Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский государственный авиационный технический университет»

На правах рукописи

СЕНЦОВА Алина Юрьевна

МОДЕЛИ И МЕТОД ЭКСПЕРТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Специальность: 05.13.19 –
Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:
доктор технических наук, доцент
Машкина И. В.

Уфа – 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования

Сегодня в индустрии информационных сервисов можно наблюдать стремительные темпы развития информационных систем, построенных на основе облачных технологий (ИСОТ). Облачные вычисления позволяют современным компаниям снизить расходы за счет использования виртуальной инфраструктуры поставщика облачных услуг, уменьшить затраты времени и ресурсов на администрирование информационных систем, а также снизить финансовые затраты на построение собственной информационной системы. Уже сейчас аналитики прогнозируют развитие рынка облачных услуг для бизнеса в России более чем в четыре раза в течение 2016 года (39 млрд. руб.), а к 2020 году объем мирового облачного рынка составит $241 млрд. В связи с тем, что, зачастую, компании-потребители облачных услуг обрабатывают в облачных средах критичные для них информационные активы, на сегодняшний день вопрос обеспечения информационной безопасности ИСОТ становится наиболее актуальным для потребителя облачных услуг.

Хотя поставщики, обслуживая предприятия с оборотом в миллиарды долларов, делают все возможное для обеспечения максимальной безопасности среды облака, особенности построения облачной инфраструктуры, использование технологии виртуализации и связанная с ней возможность нарушения изоляции виртуальных машин, а также параллельная обработка больших объемов данных разных потребителей облачных услуг, позволяют говорить о новых потенциально возможных угрозах информационной безопасности (ИБ), которые будут являться специфичными для облачных вычислений.

Объективная оценка степени защищенности данных потребителя облачных услуг в облачной инфраструктуре поставщика осуществляется в

ходе проведения аудита информационной безопасности. В результате аудита информационной безопасности ИСОТ можно выявить, насколько рационально решены вопросы безопасности информации и контроля доступа в облачной среде, определить, как минимизировать риски при обработке в ИСОТ конфиденциальной информации потребителя облачных услуг, локализовать слабые места в системе обеспечения информационной безопасности и сформулировать рекомендации о путях решения существующих проблем безопасности в системе. Кроме того, потребитель заинтересован в определении поставщиком конкретного объективного механизма для оценки качества предлагаемой облачной услуги.

В связи с вышеизложенным тема диссертационной работы, посвященная разработке методологии аудита информационной безопасности облачных вычислений, является актуальной.

Степень разработанности темы

На сегодняшней день практически отсутствуют серьезные исследования не только в области аудита информационной безопасности облачных вычислений, но и публикации, посвященные общим вопросам ИБ облачных сред. В работах П.Д. Зегжды и Д.П. Зегжды отмечается рост рынка облачных услуг и рассматриваются основные угрозы системам облачных вычислений и, в особенности, угрозы, связные с технологией виртуализации, используемой в облачных вычислениях. В работах С.В. Белима и Н.Ф. Богаченко обосновывается важность обеспечения информационной безопасности в облачных вычислениях и особенно подчеркивается необходимость контроля доступа к предоставляемым поставщику ресурсам. Однако, многие исследования вопросов безопасности облачных сред, в числе которых работы Маслова В.А., Рахматуллиной А.Р., Варновского Н.П., Захарова В.А., Шокурова А.В., сводятся к проблемам шифрования потока межоблачных данных между поставщиком и потребителем облачных услуг. Однако в них не рассматриваются специфичные для облачных вычислений угрозы и средства защиты. В работах Зубарева И.В., Радина П.К., Демурчева

Н.Г., Коваленко О.С., Алимурадова Т.К. рассматриваются основные угрозы ИСОТ, а также отмечается необходимость разделения полномочий облачной среды, но не описываются конкретные механизмы для устранения угроз ИБ и минимизации предоставления избыточных привилегий поставщику ИСОТ. В работах Шаньгина В.Ф., Нестеркиной Е.М., Бердника А.К., Царегородцева А.В., Качко А.К. подчеркивается необходимость стандартизации облачных вычислений в РФ, а также делается вывод: из-за отсутствия стандартов в области информационной безопасности облачных вычислений, проведение аудита системы обеспечения информационной безопасности ИСОТ, на сегодняшний день, затруднено. Конкретные же решения в области проведения аудита облачных вычислений также отсутствуют.

Вместе с тем, для обеспечения сохранности конфиденциальной информации, обрабатываемой в облачной среде, существующая система обеспечения информационной безопасности ИСОТ должна периодически подвергаться независимому аудиту, который в соответствии с требованиями международных стандартов, является одним из обязательных этапов жизненного цикла любой информационной системы. В связи с этим, разработка методологии аудита информационной безопасности ИСОТ является актуальной проблемой ИБ облачных вычислений.

Объектом исследования является информационная система взаимодействия поставщика и потребителя облачных услуг – система облачных вычислений (СОбВ).

Предметом исследования являются модели и метод экспертного аудита ИБ в системе облачных вычислений.

Целью исследования является повышение оперативности и адекватности оценки уровня опасности инцидентов в системе информационного взаимодействия поставщика и потребителя облачных услуг.

Задачи исследования:

1. Определить *перечень угроз* нарушения информационной безопасности, характерных для облачных вычислений, и *их источники*. Разработать *модель* преднамеренных *угроз* нарушения информационной безопасности с учетом особенностей СОбВ.

2. Разработать *методику* формирования частной политики безопасности СОбВ, основываясь на рекомендациях проектов государственных стандартов РФ в сфере облачных вычислений и учитывая специфику информационных систем, построенных на основе технологии облачных вычислений.

3. Разработать *метод проведения аудита информационной безопасности* системы облачных вычислений, основанный на получении численной оценки риска нарушения ИБ с использованием искусственной нейронной сети.

4. Разработать *программный модуль автоматизации процесса экспертного аудита ИБ* СОбВ, реализующий предложенные модели и методы. Исследовать адекватность предложенных моделей и методов на основе вычислительных экспериментов.

Методы исследования

При решении поставленных в диссертационной работе задач использованы методы системного анализа, методы теории защиты информации, теории множеств, теории нечетких когнитивных карт, методология функционального моделирования и моделирования динамических систем, а также теория искусственных нейронных сетей.

Положения, выносимые на защиту

1. Выявлен *перечень угроз* нарушения ИБ от *источников угроз*, характерных для СОбВ и разработана *модель* преднамеренных целенаправленных *угроз* нарушения информационной безопасности, основанная на построении нечетких когнитивных карт с учетом особенностей инфраструктуры СОбВ.

2. Предложены *модель политики* информационной *безопасности* ИСОТ и *методика разработки частной политики безопасности* СОбВ, основанная на ролевой модели, *позволяющая исключить* из иерархии ролей роль *суперпользователя*, имеющего полномочия напрямую обращаться к результирующим потокам данных, *управлять* всеми конфигурационными файлами СОБВ, и *увеличить* доверие потенциальных потребителей к ИСОТ

3. Разработан метод аудита информационной безопасности, основанный на использовании искусственной нейронной сети, отличающийся получением численной оценки оперативного значения риска, когда угроза проявляется по конкретным путям распространения.

4.Разработана *модель программного средства* проведения аудита ИБ системы облачных вычислений и *программный модуль*, автоматизирующий процесс проведения аудита ИБ и *позволяющий посредством информации с датчиков событий* получить численную оценку риска нарушения информационной безопасности в реальном масштабе времени и осуществить оперативный выбор рационального варианта реагирования на возможные инциденты.

Научная новизна

1. Новизна модели угроз нарушения информационной безопасности в системе облачных вычислений, построенной с помощью нечеткой когнитивной карты, заключается в визуализации путей распространения угроз в облачных средах и в расширении списка источников для СОбВ, по сравнению с другими информационными системами, что позволяет учесть угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, а также учесть такой источник угроз как другой потребитель облачных услуг, реализующий собственные бизнес-задачи.

