P_{потр}$	*threat*	$prob$
С1	0,5	0,064	0,064	0	0,136	0,244	0,122
С2	0,4	0,003	0,164	0,219	0,14	0,3572	0,143
С3	0,1	0,003	0,164	0,219	0,14	0,3572	0,036
							0,3

Значения вероятностей угроз, которые представлены в таблице выше:

$P_{зл}$ − Нарушитель (злоумышленник)

$P_{др\_кл}$ − Другой клиент облачных услуг

$P_{пост}$ − Работник на стороне поставщика

$P_{потр}$ − Работник на стороне клиента(потребителя)

threat − Уровень угрозы полученный в результате эксперимента

$prob$− Уровень вероятности возникновения угроз

Основываясь на результатах, которые были проведены в ходе эксперимента можно сделать вывод, что метод расчета прогнозируемых вероятности возникновения угроз для системы облачных вычислений, может применяться в дальнейшем.

Также в ходе эксперимента было выявлено, что множество данных обучающей выборки вырабатывает нечувствительность к вариациям входных величин у выходных сигналов, если выполняется следующие условие - вариации находятся в допустимых границах [0,1]. И выходы нейросети не зависят от шага дискретизации, который будет применяться для натренированной нейронной сети.

Решив проблему формирования обучающей выборки искусственной нейросети, появляется новый вопрос о выборе оптимальной архитектуре нейронов. Подбор количества нейронов во входном слое обусловлен размерностью входного векторного пространства признаков X. Число выходов зависит от размерности выходного векторного пространства признаков Y. Входное и выходные пространства задаются во время создания обучающей выборки. В данной работе, для проверки ИБ количество входов в сеть задано 7, а количество выходов задано 1.

Таким образом, во время процесса применения нейросетей, появляется задача о поиске закономерностей в массиве данных. Для этого были исследованы некоторые архитектуры нейросетей, которые можно считать

оптимальными для решения данной задачи. Примерами являются: Сеть Хопфилда, Самоорганизующаяся карта Кохонена, Персептрон.

Проведя сравнительный анализ архитектуры нейросетей, выбор был сделан в пользу персептрона, который может быть однослойным или многослойным.

- Однослойный персептрон – в данной сети, у нейронов есть четко-обговоренная активация.
- Многослойный персептрон – нейросеть не имеющая обратных связей, то есть проходя через несколько слоев, сигнал из входного преобразуется в выходной. Пример сети, у которой n входов продемонстрирован на рисунке 3.8. На эти входы поступают сигналы, которые переходят по синапсам на другие три нейрона, образующие первый слой. Далее эти сигналы уходят к другому слою и так далее, пока последние нейроны не выдадут выходные сигналы. [11]

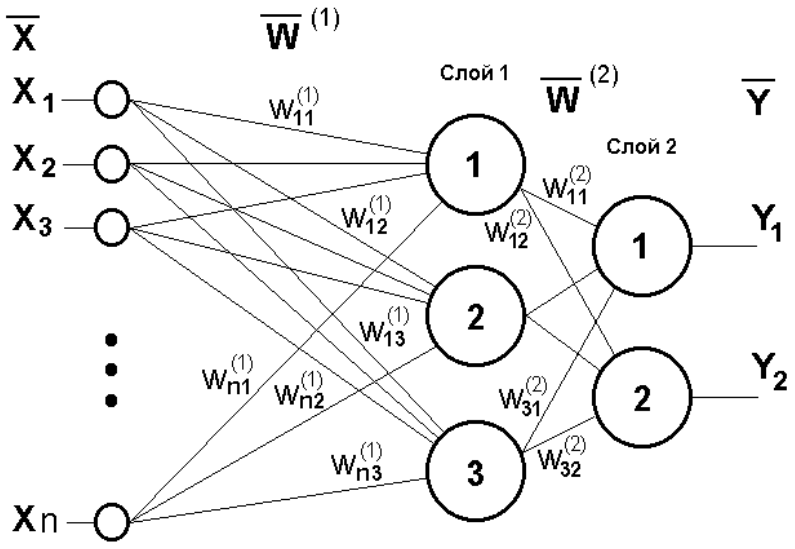


Рисунок 3.8 – Пример многослойного персептрона.

Персептрон имеет следующие преимущества, в отличии от других архитектур:

- Простой для понимания алгоритм обучения сети.

- Персептрон с лёгкостью решает задачи классификации.
- Персептрон обучается при помощи метода обратного распространения ошибки

Исходя из вышесказанного, в данной работе будет применен метод алгоритм обучения многослойных персептронов, основанный на вычислении градиента функции ошибок.

3.6 Выводы по третьей главе

1. Для того чтобы определить вероятности возникновения угроз нарушения ИБ, было предложно 2 подхода: расчет оперативного и прогнозируемого значения вероятности возникновения угрозы нарушения информационной безопасности в облаках.

2. Был предложен, для получения численной оценки оперативного значения уровня вероятности возникновения угрозы ИБ, метод проведения проверок информационной безопасности в облаке, данный метод включает в себя применение нейросети. Основываясь на расчетные значения прогнозируемого уровня нарушения, можно выполнить обучение данных обучающей выборки. Это поспособствует избежать опасных инцидентов или хотя бы адекватно реагировать на них, с целью обеспечения безопасности в облаке.

3. Для обучения нейросети при решении задачи проведения проверок ИБ системы облачных вычислений, были описаны условия достаточности множества данных обучающей выборки для обучения сети, учитывая все возможные требования.

Глава 4 Разработка и внедрение результатов исследования

В данной главе представлены блок-схема алгоритма программы, программа «Product validation», которая реализована с целью нахождения операционных значений вероятности возникновения угрозы ИБ в облаках, для анализа угроз.

Также для обучения нейросети был проанализирован и применен алгоритм обратного распространения ошибки.

В следствии анализа вопроса о возникновении источника угроз, был сделан вывод, что самым опасным источниками для безопасности ИС облачных вычислений, являются внутренние нарушения

4.1 Реализация проверок ИБ системы облачных вычислений при помощи нейросети с применением модели IDEF0

Одним из сложных процессов является аудит в облаках. Данная проверка должна включать в себя разнообразные факторы, архитектуру и особенности систем облачных вычислений, а также не стоит забывать про частную политику безопасности. Детализация процесса аудита с помощью нейронной сети будет выполнена при помощи IDEF0 модели, это связано с тем, что представить описание метода в виде текста, будет сложно. Также модель IDEF0 позволит рассмотреть процесс, как набор действий, которые взаимосвязаны с детализацией.

Существует простая и легкая методология функционального моделирования - IDEF0. Данная методология при помощи графики позволяет наглядно описывать БП (бизнес-процессы). Моделирование IDEF0 наглядно демонстрирует, как потоки, например информационные, которые поступают на вход преобразуются в исходящие потоки. На рисунке 4.1 изображен пример контекстная диаграмма IDEF0−модели, при помощи которой должна быть реализована проверка информационной безопасности системы облачных вычислений. Также на этом же рисунке приведен пример БП проверки по методу «черного ящика».

Рисунок 4.1 - модель IDEF0 для проверки ИБ в облаке

Далее на рисунке 4.2, который расположен ниже, показана диаграмма в виде иерархий, где степень детализации процессов возрастает. Функциональный блок разбивается на три составляющие блока: «Рассчитывать вероятность возникновения угроз нарушения ИБ», «настройка и обучение нейросети», «Рассчитывать операционного значения уровня вероятности возникновения угроз ИБ».

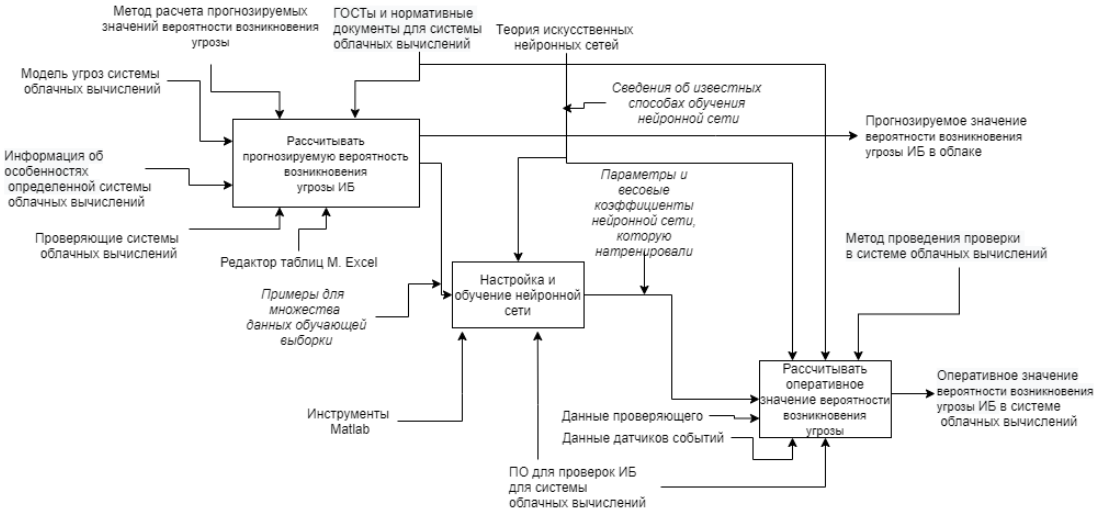


Рисунок 4.2 – диаграмма общего процесса

Первый составляющий блок «Рассчитать прогнозируемые вероятности возникновения угроз нарушения ИБ», представлен на рисунке ниже, также он разбит по предлагаемой методике.

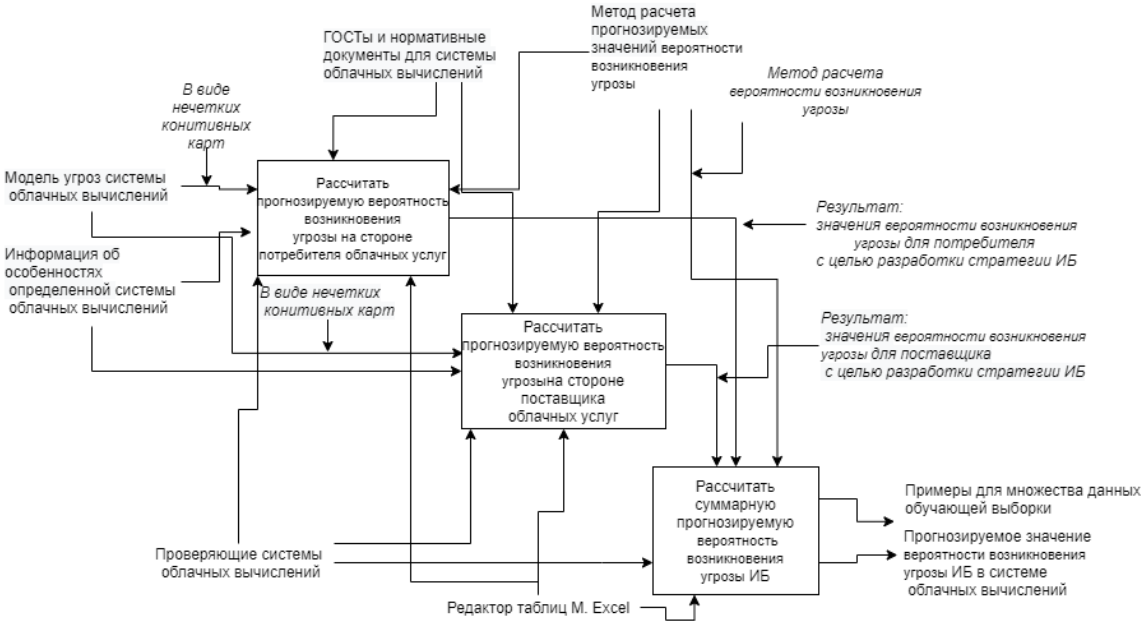


Рисунок 4.3 - Блок «Рассчитать прогнозируемые вероятности возникновения угроз повреждения ИБ»

На рисунке 4.4 продемонстрирован второй блок «Настройка и обучение нейронной сети».

Рисунок 4.4 - блок «Настройка и обучение нейронной сети»

На рисунке 4.5 представлен следующий заключительный блок «Расчет операционного значения уровня вероятности возникновения угроз ИБ» разбит еще на два дополнительных блока со следующим уровнем детализации.

Результатом этих блоков являются значения вероятности возникновения угроз безопасности для системы облачных вычислений в реальном времени.

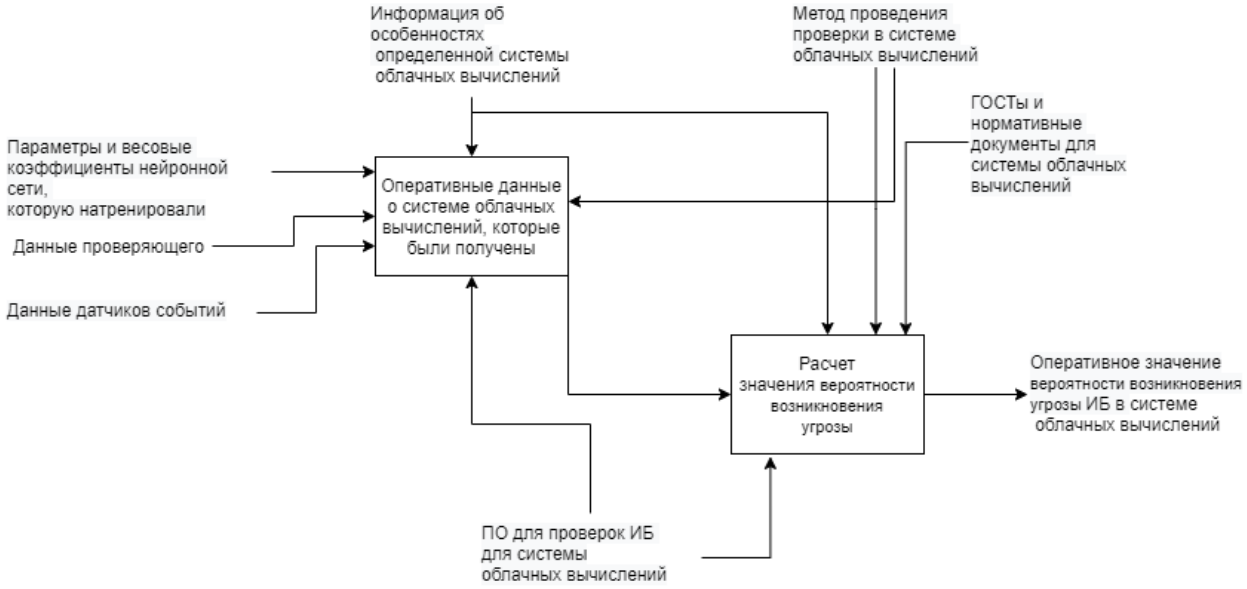


Рисунок 4.5 - блок «Расчет операционного значения уровня вероятности возникновения угроз ИБ»

Анализируя сложные процессы, таких как, например, при проверке ИС защиты информации, имеется возможность использовать модели IDEF0 для визуального отображения взаимосвязанной последовательности действий по разработанной методике с требуемым уровнем детализации, чтобы они могли эффективно использоваться рецензентом на практике.

4.2 Обучение искусственной нейронной сети. Поиск эффективности выбранного алгоритма обучения нейронной сети

Как было описано выше, в данной работе будет применен метод «обратного распространения ошибки», алгоритм обучения многослойных персептронов, основанный на вычислении градиента функции ошибок. В процессе обучения веса нейронов каждого слоя нейросети корректируются с учетом сигналов, поступивших с предыдущего слоя, и невязки каждого слоя, которая вычисляется рекурсивно в обратном направлении от последнего слоя к первому. [2]

Синаптические веса регулируются, чтобы довести выходной сигнал сети как можно ближе к нужному.

Синапс — это место соединения 2х нейронов, в котором происходит передача.

Аксон – это отросток нейрона, с которой выходной сигнал поступает на синапсы. Такой отросток может быть только один.

Вес – это характеристика каждой связи, по которой выходные сигналы поступают на входы других. Вес бывает 2х видов:

Возбуждающие -связи с положительным весом

Тормозящие – связи с отрицательным весом

$S = \sum_{i=1}^{n} x_i * w_i$ - формула определения взвешенной суммы входов нейрона, где

n – число входов нейрона;

x_i – значение i-го входа нейрона;

w_i– вес i-го синапса.

$Y = f(S)$- формула определения значения аксона нейрона,

где f –функция нейрона, которая отвечает за активацию.

В основном применяется сигмоид нейронной сети для функции, которая описана выше. Функция имеет вид:

$$f(x) = \frac{1}{1 + e^{-ax}}$$

Данная функция является дифференцируемой на всей оси абсцисс, также имеет простую производную:

$$f(x) = a * f(x)(1 - f(x))$$

Из некоторого количества слоев нейронов состоит – искусственная нейросеть, которая преобразована с помощь алгоритма обратного распространения ошибки. Здесь каждый нейрон в слое i имеет связь с каждым из них $(i + 1)$. [8]

Поиск функциональной зависимости $Y = F(X)$, где векторы – X – входные, Y – выходные. – является целью обучения искусственной нейросети.