2. Новизна *методики разработки частной политики безопасности* для СОбВ, основанной на моделях политики ИБ ИСОТ и ролевого разграничения доступа, *заключается* в назначении нескольких максимальных ролей,

которые имеют одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества, и *минимально необходимую роль* для поддержки бизнес-процессов СОбВ, что позволит исключить пользователя, получающего по иерархии ролей права *суперпользователя* поставщика и исключить возможность для него напрямую обращаться к результирующим потокам данных потребителя облачных услуг и управлять всеми конфигурационными файлами системы облачных вычислений.

3. Новизна метода проведения *экспертного аудита* информационной безопасности системы облачных вычислений состоит в получении численной оценки *оперативного* значения уровня риска нарушения информационной безопасности с использованием искусственной нейронной сети, при обработке ею информации с сенсоров и датчиков опасных событий, обучение которой осуществляется на множестве данных обучающей выборки, сформированной на основе аналитических расчетов прогнозируемого уровня риска, с использованием когнитивной карты в качестве модели угроз, что позволит поставщику облачных услуг *обеспечить* адекватное реагирование на возможные инциденты в реальном масштабе времени и *обосновать* свои возможности по обеспечению защищенности критичной информации потребителя.

4. Новизна *программного модуля*, реализующего методологию аудита информационной безопасности системы облачных вычислений, заключается в возможности оценить*: прогнозируемое* значение уровня риска нарушения информационной безопасности при проектировании системы защиты информации в СОбВ, *оперативное* значение уровня риска в *реальном масштабе времени* в процессе реализации угрозы по конкретному пути, а также *с учетом сложных сценариев атак*.

Степень достоверности и апробация результатов

Основные положения диссертационной работы докладывались и обсуждались на следующих научных конференциях:

− V, VI, VII, VIII и IX Всероссийских молодежных научных конференциях «Мавлютовские чтения», Уфа, 2011, 2012, 2013, 2014, 2015;

− XII и XIII Всероссийских конкурсах-конференциях студентов и аспирантов по информационной безопасности «SIBINFO-2012» и «SIBINFO-2013», Томск, 2012, 2013;

− VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013), Санкт-Петербург, 2013;

− XII и XIII Международных научно-практических конференциях «Информационная безопасность-2012» и «Информационная безопасность-2012», Таганрог, 2012, 2013;

− IV Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива-2014», Таганрог, 2014;

− XXI Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Москва, 2014;

− The 7th International Conference on Security of Information and Networks (SIN 2014), 2014, г. Аксарай, Турция.

Результаты диссертационного исследования внедрены в производственный процесс ООО «Атлас-Телеком» и в учебный процесс кафедры «Вычислительная техника и защиты информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет». На программный модуль, автоматизирующий процесс проведения аудита ИБ, получено свидетельство о государственной регистрации программы для ЭВМ.

Теоретическая и практическая значимость работы

Теоретическая значимость полученных результатов заключается в:

● выявленном *перечне угроз* нарушения ИБ системы облачных вычислений и дополненном списке *источников угроз,* позволяющих расширить модель угроз ИСОТ в соответствии со специфическими угрозами, не характерными для традиционных информационных систем;

● в разработанном *методе аудита ИБ в СОбВ*, апробированном на практике при решении задачи определения оперативного значения уровня риска нарушения информационной безопасности;

● в разработанном с использованием методологии функционального моделирования IDEF0 графическом представлении механизма оценивания значений уровня риска нарушения информационной безопасности в реальном масштабе времени с помощью искусственной нейронной сети;

● в разработанной *модели частной политики информационной безопасности* СОбВ, соблюдение требований которой позволит увеличить доверие потенциальных потребителей к ИСОТ и модернизированной *методике разработки частной политики безопасности* СОбВ, которая позволяет исключить роль суперпользователя из множества субъектов доступа системы облачных вычислений.

Практическая значимость разработанных моделей и методов заключается в возможности рекомендовать членам облака сообщества провести модернизацию сети и установить специфичные для облачных сред средства защиты в целях повышения уровня защищенности всей СОбВ в целом и возможности принятия решений по выбору рационального варианта реагированию в реальном масштабе времени.

ГЛАВА 1. АНАЛИЗ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНОГО ОБЛАКА

1.1. Анализ информационной системы, построенной на основе облачных технологий, как объекта защиты

1.1.1 Обзор существующих видов облачных услуг и моделей облачного размещения

Современные тенденции развития ИТ-индустрии позволяют переходить от традиционных методов обработки информации к более прогрессивным. Одним из таких методов является перенос вычислений организации-потребителя в облачные структуры провайдера облачных вычислений – поставщика облачных услуг. Вычисления в облаке – это базирующиеся на совокупности разных технологий способы предоставления потребителю через Интернет масштабируемых ресурсов как услуг, при котором средства поддержки этих услуг скрыты от него, а сами ресурсы оплачиваются потребителем по мере их использования [1]. Облачные вычисления позволяют не усложнять информационную инфраструктуру потребителя облачных услуг благодаря использованию объединенных в виртуальную инфраструктуру ресурсов поставщика.

Облачная информационная система состоит из облачного клиента и облачного сервера [2]. Под облачным клиентом понимаются средства вычислительной техники, входящие в состав информационной системы, построенной с использованием технологий облачных вычислений, при помощи которых осуществляется получение одной или нескольких облачных услуг. Облачный сервер – распределённая вычислительная сеть, обрабатывающая запросы потребителей облачных услуг. Облачный сервер может иметь в своем составе сетевое оборудование, серверы обработки

данных, операционную систему (ОС), сетевые хранилища, средства управления базами данных, прикладные программы, сетевые службы и др.

На виртуальном сервере, находящемся в «облаке» поставщика, под управлением различных операционных систем может одновременно функционировать *множество* приложений потребителей облачных услуг. Виртуальное разделение ресурсов позволяет создавать *сетевые домены*, предоставляющие услуги разным потребителям по обработке конфиденциальной информации.

При использовании модели доступа «облачные вычисления», информационные сервисы предоставляются таким образом, что обеспечивающие технологии становятся практически «невидимыми» для потребителя. А поскольку это позволяет отделить информационные сервисы от обеспечивающей их работу информационной инфраструктуры и тем самым позволить бизнесу быстрее адаптироваться к изменениям, облачные вычисления могут являться частью стратегии по повышению динамичности работы современных предприятий.

Появление первой технологии, близкой к современному пониманию термина «cloud computing», приписывается компании Salesforce.com, основанной в 1999 году [3]. Именно тогда и появилось первое предложение нового вида − «Программное обеспечение как сервис» (“Software as a Service”, “SaaS”). Первое бизнес-решение под названием «Amazon Web Services» было запущено в 2005 году компанией Amazon.com, которая активно занималась модернизацией своих центров обработки данных (ЦОД). Наиболее характерный пример широко используемых приложений облачных вычислений сегодня— служба Google Docs, позволяющая работать с офисными документами через браузер потребителя.

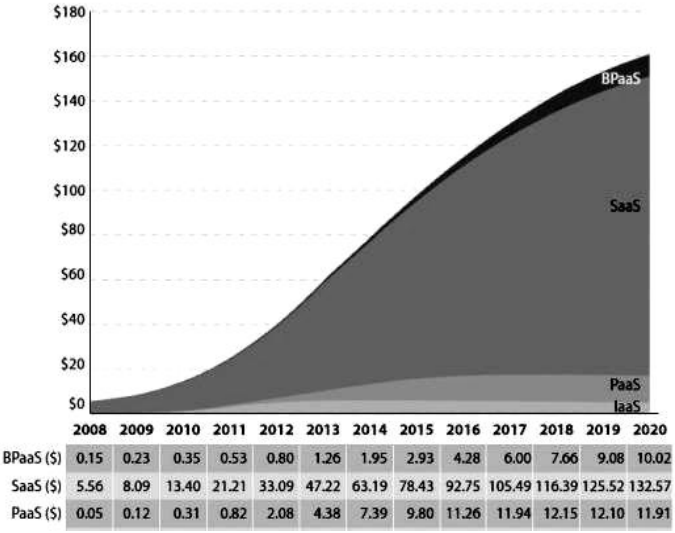
В таблице 1.1 показаны этапы развития рынка облачных вычислений с 2007 года по сегодняшний день.