Метод наименьших квадратов дает возможность уменьшить целевую функцию ошибки нейросетей, данное действие необходимо для сокращения пространства поиска при обучении

$$E(w) = \frac{1}{2}\sum_{j=1}^{p}(y_j - d_j),$$

где y_j – значение j-го выхода нейронной сети;

d_j – целевое значение j-го выхода;

p – число нейронов в выходном слое.

$\Delta w_{i,j} = -h\frac{\delta E}{\delta w_{i,j}}$ - формула для определения изменения веса на каждой итерации, где h – параметр для определения скорости обучения.

$$\frac{\delta E}{\delta w_{i,j}} = \frac{\delta E}{\delta y_j} * \frac{\delta y_j}{\delta S_j} * \frac{\delta S_j}{\delta w_{i,j}}$$

где y_j – значение выхода j-го нейрона; S_j –сумма входных сигналов(взвешенная).

$x_{i,j} = \frac{\delta S_j}{\delta w_{i,j}}$ - формула для нахождения множителя, где $x_i -$ значение i – го входа нейрона.

Определение первого множителя задается по формуле:

$$\frac{\delta E}{\delta y_j} = \sum_k \frac{\delta E}{\delta y_k} * \frac{\delta y_k}{\delta S_k} * \frac{\delta S_k}{\delta w_{i,j}} = \sum_k \frac{\delta E}{\delta y_k} * \frac{\delta y_k}{\delta S_k} * w_{jk}^{(n+1)}$$

где k – число нейронов в слое $n + 1$.

$v_j^{(n)} = \frac{\delta E}{\delta y_j} * \frac{\delta y_j}{\delta S_j}$ - введение вспомогательной переменной.

$v_j^{(n)} = \left[\sum_k v_k^{(n+1)} * w_{j,k}^{(n+1)}\right] * \frac{\delta y_j}{\delta S_j}$ - понятие рекурсивной формулы для определения n-ного слоя, если известно следующего $(n + 1)$-го слоя.

Целевой вектор – вектор значений, которой нейросети необходимо выдавать при определенном наборе входных значений. Поиск данного вектора заключается в том, что это позволит найти последний слой нейронной сети. [7]

$$v_j^{(n)} = (y_i^n - d_i) * \frac{\delta y_j}{\delta S_j}$$

$\Delta w_{i,j}^n = -h * v_j^{(n)} * x_i^n$ - формула в раскрытом виде

$\Delta w_{i,j}^{(n)} = w_{i,j}^{(n)}(t-1) + \Delta w_{i,j}^{(n)}(t)$ - формула для корректировки всех весов нейронной сети.

Ниже на рисунке 4.6 представлен пример обучения нейросети, применяя, метод обратного распространения ошибки:

Рисунок 4.6 – Алгоритм обучения нейросети

Для демонстрации эффективности метода обратного распространения ошибки для обучения нейросетей, было выполнено исследование в данной работе. Данное исследование проводилось при помощи ПО " Matlab". При обучение нейронной сети удалось минимизировать ошибки. На рисунке продемонстрировано обучение нейронной сети, которая проходила 10 эпох.

Также можно отметить, что среднеквадратичная ошибка составляла от $10^{-3} - 10^{-2}$, а при обучении 10^{-4} в метрической системе.

В следствии исследования появляется необходимость проведения контрольной работы нейронной сети, с целью проверки правильности обучения. Для такой проверки была использован инструмент для модельно-ориентированного проектирования.

В каждой нейросети существует слой с нейронами и значениями коэффициентов. На рисунке 4.7 показан такой слой, он называется внутренним.

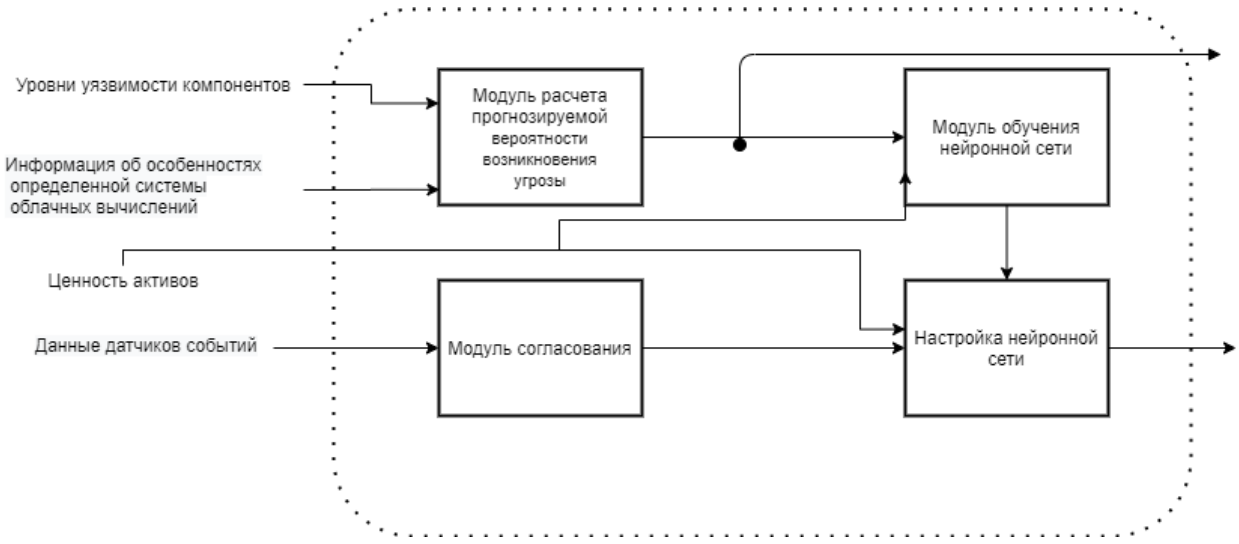


Рисунок 4.7 – Внутренний слой нейросети

Для того чтобы сделать оценку степени натренированности сети, и понять, каким образом она справится с новыми данными, которые еще не участвовали в эксперименте, должен быть проведен следующий эксперимент. В рамках данного эксперимента, будет проведен анализ действия системы, при угрозе от нескольких источников нарушения. [10]

Ниже в таблице 4.1 представлены значения, которые применялись в данном анализе.

Таблица 4.1 - значения, которые применялись в анализе действия системы, при угрозе от нескольких источников нарушения.

Объект, представляющий угрозу	Объект, цель атаки
Нарушитель (1)	ВМ и данные потребителя (0,1)
Другой клиент провайдера услуг облачных вычислений (0)	Объекты, хранящиеся в облаке (0,1)
Работник, поставщик услуг облачных вычислений (1)	Экземпляр базы SQL (0,3)
Работник, потребитель услуг облачных вычислений (1)	Информационные ресурсы, которые обрабатываются на стороне потребителя (0,5)

На рисунке 4.8 продемонстрирована работа ПО " Matlab", которая была сформирована при помощи задания второго входного вектора на входы персептрона.

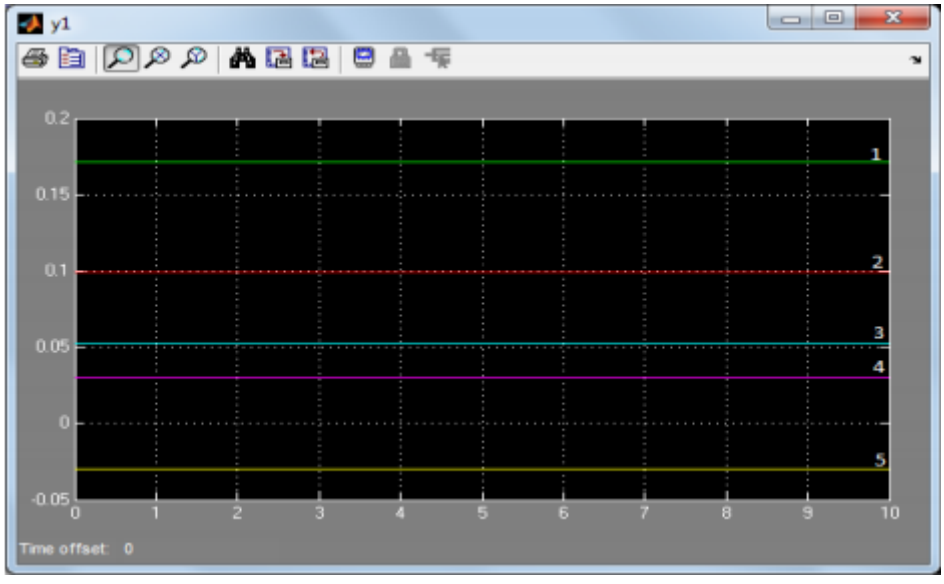


Рисунок 4.8 – Результат работы ПО “Matlab”

При моделировании нейросети был получен следующий результат, представленный в таблице 4.2. Здесь продемонстрированы выходные вектора.