Таблица 1.1 − Этапы развития рынка облачных вычислений

Этап	Продолжительность (г)	Особенности
Время первопроходцев	2007-2010	Облачные вычисления внедряют те компании, которые готовы идти на риски.
Консолидация рынка	2010-2012	Консервативные пользователи начинают обращать внимание на облачные вычисления; растет конкуренция и снижается общее число поставщиков.
Массовое распространение	2012-2017	Облачные вычисления становятся преобладающим направлением в развитии IT-индустрии; на рынке доминирует ограниченное число поставщиков

Сам факт высокой заинтересованности крупнейших игроков рынка ИТ демонстрирует определенный статус облачных вычислений как наиболее привлекательного направления для развития IT-индустрии 2012 − 2017 годов [4].

В апреле 2014 года аналитическая компания Forrester Research опубликовала прогноз развития рынка публичных облачных вычислений до 2020 г (см. рисунок 1.1). Согласно сведениям отчета, к 2020 г. объем облачного рынка составит $160 млрд [5].



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
BPaaS ($)	0.15	0.23	0.35	0.53	0.80	1.26	1.95	2.93	4.28	6.00	7.66	9.08	10.02
SaaS ($)	5.56	8.09	13.40	21.21	33.09	47.22	63.19	78.43	92.75	105.49	116.39	125.52	132.57
PaaS ($)	0.05	0.12	0.31	0.82	2.08	4.38	7.39	9.80	11.26	11.94	12.15	12.10	11.91

Рисунок 1.1 − Динамика развития рынка облачных вычислений

Существует множество видов облачных услуг и моделей облачного размещения. Компании потребителя облачных услуг необходимо понять разницу между имеющимися типами облачных сред и определить, какие из них наилучшим образом соответствуют ее бизнес-процессам.

Различают несколько моделей облачного размещения. *Частное облако (private cloud)* – инфраструктура, предназначенная для использования одной организацией, включающей несколько потребителей (например, подразделений одной организации), возможно также клиентами и подрядчиками данной организации. Частное облако может находиться в собственности, управлении и эксплуатации как самой организации, так и третьей стороны (или какой-либо их комбинации), и оно может физически существовать как внутри, так и вне юрисдикции владельца [6].

При использовании частного облака снижается время ожидания предоставления ресурсов для сотрудников компании потребителя облачных услуг, облачная среда способствует эффективному распределению ресурсов внутри организации, помогает динамически распределить нагрузку между физическими системами ЦОД, появляется возможность отслеживать реальное потребление ресурсов внутри компании.

Следующим вариантом развертывания является *публичное облако* - это облачная система, подготовленная поставщиком облачных услуг для *открытого* использования *несколькими* компаниями. Облако существует только на территории облачного поставщика, в отличие от частного облака, которое, наряду с этим, может также развертываться в пределах информационной системы потребителя облачных услуг.

Смешанное (гибридное) облако - совместное использование двух вышеперечисленных моделей развёртывания. Такая модель представляет собой композицию из двух или более различных инфраструктур облаков, имеющих уникальные объекты, но связанных между собой стандартизированными или собственными технологиями, которые позволяют переносить данные или приложения между компонентами.

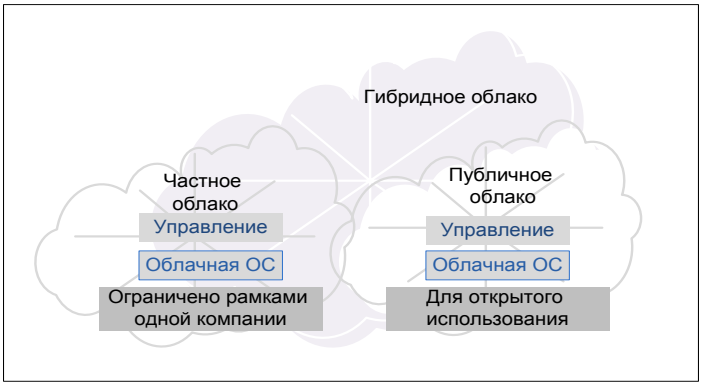


Рисунок 1.2 – Концепция гибридного облака

Использование технологий частного, публичного и гибридного облака позволяет пользователям облачных вычислений воспользоваться вычислительными мощностями и хранилищами данных, которые посредством определенных технологий виртуализации и высокого уровня абстракции предоставляются им как услуги.

Рассмотрим современные виды облачных услуг. Самые востребованные из них [7] проиллюстрированы на рисунке 1.3.

Рисунок 1.3 – Виды облачных услуг

Самый нижний уровень и наиболее простая модель развертывания облачных сервисов позволяют заказчику взять в аренду у вендора только поддерживающую инфраструктуру, которая называется IaaS.

Более сложная модель развертывания облачных вычислений охватывает уровень платформы информационной системы и получила название PaaS. Этот уровень включает в себя не только инфраструктуру, но и

некоторые сервисные службы, например операционные системы и их обслуживание.

Модель развертывания облачных сервисов, характеризующаяся наиболее полным предоставлением услуг заказчику, предполагает использование приложений из облака для работы на локальном компьютере заказчика и называется SaaS. Многие SaaS решения являются заменой традиционного программного обеспечения и формой переноса его в облачную среду

Таблица 1.2 – Современные SaaS-решения и их аналоги

Традиционное ПО	Облачное ПО
MS Outlook	Gmail, Office 365
Dynamics CRM/Oracle CRM	Saleaforce.com
1С	Эльба, Мое дело, Мой склад
MS Project	Мегаплан, Basecamp
Microsoft Office	Google Apps, Office 365

Таким образом, для потребителя облачных услуг открываются широкие возможности, позволяющие снизить требования к вычислительной мощности собственной информационной системы, а любому, сколь угодно слабому вычислительному устройству получить потенциал самого современного и дорогостоящего оборудования [8].

Рассмотрим пример архитектуры ИСОТ, реализуемого компанией IBM. С точки зрения аппаратной части облако представляет собой шасси IBM BladeCenter H с необходимым количеством серверов HS22 на Intel-архитектуре. К встроенному в шасси SAN коммутатору подключается внешняя система хранения данных DS5020, являющаяся облачным хранилищем данных. Один сервер выделен под управление облаком, компоненты которого не рекомендуется ставить как виртуальные машины гипервизора в целях безопасности. Два других используются под менее критичные средства управления облачной средой. На оставшиеся устанавливаются виртуальные машины с пользовательскими приложениями и гостевыми операционными системами. В качестве гипервизора в данной

архитектуре представлен VMware ESX. Управляющие компоненты гипервизора разделены на две части. Первые работают под управлением Windows 2003 по той причине, что VMware Virtual Center — средство управление VM Ware ESX, не поддерживает другие платформы. Эти компоненты нельзя поставить в виртуальную среду, потому что они не являются ее частью, а служат надстройкой, управляют виртуальной средой. Virtual Center позволяет быстро диагностировать проблемы с виртуальной инфраструктурой. Systems Director управляет аппаратной платформой и с помощью модуля VM Control обеспечивает надежность виртуальной среды в случае аппаратных сбоев. Большинство компонентов облака находится на внешней системе хранения данных, потому что данные должны быть доступны с нескольких серверов одновременно. Вторая группа управляющих компонентов работает под управлением гипервизора и предоставляет базовые облачные сервисы, такие как управление сервисами, управление образами программного обеспечения, разворачивание новых приложений, мониторинг, учет использования ресурсов. На рисунке 1.4 представлена общая типичная архитектура облака, предложенная в [9].

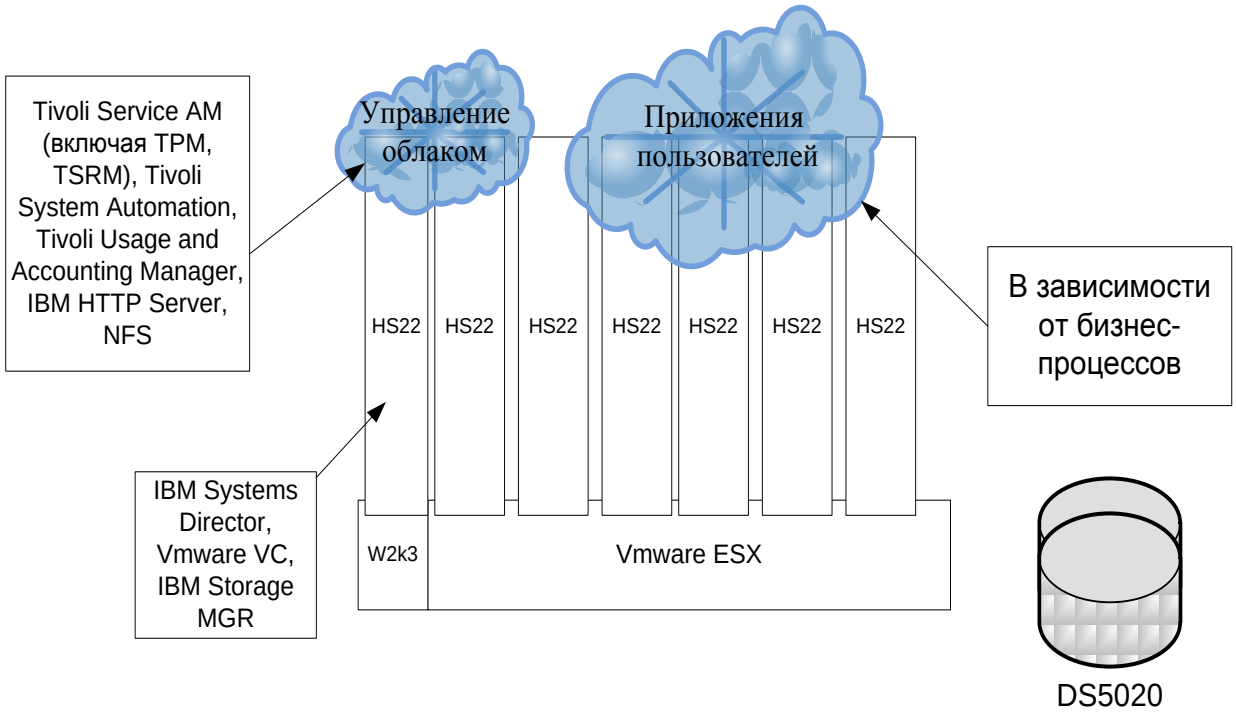


Рисунок 1.4 − Типичная архитектура облака, предложенная IBM

1.1.2 Обзор литературных источников, освещающих проблемы облачных вычислений

Облачные вычисления представляют собой важное направление в развитии современных ИТ технологий и являются эффективным решением по поддержке информационной системы для многих предприятий, так как имеют множество неоспоримых преимуществ по сравнению с традиционными средствами хранения данных [10]. Кроме того, специалисты предвидят, что многие будущие приложения, ориентированные на обработку данных, будут опираться на облачные сервисы данных [11].

Однако концепция вычислительного облака не лишена недостатков, из-за чего возникают некоторые трудности ее использования. Первым и самым важным недостатком облачных вычислений называют безопасность и приватность данных [1,11]. Согласно исследованию Forrester Research 65% мировых компаний назвали *безопасность важнейшей проблемой* при использовании модели SaaS [12]. Согласно исследованию компании Platform Computing [13] 49% респондентов обеспокоенны обеспечением безопасности в «облаках». Многие эксперты предостерегают от чрезмерного доверия заявлениям поставщиков о безопасности облачных вычислений [14**]** . Для решения проблем безопасности облачных систем нужны новые технологические решения и новые стандарты безопасности.

Второй существенной проблемой использования облачных сервисов называют отсутствие принятых стандартов в сфере облачных вычислений в РФ [12]. Сегодня предложения поставщиков даже простейших облачных сервисов практически не стандартизованы. Отсутствие стандартов затрудняет конкуренцию между поставщиками облачных услуг и не позволяет им активно развиваться, рынок таких услуг становится непрозрачным, а значит неминуемо более дорогим [15].

Кроме того, существует проблема доверия потребителя облачной услуги к данной технологии, а также доверия к самим поставщикам облачных услуг. Причин же недоверчивого отношения малого и среднего

бизнеса к центрам обработки данных, как подчеркивается в [16], может быть несколько. В общем случае это опасения лишиться контроля над ИТ-ресурсами, опасения насчет гарантии сохранности и защиты переданной информации и представление центра обработки данных лишь как площадки для размещения оборудования.

Таким образом, поставщикам сервисов облачных вычислений следует *понимать важность создания у потребителя* осведомленности об услуге, а так же уверенности в безопасности собственных данных.

Некоторые эксперты, например [17], утверждают, что облачные вычисления ведут к созданию огромной, невиданной ранее монополии. Не лишено смысла то, что на рынке облачных вычислений для заказа на какую-либо облачную услугу, в отношении которой существуют правила информационной безопасности, компании будут скорее использовать поставщиков, которым доверяют они и их партнеры по бизнесу. Таким образом, существует определенная опасность того, что все вычисления и данные будут агрегированы в руках одной сверхмонополии. Однако на данный момент на рынке уже существуют несколько компаний с примерно одинаковым высоким уровнем доверия со стороны клиентов (Microsoft, Google, Amazon), и нет никаких фактов, которые бы указывали на возможность доминирования одной компании. Поэтому в ближайшем будущем появление глобальной сверхкомпании, которая будет координировать и контролировать все вычисления в мире, очень маловероятно, хотя одна лишь возможность зависимости от поставщика облачных услуг ставит под вопрос решение использования облачных вычислений потребителями.

Есть также проблема, связанная с тем, что центры обработки данных одной компании могут располагаться в разных странах и даже на разных континентах. Государство, на территории которого размещен центр обработки данных поставщика облачных услуг, может получить доступ к любой информации, которая в нем хранится. Например, по законам США,

где на сегодняшний день находится самое большое количество центров обработки данных, компания-поставщик даже не имеет права разглашать факт передачи конфиденциальной информации кому-либо, кроме своих адвокатов [18]. Эта проблема является одной из самых существенных в вопросе обработки конфиденциальной информации в облачной среде [19].

В результате анализа литературных источников и публикаций, освещающих проблемы облачных вычислений, можно сделать вывод, что на сегодняшний день проблемы, связанные с информационной безопасностью облачных сред являются одними из самых важных и трудно решаемых.

1.2 Анализ существующих стандартов и нормативных правовых документов в области информационной безопасности облачных сред

Деятельность специалистов по защите информации в процессе обеспечения безопасности информационных ресурсов в информационной системе, построенной на основе облачных технологий, должна подкрепляться соответствующими нормативными правовыми документами.

На сегодняшний день отечественные стандарты, которые регламентировали бы проектирование и эксплуатацию информационных систем на основе облачных технологий (ИСОТ), а также, на основе которых можно строить систему обеспечения информационной безопасности для облачных сред, находятся в процессе разработки. В настоящее время согласно планам ТК 362, указанным на портале Росстандарта [33], в стадии планирования редактирования, подготовки и разработки находятся ряд проектов стандартов, среди которых ГОСТ Р «Защита информации. Защита информации при использовании облачных технологий. Общие положения», а также ГОСТ Р «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие

положения», исполнителем которых согласно плану является ФАУ "ГНИИИ ПТЗИ ФСТЭК России". Так же существует методический документ «Меры защиты в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014г., в котором вскользь упоминаются облачные вычисления, как перспективная область развития информационных технологий.

Стандарт [2] устанавливает требования по технической защите информации от несанкционированного доступа в информационных системах, построенных с использованием облачных технологий. Особое внимание уделяется терминам и определениям, таким как «облачные вычисления», «облачные ресурсы», «облачная услуга» и т.д., появившимся впервые в терминологии облачных сред. Так же здесь приведено огромное количество видов облачных услуг, среди которых есть и как общеизвестные, как SaaS, PaaS и IaaS, так и облачные услуги, которые распространены не так широко. Среди таких услуг, например, можно отметить такие как SecaaS (безопасность как услуга) или TaaS (доверие как услуга).