Таблица 4.2 - Выходные вектора при моделировании нейросети

№ вектора на графе	Объект, представляющий угрозу (активный 0; неактивный 1)	Значение при расчете по формуле	Значение из нейронной сети	Δ Значений
1	Общий (1)	0,164	0,17	0,006
2	Нарушитель (1)	0,016	0,02	0,004
3	Работник, поставщик услуг облачных вычислений (1)	0,1097	0,1	0,0097

Продолжение таблицы 4.2 - Выходные вектора при моделировании нейросети

4	Работник, потребитель услуг облачных вычислений (1)	0,042	0,05	0,008
5	Иной клиент провайдера облачных услуг (0)	0	-0,025	0,025

Проведя ручной расчет и анализ таблицы, которая представлена выше. За эталонный расчет будет принят – ручной расчет. В результате сверки расчетов, можно сделать вывод. Что нейронная сеть достаточно обучена и разница отклонения равна не больше 0.03.

Вывод: обучив и выполнив тестирование нейросети, появилась возможность использования выбранной архитектуры и метода обучения нейросети, с целью реализации программы, для автоматизации проверок системы облачных вычислений.

4.3 Реализация блоксхемы и модели программы для проверок информационной безопасности в облаке.

Автоматизированный инструмент контроля ИБ дает возможность проверяющему увеличить скорость процедуры для принятия решения, для того чтобы появилась возможность подобрать определенную стратегию реагирования на нарушения. На рисунке 4.9 показана модель системы, которая была автоматизирована для экспертных проверок.

Рисунок 4.9 - модель системы, которая была автоматизирована для экспертных проверок.

XML-таблица, содержащая в себе данные об уровнях вероятности возникновения угроз, преобразуется в формат класса DATA. Вес файла составляет примерно 64 КБ. Такой файл необходим для создания данных, которые будут наполнять базу выборки для нейросети. Стоит отметить, что он позволяет сократить время на обучение нейросети, так как объем входных данных никак не влияет на обученность сети.

Юзеру, который применяет программу для проверки, необходимо внести в модуль расчета, данные, которыми он обладает о облаке, а также, данными о значениях уязвимости компонентов. Данные значения можно получить с помощью изучения стандартизации компонентов, которые соответствуют международной БД уязвимостей.

Описанный выше метод обратного распространения ошибки требуется при обучении нейросети. Выборка, модуля расчета вероятности возникновения угроз, грузит построчно данные для обучения сети. Процесс обучения подходит к концу, в момент получения нужного уровня среднеквадратичной ошибки. Далее можно переходить к проведению проверки ИБ системы.

Приступив к проведению проверки, необходимо иметь актуальную информацию с датчиков событий системы. Такое требование необходимо для

выполнения расчета значения вероятности возникновения угроз нарушения ИБ. Нейросеть, используя данные с датчиков событий, произведет вычисление значения нарушения ИБ в системе. Основываясь на этих расчетах, проверяющий делает заключение в виде отчета, где заполняет итоговое значение и метод оценки вероятности возникновения угроз, и выносит рекомендации для улучшения системы защиты.

В результате программа, которая будет разработана в данной работе, поможет не только проведение проверок в облаке, но и поможет проверяющему в написании рекомендаций о защите, и в проведение мероприятий по защите ИБ облачных вычислений.

Данная программа реализована при помощи языка программирования C#, с использованием готовых библиотек из свободного доступа. Данные библиотеки дают возможность применения нейросетей в ИС для увеличения возможностей ПО. Также стоит отметить, что, используя данные библиотеки, появляется возможность спроектировать нейросеть, которую просто обучить.

В библиотеки включены следующие модули:

Модуль check - главное окно ПО, также создает анимацию процесса обучения нейросети.

Модуль M_Neuron - процесс работы с весовыми коэффициентами нейросети.

Модуль M_NeuronB - реализация в программе многослойных нейросетей.

Модуль PrevIter – Значения коррекции весовых коэффициентов, которые хранятся на шаге, который был до этого.

Модуль M_NeuronLC - объединение всех нейронов сети в слои.

Модуль M_NeuralNetworkB - реализация нейронносети, которую в обучение которой был применен метод обратного распространения ошибки.

Модуль M_NeuralNetwork - построение нейросети. Здесь включены методы работы с сетевыми слоями и манипулирования исходными данными.

Модуль Create/Remove_Layer - манипуляции со слоями нейросети.

Модуль Create/Remove/Reset_Pattern - манипуляции с исходными данными обучающей выборки искусственной нейросети.

На рисунке 4.10 представлена диаграмма компонентов UML

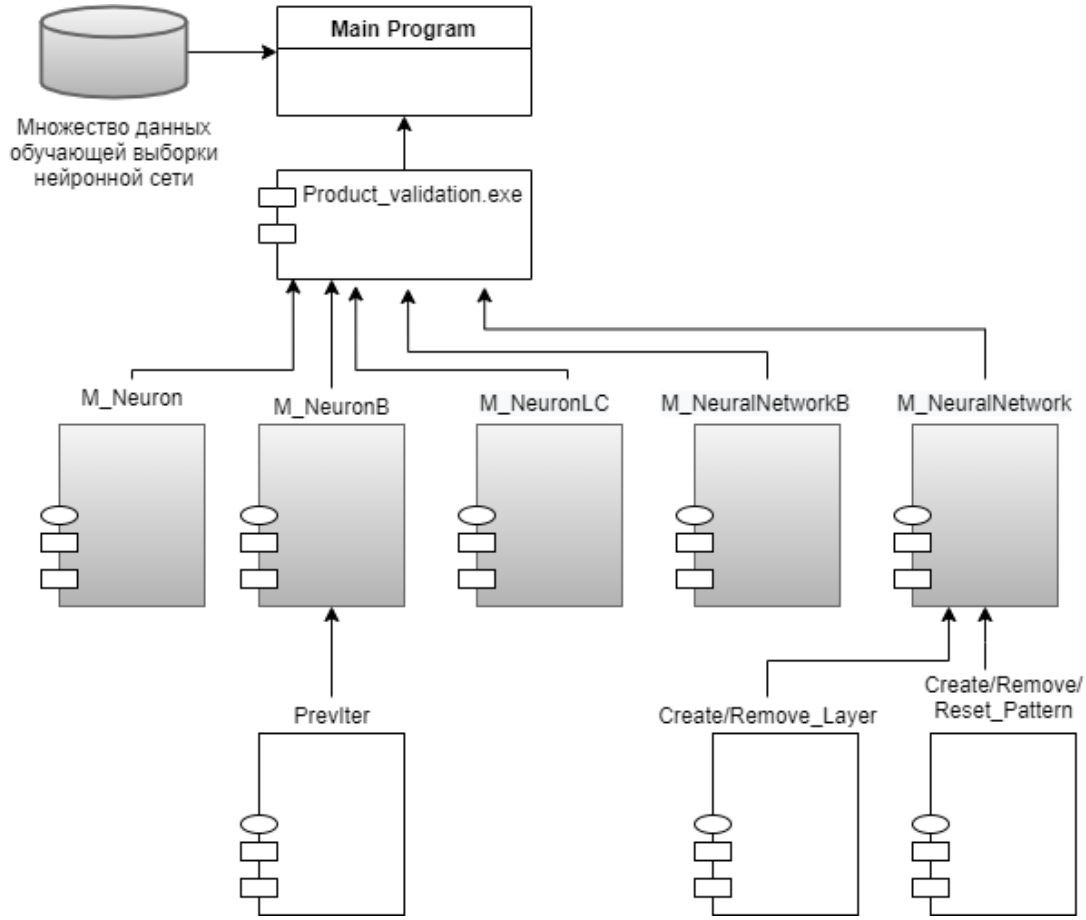


Рисунок 4.10 - Диаграмма компонентов UML

Данное ПО обладает простым и понятным интерфейсом. Для определения времени до окончания обучения, добавлено визуальное отображение процесса обучения. Для установления точности оценки вероятности возникновения угроз угрозы ИБ реализовано отображение среднеквадратичной ошибки.