В пятом разделе настоящего стандарта содержится список защищаемых объектов в облачной среде и перечень угроз безопасности облачным вычислениям. В качестве основных объектов защиты указаны информационные ресурсы и носители информации в облаке, физические и виртуальные устройства обработки данных, служебная информация физических и виртуальных машин облака, каналы передачи данных, системное и прикладное программное обеспечение, сетевые службы, резервные копии данных гипервизоры, средства защиты информации и т.д.

Шестой раздел документа содержит требования по защите информации при оказании облачных услуг, то есть требования предъявляются именно к владельцу облака (поставщику облачных услуг). При этом требования расписаны для *каждого* типа услуг. В каждом разделе с требованиями приведено описание услуги, угрозы безопасности, характерные для

конкретной услуги и меры по защите информации с расстановкой по разделам.

К недостаткам данного стандарта можно отнести то, что он не содержит список конкретных требований к средствам защиты информации, которые могут быть установлены в ИСОТ.

В июле 2015 года предложен порядок использования услуг облачных вычислений в деятельности органов государственной власти [34]. Данный порядок регламентирует проект Федерального закона «О внесении изменений в отдельные законодательные акты РФ в части использования облачных вычислений».

По мнению разработчиков законопроекта, использование облачных технологий обеспечивает:

- повышение эффективности использования вычислительных ресурсов органов и организаций;

- сокращение расходов на приобретение ИТ-оборудования, его техническое обслуживание и ремонт, программное обеспечение, оплату труда обслуживающего персонала, а также расходов на электроэнергию;

- повышение управляемости ИТ-инфраструктуры, гибкости и скорости реагирования системы;

- обеспечение бесперебойной работы органов и организаций благодаря системе резервного копирования и миграции виртуальных сред.

Законопроектом предлагается внести изменения в Федеральный закон "Об информации, информационных технологиях и о защите информации" в части определения основных понятий, используемых при организации предоставления услуг облачных вычислений, условий использования облачных вычислений, способов организации предоставления облачных услуг, ответственности сторон и иные.

Проект также содержит положения, определяющие специфику организации предоставления облачных услуг органам власти, включая квалификационные требования к поставщикам услуг облачных вычислений,

требования к финансовой устойчивости соответствующих поставщиков, а также к защите информации, обрабатываемой такими поставщиками и порядок тарифного регулирования цен на услуги облачных вычислений.

Одновременно законопроектом предлагается внести изменения в Федеральный закон "О персональных данных" в части обеспечения защиты персональных данных при осуществлении их обработки в облачной среде.

Проект ГОСТ Р XXXXX-20XX «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Основные положения» [35], был разработан ФАУ "ГНИИИ ПТЗИ ФСТЭК России". Данный стандарт рассматривает требования по защите виртуализации во всех аспектах. В первой части документа приведена общая информация, указывается, что стандарт касается только виртуализации и является дополнительным требованием при использовании виртуализации. В третьем разделе "Термины и определения" даны четкие определения терминам "виртуализация", "виртуальная машина", "гипервизор" и другим, стандарт заполнит пробелы в терминологии, возникшие после появления данных терминов в 21/17 приказах ФСТЭК.

В пятом разделе приводится перечень объектов, подлежащих защите. К таким объектам относятся:

− файлы виртуальных жестких дисков и файлы с настройками виртуальных машин;

− гипервизоры;

− системное и прикладное ПО, используемое в виртуализации, и их данные;

− средства ЗИ и их данные;

− каналы передачи данных;

− сетевое оборудование и их данные;

− резервные копии данных.

В шестом разделе перечислены основные требования по защите информации при использовании каждого из шести перечисленных в ГОСТ

типов виртуализации. По каждому из типов виртуализации приводится описание типа виртуализации, описание угроз безопасности информации и перечень мер по защите.

Однако, не смотря на то, что в нашей стране нормативная правовая база, регламентирующая отношения в ИСОТ, находится в стадии становления, зарубежные специалисты уже разработали ряд требований для системы облачных вычислений, ее развертывания и безопасности.

Стандартная архитектура системы облачных вычислений описана в американском стандарте NIST (National Institute of Standards and Technology − Национальный Институт стандартов и технологий США).

Цель этого стандарта состоит в том, чтобы четко описать разделение систем облачных вычислений или облачных систем на пять значимых сценариев и, для каждого из этих сценариев, объяснить основные аспекты, требующие внимания или вызывающие споры, и как эти аспекты адресуются в отношении каждого из сценариев [36].

Как это предполагается в определении облачных вычислений NIST, облачная система является коллекцией ресурсов, доступных по сети для заказчиков (в соответствии с [2] – потребителей облачных услуг).

Стандарт NIST предлагает следующие обязательные утверждения для системы облачных вычислений, в независимости от модели ее развертывания или сервисной модели:

• *Зависимость от сети – потребители облачного сервиса*, нуждаются в работающем и защищенном сетевом доступе к облаку. Если сеть ненадежна, облако не будет считаться надежным с точки зрения потребителя.

• *Потребители должны обладать навыками работы в информационных технологиях* − эксплуатируя серверные компьютеры в своей системе, поставщик облачных услуг может уменьшить потребность организаций-потребителей в персонале, обслуживающем информационную систему организации. Однако потребители будут осуществлять доступ в

облако со своих клиентских систем, требующих управления, сопровождения, поддержки, обеспечения безопасности, что также требует сопровождения со стороны потребителя.

- *Место выполнения рабочих нагрузок назначается динамически и скрыто от клиентов* – для эффективного управления облачными аппаратными ресурсами поставщики должны быть способны распределять рабочие нагрузки клиентов между машинами без необходимости требований к потребителям отслеживать и адаптироваться к такого рода изменениям и без извещения о произведенных изменениях.

- *Риски множественной аренды* – вычислительные процессы различных потребителей могут выполняться одновременно на одних и тех же облачных системах и локальной сети, будучи разделенными только с помощью политик доступа, определенных на уровне программного обеспечения поставщика. Уязвимости в этом программном обеспечении или в политиках могут нанести урон безопасности потребителей.

- *Импорт/экспорт данных и ограничения возможности их выполнения* − в силу того, что потребители осуществляют доступ к «облаку» по сети, требуемые временные характеристики пакетного импорта и экспорта данных могут превысить возможности сети. Кроме того, работа в режиме реального времени или обработка критически важных запросов могут оказаться проблематичными из-за сетевых задержек и других ограничений [35].

В определении облачных вычислений NIST описывается четыре модели развертывания: частное облако (private), облако сообщества (community), публичное облако (public), и гибридное облако (hybrid). Различные модели развертывания облаков, подразумевают размещение контролируемого клиентом периметра безопасности и, следовательно, уровень контроля, который подписчики могут осуществлять в отношении ресурсов, доверяемых облаку

Что касается *информационной безопасности*, на сегодняшний день лучшим *экспертом* в этой сфере является Cloud Security Alliance (CSA). Эта организация выпустила и недавно обновила руководство, включающее описание сотни нюансов и рекомендаций, которые необходимо принимать во внимание при *оценке рисков в облачных вычислениях* [36].

Всего эксперты Cloud Security Alliance обозначили 7 категорий рисков ИБ: неправомерное использование облачных сервисов, незащищенные интерфейсы прикладного программирования, деятельность сотрудников компании — поставщика услуг, уязвимости разделяемой среды, потеря или утечка данных, кража учетных данных, неизвестные и не выявленные риски.

Неправомерное использование облачных сервисов связано с несовершенством механизмов регистрации и аутентификации пользователей, что дает возможность как использования соответствующих ресурсов без оплаты услуг, так и возможность использования их для противоправной деятельности (рассылка спама, атаки, размещение вредоносного кода, обхода механизмов защиты и т. д.). По мнению экспертов, наиболее уязвимы сервисы IaaS и PaaS. В качестве мер противодействия рекомендуется вводить строгие правила начальной регистрации, использовать средства мониторинга и анализа сетевого трафика клиентов, отслеживать информацию фрод-мониторинга платежных систем и публичных черных списков IP-адресов.