Для того, чтобы производить контроль над точностью и корректностью данных, которые вводит пользователь, были добавлены следующие предупреждения об ошибках, в таких ситуациях:

– Сумма реквизитов при вводе исходных данных поставщика\клиента в программу, не должно быть равно 1

– ценность клиентских данных должна быть равна 0.

Данная программа обладает следующими плюсами: здесь можно применить модель, которая дает возможность анализа угроз, которые были выявлены, учитывая непростые сценарии атак. Например: активация несколько источников угроз.

4.4 Демонстрация работы с программой «Product validation»

При работе с программой пользователю доступна альтернатива выборки для загрузки с целью обучения нейросети. Варианты выбора: клиент\поставщик облачных услуг. Кнопка «Обучение нейронной сети» не будет доступна до тех пор, пока проверяющий не укажет тип выборки для загрузки в форму ввода исходных данных, которая уже заранее была сформирована на основе прогнозируемых значений вероятности возникновения угроз нарушения ИБ в облаке. И также заранее данные преобразована в формат DATA.

На рисунке 4.11 представлена ЭФ (экранная форма) выбора вида выборки.

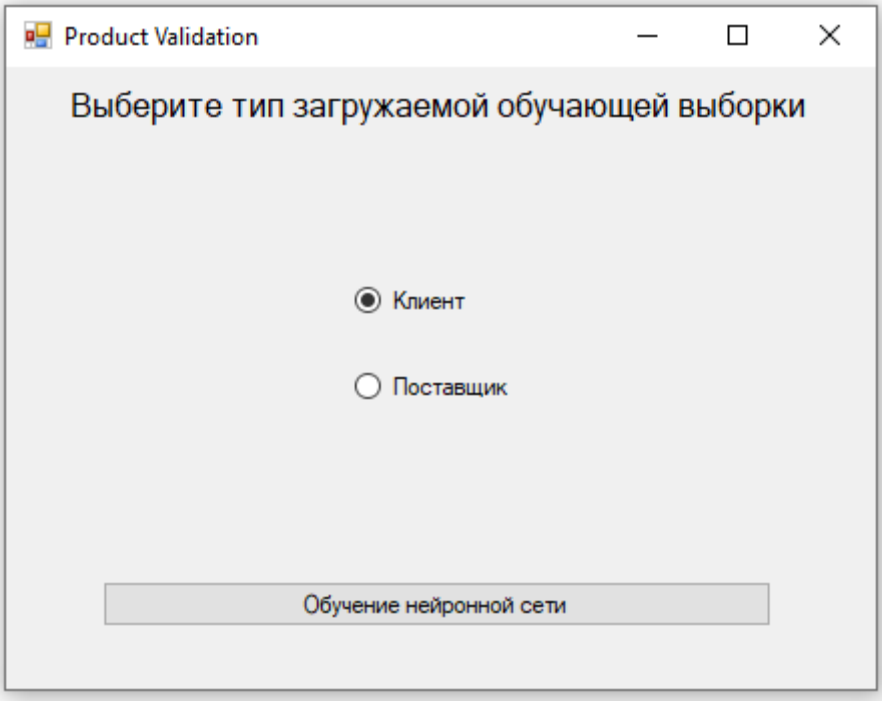


Рисунок 4.11 - ЭФ выбора вида выборки

Метод алгоритма обратного распространения ошибки принимает участие в следующем этапе – обучение нейросети. Данный этап наступает сразу после загрузки данных для выборки.

После того, как кнопка «Начало работы» появляется на экранной форме, заканчивается этап подготовки работы нейросетей, и пользователь программы может начать реализовывать процесс проверки системы облачных вычислений. Также на ЭФ демонстрируется сообщение об обучении и отображается значение среднеквадратичной ошибки обучения нейронной сети в метрической системе. Пример ЭФ представлен на рисунке 4.12

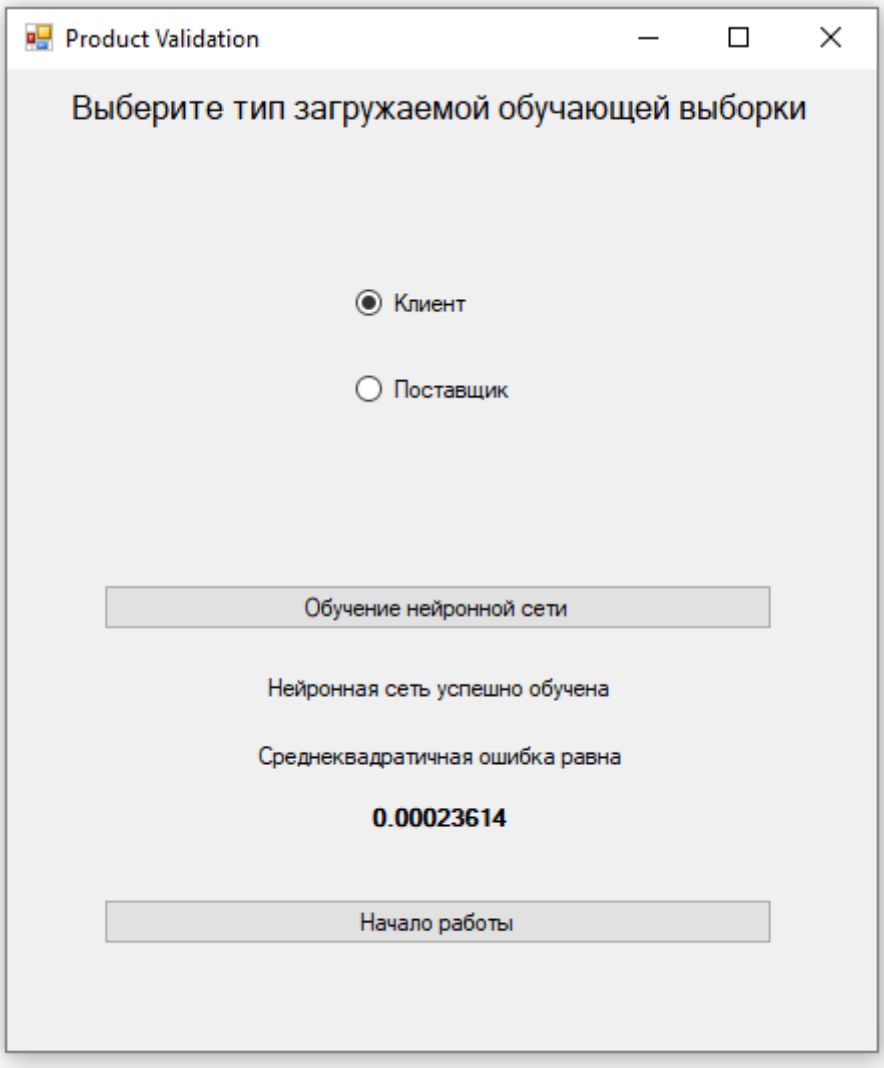


Рисунок 4.12 – ЭФ обучения нейросети

На рисунке 13 представлена экранная форма "ввода исходных данных". Здесь пользователю необходимо ввести исходные данные, содержащие приблизительную вероятность возникновения и активизации данной угрозы.

Защищенные реквизиты недоступны для получения используя объективное измерение. Все они задаются собственником информации и определяются, используя степень их важности. Все виды последствий, а также их ценность определяются владельцем, который для оценки может полагаться на рекомендации.

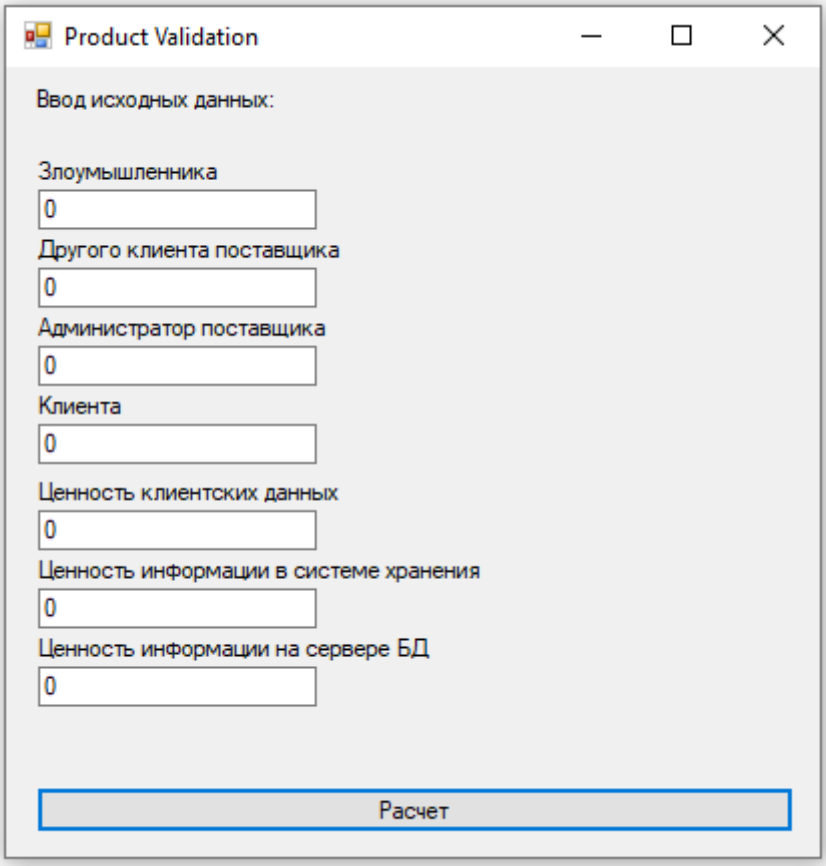


Рисунок 4.13 – ЭФ «Ввод исходных данных»