Уязвимости в интерфейсах прикладного программирования обычно связаны с их доработкой поставщиками услуг. Это делается для того, чтобы предоставлять дополнительные сервисы, но побочным эффектом является повышение сложности API и различным рискам. Этот риск касается всех типов сервисов, включая SaaS, IaaS и PaaS. В качестве мер противодействия рекомендуется применять такие средства как анализ подходов обеспечения безопасности программных интерфейсов, обеспечение строгой аутентификации и контроля доступа, применение средств шифрования

трафика, а также анализ цепочек зависимостей, связанных с интерфейсами прикладного программирования.

Деятельность сотрудников компании-поставщика услуг также может представлять угрозу. Это связано с сосредоточением в одном месте множества ИТ-сервисов, работающих под единым управлением в интересах различных заказчиков, причем процессы и процедуры поставщика часто непрозрачны для его заказчиков.

При этом персонал теоретически имеет полный доступ к данным и прочим ресурсам поставщика, что создает риск несанкционированного доступа, причем обнаружить его может оказаться сложно или даже вовсе невозможно.

Данный риск также касается всех типов сервисов, включая SaaS, IaaS и PaaS. В качестве контрольных мер рекомендуется провести детальную оценку уровня обеспечения безопасности в компании-поставщике в контексте вопросов, связанных с персоналом, внести требования к персоналу в договор обслуживания, требовать от поставщика предоставления всей актуальной информации о подходах и практиках корпоративного управления и соответствия требованиям.

Риски условий разделяемой среды, связаны с тем, что не всегда возможно обеспечить надежную изоляцию сред, принадлежащих разным клиентам. Данная уязвимость касается IaaS сервисов. В качестве контрольных мер рекомендуется осуществлять инсталляцию и конфигурирование в соответствие с лучшими практиками, внедрить средства мониторинга, позволяющие выявлять несанкционированную активность, использовать средства строгой аутентификации и контроля доступа, внести в договоры положения, регламентирующие своевременную установку обновлений и исправлений ПО, регулярно проводить сканирование на наличие уязвимостей и анализ конфигураций.

Наиболее вероятной причиной утечки данных ИСОТ являются несанкционированный доступ, в результате нарушения порядка вывода

из эксплуатации носителей информации, а также вследствие политических рисков. Данные уязвимости характерны для всех классов сервисов. В качестве контрольных мер рекомендуется контролировать доступ к интерфейсам прикладного программирования, шифровать данные и контролировать их целостность при передаче, анализировать средства защиты данных как на этапе проектирования, так и в ходе эксплуатации, требовать от поставщика неукоснительного соблюдения регламентов уничтожения информации при выводе оборудования из эксплуатации, а также определить порядок резервного копирования данных.

Кража учетных данных может произойти вследствие мошенничества, с использованием фишинга, вредоносного ПО, а также при реализации уязвимостей в оборудовании и ПО. В качестве контрольных мер рекомендуется не допускать использования общих учетных записей, использовать средства многофакторной аутентификации, вести мониторинг несанкционированной активности, анализировать политики безопасности поставщика.

Неизвестные риски связаны с тем, что клиент не обладает полной информацией об облачной среде, и, следовательно, не обладает всей полнотой информации о рисках информационной безопасности. В качестве контрольных мер рекомендуется требовать от поставщика информации об инфраструктуре, включая версии ПО, наличие средств защиты, данных журналов, внедрение средств мониторинга событий и управления инцидентами [37].

Еще одной организацией, деятельность которой затрагивает аспекты безопасности в облаке, выступает Trusted Computing Group (TCG). Она является автором нескольких стандартов в этой и других сферах, в том числе широко используемых сегодня Trusted Storage, Trusted Network Connect (TNC) и Trusted Platform Module (TPM) [36].

Целям стандартизации облаков служат также спецификации, подготавливаемые двумя недавно созданными рабочими группами IEEE.

Участники групп ставят своей задачей создание универсальных стандартов переносимости, управления и интероперабельности облачных платформ.

Целям стандартизации облаков служат также спецификации, подготавливаемые двумя созданными рабочими группами IEEE. Участники групп ставят своей задачей создание универсальных стандартов переносимости, управления и интероперабельности облачных платформ [38]. IEEE P2301 — будет содержать перечни стандартов и спецификаций, необходимых для создания совместимых облачных систем, а — IEEE P2302 — включит в свой состав базовые сведения и рекомендации по переносимости в «облака».

Таким образом, проведенный анализ существующих стандартов и нормативных правовых документов в области информационной безопасности облачных сред показал, что принятые специализированные отечественные стандарты по данной тематике отсутствуют, проекты ГОСТ на данный момент не имеют юридической силы и не могут быть использованы для построения систем защиты облачных вычислений, а также для проведения аудита информационной безопасности. Зарубежные стандарты, посвященные безопасности в облачных вычислениях, в настоящий момент активно используются рядом стран, однако они не являются общепринятыми нормативными правовыми актами в РФ и не могут применяться для построения систем обеспечения информационной безопасности облаков.

1.3 Выявление проблем обеспечения информационной безопасности в облачных средах

Как уже отмечалось ранее, сегодня в ИТ-индустрии можно наблюдать стремительные темпы развития облачных вычислений, однако при этом не достаточно широко освещается проблема использования облачных сервисов

с точки зрения информационной безопасности. Концепция вычислительного облака является отражением всеобщей тенденции глобализации информационных систем, которая, однако, сопровождается расширением перечня информационных *угроз*, появлением *новых,* ранее *неизвестных уязвимостей*, совершенствованием способов реализации информационных атак [20].

Многие эксперты предостерегают от чрезмерного доверия заявлениям поставщиков о безопасности облачных вычислений [21], так как широко распространено мнение, что потребитель облачных услуг имеет тот уровень защищенности в облачной среде, который обеспечивается поставщиком [1, 22]. Чтобы убедить потребителя облачных услуг в сохранности его конфиденциальной информации, хранящейся в облачной среде, существующая система обеспечения информационной безопасности «облака» должна периодически подвергаться независимому *экспертному аудиту*, который в соответствии с требованиями международных стандартов, является одним из обязательных этапов жизненного цикла любой информационной системы [23].

Что касается создания защищенной среды облачных сервисов, то данная проблема обостряется отсутствием не только в России, но и за рубежом общепринятых стандартов обеспечения информационной безопасности для облачных вычислений [22]. В США ассоциация Cloud Security Alliance выпустила Cloud Controls Matrix. Этот документ представляет собой перечень существующих технологий информационной безопасности, которые могут быть использованы в облачных сервисах [24]. Хотя некоторые специалисты считают, что для управления ИБ при построении облака SaaS могут быть использованы стандарты ISO 27001 и ISO 27002 [25], все же необходима разработка специальных стандартов для облачных вычислений.

Кроме того, в различных странах действуют разные законы в области безопасности данных и защиты конфиденциальной информации, а

поставщики облачных услуг могут иметь облачные хранилища данных физически расположенные удаленно друг от друга, вплоть до расположения на разных континентах [26]. Соответственно, можно нарушить законодательство страны, в которой поставщиком было развернуто хранилище, соблюдая законодательство другой страны, совершенно непреднамеренно.

Использование средств виртуализации в облачной среде позволяет сократить затраты на инфраструктуру облака и позволяет достичь гибкой масштабируемости всей системы. Однако использование виртуализации и переход к облачным средам посредством виртуализации приводят к появлению принципиально новых угроз [1]. Для облачных сред угрозы удаленного взлома и заражения вредоносным кодом весьма значимы из-за параллельного существования множества виртуальных машин. Отличительной *особенностью* виртуальной машины, которую нужно учитывать, является возможность ее заражения в *выключенном* состоянии [1, 27], если есть доступ к хранилищу образов виртуальных машин через сеть «Интернет». Поэтому особое внимание должно быть уделено *частным политикам безопасности,* особенно политикам разграничения доступа, информационных систем, построенных на основе технологий облачных вычислений.