В данном ПО присутствует контроль над вводимыми данными, применимый к проверке ценности информации и потенциальных значений возможности возникновения и активизации угроз. Как только все данные вводятся в программу, становится возможным рассчитать вероятность возникновения угрозы. Данное действие происходит при помощи клика на

кнопку "Расчет". На рисунке продемонстрирован контроль над значениями, которые были введены.

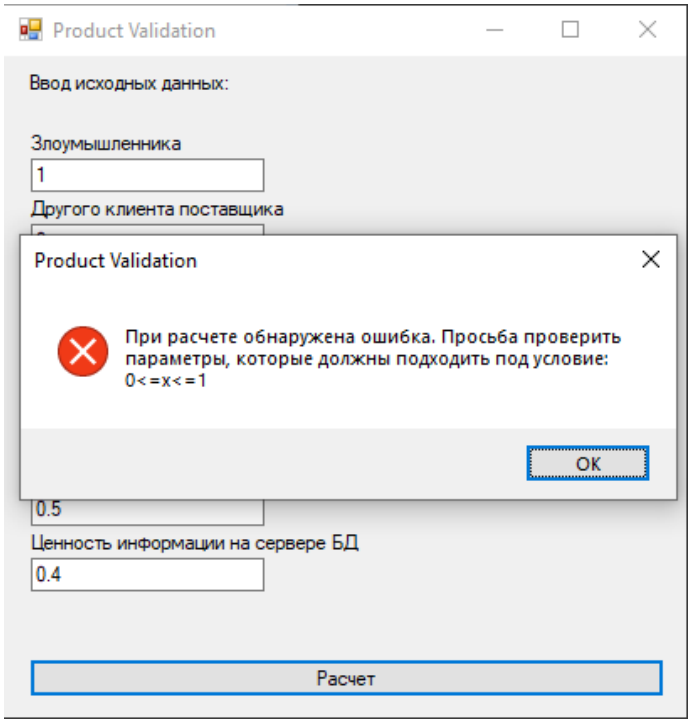


Рисунок 4.14 – ЭФ ошибки контроля данных

Полагаясь на введенную информацию, которая обрабатывается в системе облачных вычислений, и о вероятности появления угрозы. Программа может произвести расчет оперативного значения уровня вероятности возникновения угроз нарушения ИБ для облака.

Расчет вероятности возникновения угроз нарушения реализован при помощи модуля, разработанного в данной работе. Результат выводится в виде информативного сообщения, пример представлен на рисунке 15.

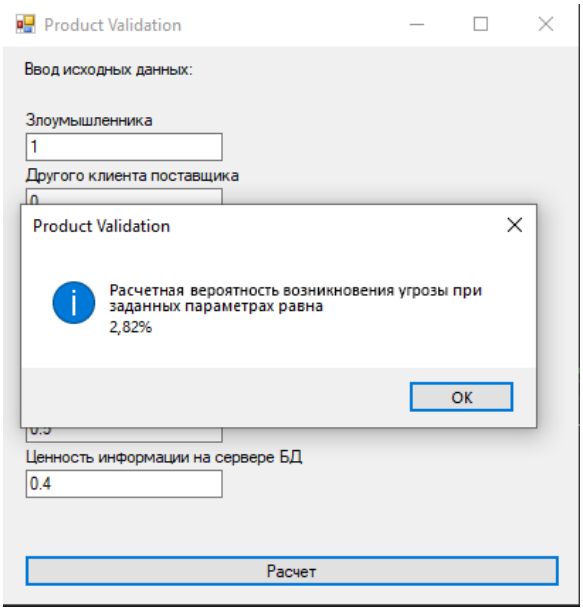


Рисунок 4.15 – ЭФ сообщения о результате расчета

Таким образом была продемонстрирована функциональность программы «Product validation», и продемонстрирована его способность для проверки ИБ в облачных вычислениях.

4.5 Демонстрация итогов исследований, при использовании программы «Product validation» для проверки системы облачных вычислений

Применяя программу, которая была описана выше, был выполнен эксперимент. В рамках которого произошло изменение значений возможности возникновения угрозы, а также произошло изменение ценности ресурсов информации в объеме [0,1]. Была выполнена реализация набора значений выходов нейросети, который до этого не применялся в обучающей выборке. Такой набор называется тестовым набором. Задачей набора является проверка способности нейросети выполнить вычисления по набору, не входившего в список наборов, использованных для обучения нейросети. На входной уровень сети поступали значения при одновременном срабатывании нескольких источников угроз, а также разные значения большой разрядности.

Выполнена сверка результатов ручного расчета и численного. Данные расчеты были получены при вычислении вероятности возникновения угроз нарушения ИБ

Ниже в таблице 4.3 показано сравнение ручного расчета и численного, выполненного с помощью программы.

Обозначения вероятностей угроз, которые реализованы:

$Р^{зл}$- нарушитель политики безопасности;

$Р^{пт}$ - любой потребитель облачных сервисов;

$Р^{р\_пост}$ - работник поставщика;

$Р^{р\_пот\_н}$- работник клиента (нарушитель политики безопасности)

$R^{рр}$ – ручной расчет

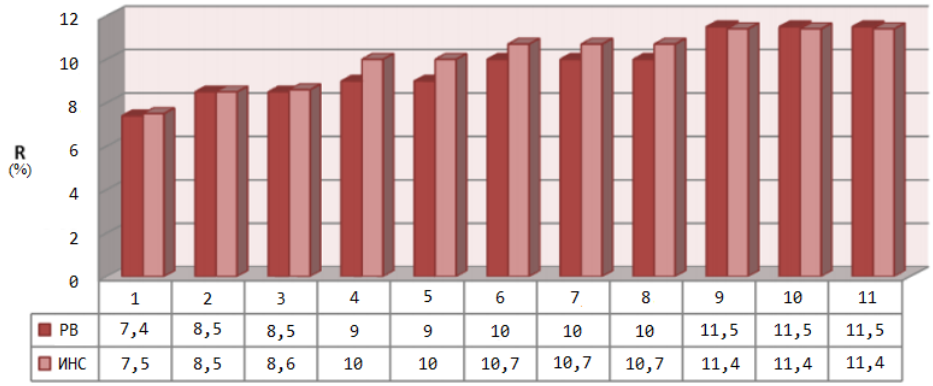
$R^{рп}$ –программный расчет

С - ценность информационных активов

Таблица 4.3 - Сравнение ручного и численного расчетов.

$Р^{зл}$	$Р^{пт}$	$Р^{р\_пост}$	$Р^{р\_пот\_н}$	С1	С2	С3	$R_{оп}$ (рас, %)	$R_{оп}$ (пр, %)
1	0	1	0	0,5	0,4	0,1	14	14,1
0	1	0	1	0,5	0,4	0,1	18	17,9
0	1	1	0	0,5	0,4	0,1	21	21
1	1	0	0	0,5	0,4	0,1	14	14,2
1	1	1	0	0,5	0,4	0,1	23,1	23
0	0	1	0	0,55	0,27	0,18	9,8	10
0	0	1	0	0,66	0,12	0,22	7,5	7,5
0	0	0	1	0,14	0,38	0,48	2,9	2,95
0	0	0	1	0,82	0,12	0,06	11,3	11,3
0	0	0	1	0,53	0,25	0,22	7,8	7,9

На рисунке 4.16 представлена диаграмма - точности настройки весовых коэффициентов нейронной сети, разработанных в программе.



	1	2	3	4	5	6	7	8	9	10	11
РВ	7,4	8,5	8,5	9	9	10	10	10	11,5	11,5	11,5
ИНС	7,5	8,5	8,6	10	10	10,7	10,7	10,7	11,4	11,4	11,4

Рисунок 4.16 - диаграмма - точности настройки весовых коэффициентов нейронной сети разработанных в программе

На рисунке 4.16 темно-красным цветом обозначены значения, которые были рассчитаны вручную по формулам. Розовым цветом – значения, которые были получены с помощью программы. Входные параметры для обоих вычислений задавались одинаковые. Результатом данного эксперимента является, то, что расчеты различаются всего на тысячную. Следовательно, 10^{-3}в метрической системе – среднеквадратичной ошибки обучения нейросети в программе.

Также был выполнен дополнительный эксперимент, где данные, которые хранятся на облачном сервере были взяты, как актив. Суть эксперимента была в том, что при помощи программы проанализировать, каким образом деятельность пользователя облака может нанести ущерб системе облачных вычислений. При этом в статистике инцидентов участвуют угрозы преднамеренные и случайные.

На рисунке 4.17 представлены графики зависимости величины оперативного значения вероятности возникновения угроз нарушения информационной безопасности $\overline{R}$ от значения ценности информации объектов облачного хранилища.

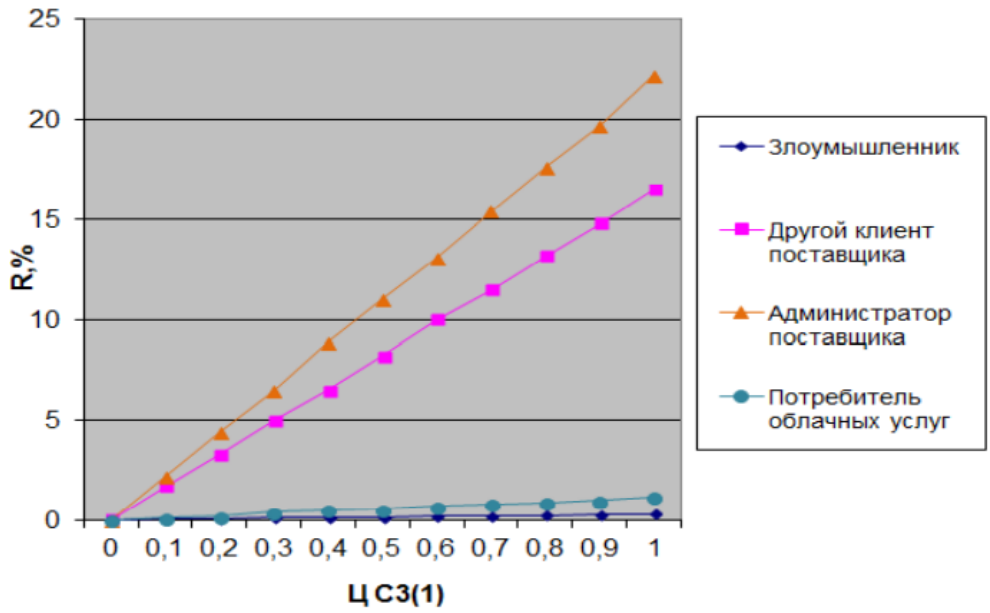


Рисунок 4.17 - графики зависимости величины оперативного значения вероятности возникновения угроз нарушения информационной безопасности $\bar{R}$

Исходя из всего вышеперечисленного, можно сделать вывод о том, что с помощью расчетов было доказано, что самые опасные угрозы информационной безопасности для системы облачных вычислений - внутренние нарушения ИБ, то есть угрозы, которые происходя из деятельности поставщика\потребителя облачных услуг. Также стоит отметить, методология, которая была предложена в данной работе эффективна и целесообразна, основываясь на проведенных экспериментах главы 4.

4.6 Выводы по четвертой главе

1. Для демонстрации эффективности метода обратного распространения ошибки для обучения нейросетей, было выполнено исследование в данной работе. Данное исследование проводилось при помощи ПО " Matlab". При обучение нейронной сети удалось минимизировать ошибки. обучение нейронной сети, которая проходила 10 эпох. Также можно отметить, что среднеквадратичная ошибка составляла от $10^{-3} - 10^{-2}$, а при обучении 10^{-4} в метрической системе. После тестирования и обучения нейросети, результаты продемонстрировали возможность использования данного алгоритма и архитектуры для создания модуля расчета потенциальных оценок вероятности

возникновения угроз нарушения ИБ, для дальнейшего его использования в программе, с целью автоматизации проверок безопасности в системе.

2. Созданы блок-схемы работы программы и модель автоматизированного средства для проверок ИБ. При помощи UML-диаграммы были описаны модули библиотеки, которая применяется в программе.

3. Реализована программа для автоматизации процесса проведения проверок ИБ в системе облачных вычислений, цель которых, понять и выполнить оценку оперативного значения уровня вероятности возникновения угроз нарушения. В приведенном в примере суммарный вероятности возникновения угроз нарушения ИБ равен 2,82%. Точность согласования весовых коэффициентов нейросети, которая реализована в данной программе, равна 0,1%.

4. При помощи расчетов было доказано, что самые опасные угрозы информационной безопасности для системы облачных вычислений - внутренние нарушения ИБ, то есть угрозы, которые происходя из деятельности поставщика\потребителя облачных услуг.

Заключение

1. Предложен способ разграничения доступов для ролей, что приводит к исключению роли пользователя с максимальными доступами, и убирает его вероятность прямого использования потоков данных клиента и устранение возможности распоряжения конфигурационными файлами облака. Стоит отметить, что способ применяется при разработке методики частной политики.

2. Предложено 2 подхода к проведению проверок ИБ в облаке, применяя прогнозируемое и оперативное значение уровня вероятности возникновения угроз нарушения ИБ. Перове значение применяется на стадии проектирования защиты информации в облаке, а второе для определения вероятности возникновения угроз в настоящее время, учитывая возможность возникновения сложной атаки.

3. С помощью метода нечетких когнитивных карт была реализована модель преднамеренных угроз нарушения ИБ в облаке.

4. Реализована программа для автоматизации процесса проведения проверок ИБ в системе облачных вычислений, цель которых, понять и выполнить оценку оперативного значения уровня вероятности возникновения угроз нарушения. В приведенном в примере суммарная вероятность возникновения угрозы нарушения ИБ равна 2,82%. Точность согласования весовых коэффициентов нейросети, которая реализована в данной программе, равна 0,1%.

5. При помощи расчетов было доказано, что самые опасные угрозы информационной безопасности для системы облачных вычислений - внутренние нарушения ИБ, то есть угрозы, которые происходя из деятельности поставщика\потребителя облачных услуг.

Список используемой литературы

Научная и методическая литература

1. Баранова Е., Бабаш А. – Информационная безопасность и защита. Инфра – М. 2017 – 324 с.
2. Бостром Н. – Искусственный интеллект Этапы. Угрозы. Стратегии– М.: Издательство « МИФ», 2016 – 760 с.
3. Брэгг, Роберта Безопасность сетей. Полное руководство // Р. Брэгг, М. Родс-Оусли, К. Страссберг; пер. с англ. – М.: Издательство «Эконом», 2018. – 912 с.
4. Глеске Д.О. Понятие аудита информационной безопасности. / Вестник научных конференций. 2020. №11-4(63). Наука, образование, общество: по материалам международной научно-практической конференции 30 ноября 2020 г. Часть 4. – С. 26-27
5. Глеске Д.О. Программное обеспечение, предусматривающее полный анализ рисков. / Вестник научных конференций. 2020. №11-4(63). Наука, образование, общество: по материалам международной научно-практической конференции 30 ноября 2020 г. Часть 4. – С. 27-28
6. Гребнев Е. Облачные сервисы. Взгляд из России – М.: CNews, 2018. – 282с.
7. Кан К.А. –Нейронные сети. Эволюция – М.: Издательство «ЛитРес» , 2018. – 380 с.
8. Клейнбер Д. – Алгоритмы. Разработка и применение – М.: Издательство «Питер», 2016 – 800 с.
9. Маркелов А. А. - OpenStack. Практическое знакомство с облачной операционной системой – М.: Издательство «ДМК-Пресс, 2.», 2018. – 306 с.
10. Николенко С – Самообучающиеся системы – М.: Издательство «МЦНМО» , 2015. – 289 с.

11. Николенко С. - Глубокое обучение. Погружение в мир нейронных сетей // Кадурин .А., Архангельская Е – М.: Издательство «Питер СПб» , 2020. – 480 с.

12. Околов, А.Р. Использование «облачных вычислений» в автоматизированных системах обработки информации // А.Р.Околов, А.А. Трекало, А.В. Николаенок. 2017-543с.