Кроме того, проблема обеспечения безопасности в облачной среде связана с *постоянной изменчивостью* виртуальной машины (перемещение между физическими серверами). Определенную сложность создает процедура *взаимной аутентификации* потребителей и поставщиков облачных услуг, так как серверов может быть несколько, они передают данные с одного узла на другой [28].

Некоторые проблемы возникают и в процессе интеграции антивирусного программного обеспечения в облачные виртуальные среды. Для обеспечения работы традиционного антивирусного решения необходимы большие вычислительные ресурсы. Установка антивируса на каждую

виртуальную машину потребует затрат большого количества оперативной памяти и ресурсов процессоров [25,22].

Также стоит отметить, что специализированные средства обеспечения информационной безопасности, которые применяются в современных информационных системах, снижают эффективность и скорость обработки информации клиента в облаке, а облачные продукты безопасности, помогающие преодолеть эту проблему, в настоящее время не сертифицированы ФСТЭК и ФСБ [29,30].

Потребитель облачных услуг не обладает полной информацией об облачной среде, ее инфраструктуре и местоположении центра обработки данных, где обрабатывается критичная для потребителя информация, и, следовательно, не обладает всей полнотой информации о рисках информационной безопасности всей системы в целом. В связи с этим, при заключении контракта между поставщиком и потребителем облачных услуг рекомендуется требовать от поставщика информацию об инфраструктуре, включая версии ПО, наличие средств защиты, данных журналов регистрации опасных событий [36]. Однако, поставщик может не согласится на данное условие, мотивируя это соображением безопасности других потребителей ИСОТ. Компромиссом между поставщиком и потребителем здесь может выступать внедрение средств мониторинга событий и управления инцидентами [36], что позволило бы оценить риск нарушения информационной безопасности ИСОТ в реальном масштабе времени, когда угроза проявляется по конкретному пути распространения к конкретному критичному объекту определенного потребителя.

Информационная безопасность должна обеспечиваться на всей цепочке, включая поставщика облачного решения, потребителя и связывающих их коммуникаций [24,28]. Потребитель облачных услуг обязан вводить в своей системе соответствующую *политику безопасности*, исключающую передачу прав доступа к информации, предоставленной поставщиком, третьим лицам. Облака не отменяют необходимости

разработки и внедрения политики безопасности в *сегменте потребителя* и использования сервисов безопасности, призванных гарантировать защиту пользовательских рабочих мест на *стороне потребителя* облачных услуг.

Уровень же применяемых подходов и средств защиты как со стороны поставщика, так и со стороны потребителя должен определяться исходя из *критичности* облачных приложений для обеспечения бизнес-процессов потребителя облачных услуг.

В результате анализа выявлены следующие проблемы обеспечения информационной безопасности в облачных средах:

− появление наряду с рисками нарушения информационной безопасности, присущими любой традиционной информационной системе, рисков, связанных с особенностями технологии облачных вычислений;

− отсутствие в РФ нормативной правовой базы, регулирующей вопросы обеспечения информационной безопасности для облачных вычислений;

− применение средств обеспечения информационной безопасности, которые широко используются в современных информационных системах, снижает эффективность и скорость обработки информации заказчика облачных услуг в облачной инфраструктуре, что сводит на «нет» почти все достоинства облачных сред, по сравнению с традиционными информационными системами;

− специализированные облачные продукты безопасности, учитывающие особенности облачных сред, в настоящее время практически не сертифицированы ФСТЭК и ФСБ;

− вопреки общепринятому мнению, что сохранность информации в «облаке» полностью зависит от поставщика облачных услуг, информационная безопасность должна обеспечиваться на всей цепочке, включая поставщика облачного решения, потребителя и связывающих их коммуникаций;

− потребитель, заключая договор на предоставление облачных услуг, должен требовать от поставщика внедрения средств мониторинга событий и управления инцидентами, что позволило бы оценить риск нарушения информационной безопасности ИСОТ в реальном масштабе времени, когда угроза проявляется по конкретному пути распространения к конкретному критичному объекту определенного потребителя;

− существующая система обеспечения информационной безопасности облачной среды должна периодически подвергаться независимому *экспертному аудиту*, который в соответствии с требованиями международных стандартов, является одним из обязательных этапов жизненного цикла любой информационной системы.

1.4 Анализ проблемы проведения аудита информационной системы, построенной на основе технологии облачных вычислений

1.4.1 Обзор современных источников литературы, посвященных аудиту информационной безопасности

Согласно [40] термин «аудит» означает независимую экспертизу отдельных областей функционирования организации. В [40] различается два вида аудита: внешний и внутренний. Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров.

Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием. Внутренний аудит представляет собой *непрерывную* деятельность, которая осуществляется на основании принятого в организации «Положения о внутреннем аудите» и в соответствии с планом,

подготовка которого осуществляется подразделением внутреннего аудита и утверждается руководством организации.

Аудит безопасности информационных систем является одной из составляющих ИТ аудита [41]. Исходя из [43,44] целями проведения аудита безопасности могут являться:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС
- оценка *текущего* уровня защищенности ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

В [44] отмечается, что аудит является основным инструментом оценки эффективности корпоративной системы безопасности и ее соответствия потребностям бизнеса, а также оптимизации и планирования затрат на обеспечение информационной безопасности предприятия.

Аудит информационной безопасности, в свою очередь, один из важнейших этапов построения надежной системы защиты информации любой компании. В [45] вводится понятии комплексной аудиторской проверки, которая позволяет увидеть полную картину состояния ИБ в компании, локализировать имеющиеся проблемы и слабые места системы защиты информации и разработать эффективную программу построения системы информационной безопасности на предприятии.

Понятие «комплексный аудит информационной безопасности», согласно [45], может быть детализирован, как показано на рисунке 1.5.

Рисунок 1.5 – Детализация понятия «Комплексный аудит информационной безопасности»

В [45] приводятся этапы работ по проведению аудита безопасности информационных систем (см. рисунок 1.6).

Рисунок 1.6 – Этапы проведения аудита информационной безопасности

Согласно [43] используемые аудиторами методы анализа данных определяются выбранными подходами к проведению аудита, которые могут *существенно различаться*.

В [2, 46] описываются два подхода к проведению аудита информационной безопасности ИС.

Первый подход, базируется на *анализе рисков* нарушения информационной безопасности. Опираясь на методы анализа рисков, аудитор определяет для обследуемой ИС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной ИС, среды ее функционирования и существующие в данной среде угрозы безопасности. Данный подход является наиболее трудоемким и требует наивысшей квалификации аудитора. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками и ее применимость к данному типу ИС. Однако, как отмечается в [18] на данный момент отсутствует методология анализа рисков нарушения ИБ, которая была бы применима для ИСОТ, то есть, учитывала специфику данного объекта защиты.

Второй подход опирается на использование стандартов в области информационной безопасности. Стандарты определяют базовый набор требований безопасности для широкого класса ИС, который формируется в результате обобщения мировой практики. Стандарты могут определять разные наборы требований безопасности, в зависимости от уровня защищенности ИС, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т.п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для данной ИС. Необходима также методика, позволяющая оценить это соответствие. Из-за своей простоты (стандартный набор требований для проведения аудита уже заранее определен стандартом) и надежности, описанный подход наиболее

распространен на практике (особенно при проведении внешнего аудита). Он позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии ИС.

Однако, как отмечается в [43] подход к проведению аудита ИБ, основанный на соответствии стандартам и нормативным правовым документам, имеет существенный недостаток: некоторые требования стандарта могут не учитывать специфику исследуемого объекта аудиторской проверки.

Кроме того, в [45] отмечается, что на сегодняшний день большинство компаний сталкиваются с проблемой оценки необходимого уровня инвестиций в ИБ для обеспечения адекватной защищенности информации. Для решения этой задачи рекомендуется проводить не только аудит на соответствие стандартам, но проводить регулярную оценку и анализ рисков, что позволит выбрать оптимальный по эффективности вариант защиты по соотношению существующих в информационной системе рисков/затрат на ИБ.