13. Разумников С.В. Интегральная модель оценки эффективности и рисков облачных ИТ-сервисов для внедрения на предприятие // Фундаментальные исследования. – 2015. – № 2-24. – С. 5362-5366;

14. Рашид Тарик – Создаем нейронную сеть – М.: Издательство «Вильямс», 2018 – 220 с.

15. Родичев Ю. – Нормативная база и стандарты в области информационной безопасности – М.: Издательство « Питер», 2017 – 256 с.

16. Савельев А.О. — Введение в облачные решения Microsoft - Национальный Открытый Университет "ИНТУИТ" - 2016. -230с.

Электронные ресурс

17. Arif Mohamed. A history of cloud computing. [Электронный ресурс]: - Режим доступа: http://www.computerweekly.com/feature/A-history-of-cloud-computing .

18. Introduction to combinatorial mathematics Liu C.L. [Электронный ресурс]: - Режим доступа: http://en.bookfi.net/book/560269

19. Peter M. Mell, Timothy Grance The NIST Definition of Cloud Computing [Электронный ресурс]: - Режим доступа: https://www.nist.gov/node/568586

20. Share [Электронный ресурс]: - Режим доступа:https://www.cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf

21. Алан Вестин [Электронный ресурс]: - Режим доступа:https://en.wikipedia.org/wiki/Alan_Westin

22. Высокопроизводительные вычисления как облачный сервис: ключевые проблемы [Электронный ресурс] / А. О. Кудрявцев [и др.]. –Режим доступа: http://omega.sp.susu.ac.ru/books/conference/PaVT2013/short/032.pdf.

23. Модели системной динамики на основе нечетких реляционных когнитивных карт [Электронный ресурс]: - Режим доступа: https://sccs.intelgr.com/archive/2016-01/04-Fedulov.pdf

24. Москаленко А. Облачно и мобильно: что может спасти российский ИТ-рынок? [Электронный ресурс]. – Режим доступа: http://www.inlinegroup.ru/events/press-releases/5635.php

25. Орлов, С. Интегрированные системы для частного облака / С. Орлов // Журнал сетевых решений [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/2017/03/13040161/.

26. Построение нечетких когнитивных карт для анализа управления рисками [Электронный ресурс]: - Режим доступа: https://cyberleninka.ru/article/n/postroenie-nechetkih-kognitivnyh-kart-dlya-analiza-i-upravleniya-informatsionnymi-riskami-vuza/viewer

27. Угрозы облачной безопасности по версии Cloud Security Alliance [Электронный ресурс]: - Режим доступа: https://iaas-blog.it-grad.ru/bezopasnost/top-12-ugroz-oblachnoj-bezopasnosti-po-versii-cloud-security-alliance/

28. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) [Электронный ресурс]: - Режим доступа:http://www.consultant.ru/document/cons_doc_LAW_61801/

Литература на иностранном языке

29. D. Talia, P. Trunfio, F. Marozzo. Data analysis in the cloud: models, techniques and applications, 2016. – 138 c- Amsterdam [etc.]: Elsevier.

30. John Rhoto. Cloud Computing Architected: Solution Design Handbook. – 2013 - 423 c. - Kindle Edition

31. John Rhoton. Cloud Computing Explained: Implementation Handbook for Enterprises 2nd ed. Edition second edition Edition / Gerhard Weiss. - Cambridge:The MIT Press, 2018 - 450 с. - 2nd Edition

32. M. Hugos, D. Hulitzky. – Hoboken: John Wiley & Sons. Business in the cloud: what every business needs to know about cloud computing /, 2011. – 205 с.

33. T. Mather, S. Kumaraswamy, S. Latif. Cloud security and privacy /– Beijing [etc.]: O'Reilly, 2019. – 312 с

Приложение 1. Программный код «product validation»

File Program.cs

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.IO;
using System.Threading.Tasks;
using static System.Math;
using System.Windows.Forms;
using System.Numerics;
using NeuralNetLib;

namespace Product_validation
{
    static class Program
    {
        public static Form1 form1;
        public static NeuralNet NN;
        public static NeuralNetworkB NeuralNetB1;

        [STAThread]
        static void Main()
        {
            form1 = new Form1();
            NN = new NeuralNet();
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(form1);
        }
    }

    public class NeuralNet
    {
        public List<String> lines;

        public List<float> xInputVector;      //входной вектор
        public List<float> xOutputVector;     //выходной вектор

        public void TrainNetwork(bool isClient)
        {
            string s = "";
            int k = 0;
            lines.Clear();
            Program.form1.GetProgressBar().Show();
            if (isClient)
            {
                foreach (var item in File.ReadAllLines("client.txt"))
                {
                    lines.Add(item);
                }
            }
            else
            {
                foreach (var item in File.ReadAllLines("vendor.txt"))
                {
                    lines.Add(item);
                }
            }
            NeuralNetB1.ResetPatterns();

            xInputVector = new List<float>();
            xOutputVector = new List<float>();
```

```
            for (int i = 0; i < lines.Count; i++)
            {
                k = 0;
                for (int j = 0; j < lines[i].Length; j++)
                {
                    if (lines[i][j] != '\t') {
                        s += lines[i][j];
                    }
                    else
                    {
                        xInputVector[k] = float.Parse(s);
                        k++;
                    }
                    if (j == lines[i].Length - 1)
                    {
                        xOutputVector[0] = float.Parse(s);
                    }
                }
            }
            NeuralNetB1.AddPattern(xInputVector, xOutputVector);
            NeuralNetB1.TeachOffLine();
        }


    }
}
```

File form1.cs

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace Product_validation
{
    public partial class Form1 : Form
    {
        private ProgressBar progressBar1;
        private TextBox tb1;

        public Form1()
        {
            InitializeComponent();
        }

        private void Form1_Load(object sender, EventArgs e)
        {

        }

        public ProgressBar GetProgressBar() {
            return progressBar1;
        }
        private void button1_Click(object sender, EventArgs e)
        {
            Program.NN.TrainNetwork(clientRB.Checked);
```

```
        }
        private void button2_Click(object sender, EventArgs e)
        {
            List<float> xInputVector = new List<float>(7);
            bool[] err = new bool[8];

            for (int i = 0; i < 8; i++)
            {
                err[i] = false;
            }
            if (TextBox1.Text = '0' || TextBox1.Text = '1')
            {
                err[0] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label1.Text + " должно быть равно 1 или 0");
            }
            if (TextBox2.Text = '0' || TextBox2.Text = '1')
            {
                err[1] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label2.Text + " должно быть равно 1 или 0");
            }
            if (TextBox3.Text = '0' || TextBox3.Text = '1')
            {
                err[2] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label3.Text + " должно быть равно 1 или 0");
            }
            if (TextBox4.Text = '0' || TextBox4.Text = '1')
            {
                err[3] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label4.Text + " должно быть равно 1 или 0");
            }

            if (float.Parse(TextBox5.Text) > 0 && float.Parse(TextBox5.Text) < 1)
            {
                err[4] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label5.Text + " должно быть больше 0 и меньше
1");
            }

            if (float.Parse(TextBox6.Text) >= 0.2f && float.Parse(TextBox6.Text) <= 0.7f)
            {
                err[5] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label6.Text + " должно быть больше 0,2 и меньше
0,7");
            }

            if (float.Parse(TextBox7.Text) > 0 && float.Parse(TextBox7.Text) < 1)
```

```
            {
                err[6] = true;
            }
            else
            {
                MessageBox.Show("значение" + Label7.Text + " должно быть больше 0 и меньше
1");
            }

            if      (float.Parse(TextBox5.Text)      +      float.Parse(TextBox6.Text)      +
float.Parse(TextBox7.Text))
            {
                err[7] = true;
            }
            else
            {
                MessageBox.Show("сумма параметров" + Label5.Text + ' + ' + Label6.Text + ' +
' + Label7.Text + " должно быть равно 1");
            }
            bool isAllClear = true;
            foreach (var item in err)
            {
                if (!item)
                {
                    isAllClear = false;
                    break;
                }
            }
            if (isAllClear)
            {
                xInputVector[0] = float.Parse(TextBox1.Text);
                xInputVector[1] = float.Parse(TextBox2.Text);
                xInputVector[2] = float.Parse(TextBox3.Text);
                xInputVector[3] = float.Parse(TextBox4.Text);
                xInputVector[4] = float.Parse(TextBox5.Text);
                xInputVector[5] = float.Parse(TextBox6.Text);
                xInputVector[6] = float.Parse(TextBox7.Text);

                Program.NeuralNetB1.Compute(xInputVector);
            }
        }
    }
}
```