Что касается информационных систем, отечественные нормативные документы, для которых находятся в стадии разработки (такие как ИСОТ), то единственным способом проведения объективной аудиторской проверки таких систем на сегодняшний день является аудит, основанный на оценке рисков нарушения информационной безопасности.

1.4.2 Анализ существующих стандартов и нормативных правовых документов в области аудита информационной безопасности

В настоящем разделе проводится анализ стандартов информационной безопасности, являющихся наиболее значимыми и перспективными с точки зрения их использования для проведения аудита безопасности ИСОТ с помощью оценки рисков нарушения информационной безопасности.

На сегодняшний день разработано несколько стандартов, посвященных процессному подходу к организации управления рисками, среди которых стоит отметить американский стандарт NIST SP 800-30:2002 [47] и британский стандарт BS 7799-3:2006, а также ISO 17799 и ISO 15408 [48]. Основные положения стандартов NIST SP 800-30:2002 и BS 7799-3:2006 учтены в стандарте ИСО/МЭК 27005-2010 [49]. Сравнительный анализ BS 7799-3 и NIST SP 800-30:2002 показал идентичность изложенных в них подходов к анализу, оценке и управлению рисками [50].

Стандарт ISO 17799 является полной копией британского BS 7799-3 [51], стандарты ISO 17799 и ISO 15408 служат основой для проведения любых работ в области информационной безопасности, в том числе и аудита. ISO 17799 сосредоточен на вопросах организации и управления безопасностью, в то время как ISO 15408 определяет детальные требования, предъявляемые к программно-техническим механизмам защиты информации.

Среди зарубежных стандартов существует также спецификация SysTrust. Данная спецификация в настоящее время достаточно широко используется аудиторскими компаниями, традиционно выполняющими финансовый аудит для своих клиентов и предлагающих услугу аудита информационной безопасности в качестве дополнения к финансовому аудиту [52].

ГОСТ Р ИСО/МЭК 27005 – 2010 представляет собой руководство по менеджменту риска информационной безопасности в организации, поддерживая, в частности, требования к системе менеджмента информационной безопасности (СМИБ) в соответствии с ИСО/МЭК 27001.

Стандарт предназначен для адекватного обеспечения информационной безопасности на основе системного подхода, связанного с менеджментом риска, который необходим для того, чтобы идентифицировать потребности организации, касающиеся требований ИБ и создать эффективную систему менеджмента ИБ. Согласно стандарту, риск

информационной безопасности − это возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации [53].

До принятия решения о том, что и когда должно быть сделано для снижения риска до приемлемого уровня, в рамках менеджмента риска анализируется, что может произойти, и какими могут быть возможные последствия.

Согласно стандарту [53], процесс менеджмента рисков информационной безопасности может носить *итеративный* характер для таких видов деятельности, как оценка риска и/или обработка риска, что позволяет увеличить глубину и детализацию оценки при каждой итерации.

Стандарт допускает использование *качественных* и *количественных* методов оценки рисков. Оценивание риска проводится путем его вычисления и сопоставления с *заданной шкалой*, с учетом значимости бизнес-процесса или деятельности для организации.

Стандарт ГОСТ Р ИСО/МЭК 27007 – 2014 предоставляет собой руководство по проведению аудитов и по определению компетентности аудиторов системы менеджмента информационной безопасности. Данный ГОСТ применим для тех организаций, которые нуждаются в понимании или проведении внутренних или внешних аудитов системы менеджмента информационной безопасности или осуществлении менеджмента программы аудита системы менеджмента информационной безопасности.

В стандарте отдельно подчеркивается, что для успешного проведения аудита информационной безопасности должна быть разработана программа аудита, основанная на ситуации, связанной с риском информационной безопасности проверяемой организации. Причем, под программой аудита понимается совокупность мероприятий по проведению одного или нескольких аудитов, запланированных на конкретный период времени и направленных на достижение конкретной цели.

На основе изучения ГОСТ Р ИСО/МЭК 27007 – 2014 составлено описание типовой аудиторской деятельности в области информационной безопасности, приведенное на рисунке 1.7.

Рисунок 1.7 − Описание типовой аудиторской деятельности в области информационной безопасности

При осуществлении аудиторской проверки на основе оценки рисков, стандарт требует определения подхода и метода для оценки риска. Хотя в стандарте не указан какой-то определенный подход к оценке рисков.

Согласно стандарту, аудитор должен проверить и подтвердить, что выбранный подход к оценке риска реализован с целью идентификации рисков бизнес-процессов и принятия соответствующих мер в отношении рисков.

Аудитор должен осознавать, что для оценки риска нарушения информационной безопасности существуют количественные и качественные методы или любые их комбинации, а решение о том, какой подход использовать, зависит от организации.

Также аудитор должен подтвердить, что результаты оценок риска, полученные в соответствии с подходом к оценке риска, сопоставимы и воспроизводимы. Иными словами, аудитор должен подтвердить, что подход позволяет любым сотрудникам, отвечающим за оценку риска, придти к одинаковым результатам независимо от того, кто и когда проводит оценку риска, при условии, что они обладают определенным уровнем компетентности в сфере оценки риска нарушения ИБ и проводят оценки одних и тех же активов в соответствии с процессами и процедурами, определенными в выбранном методе оценки риска.

ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» содержит рекомендации по выбору и применению методов оценки риска. В настоящем стандарте представлены методы оценки риска и даны ссылки на другие международные стандарты, в которых более подробно описано применение конкретных методов оценки риска. Отдельным пунктом в стандарте значатся факторы, влияющие на выбор метода оценки риска: сложность проблемы и методов, необходимых для анализа риска; необходимые ресурсы: временные, информационные и т.д.; возможность получения количественных оценок выходных данных.

В качестве некоторых методов, предложенных в ГОСТ Р ИСО/МЭК 31010-2011 можно выделить:

− *метод PHA.* Входными данными является информация об оцениваемой системе, доступные и относящиеся к делу детали проекта

системы. Выходные данные: перечень опасностей и соответствующего риска, рекомендации по принятию риска, рекомендуемые средства управления, требования к конструкции или запрос на выполнение более детальной оценки. Вид оценки по методу: качественный. Преимущество метода: позволяет исследовать риск на самых ранних стадиях жизненного цикла системы. Недостаток метода: не является всесторонним методом и не может обеспечить подробную информацию об опасных событиях и способах их предотвращения;

− *метод HACCP.* Входными данными является технологические карты или блок-схемы процесса и сбора информации об опасных событиях. Выходные данные: карта анализа опасностей (оценка значимости риска данных опасностей), заключение о значимости совокупного риска; возможные предупреждающие действия для каждой опасности. Вид оценки по методу: качественный. Преимущество метода: представляет собой структурированный процесс, который обеспечивает документированные свидетельства качества идентификации опасности, управления и снижения риска. Недостаток метода: для применения метода HACCP необходимо, чтобы опасности были идентифицированы и определен соответствующий им риск;

− *причинно-следственный анализ.* Входными данными являются результаты экспертизы, опыт участников рабочей группы, ранее разработанные модели, использованные в предыдущих исследованиях. Выходные данные: диаграммы или древовидные схемы, которые показывают возможные причины исследуемого события. Вид оценки по методу: качественный. Преимущество метода: привлечение компетентных экспертов в работу группы, применение структурированного анализа, графическое отображение результатов в простой для восприятия форме. Недостаток метода: группа экспертов может не иметь необходимой компетентности, - для разработки рекомендаций метод необходимо применять только как часть анализа первопричины;

− *метод LOPA*. Входными данными является основная информация о риске, включая опасности, причины и последствия, частота причинных событий, оценки вероятности отказа барьеров защиты, оценки последствий и допустимого риска; частота инициирующих причин, оценки вероятности отказа барьеров защиты, оценки последствий и допустимого риска. Выходные данные: рекомендации относительно дальнейшего применения средств управления и их эффективности для снижения риска. Вид оценки по методу: количественный. Преимущество метода: помогает идентифицировать наиболее критичные барьеры защиты и обеспечить их ресурсами, помогает идентифицировать операции, системы и процессы с недостаточным уровнем защитных мер. Недостаток метода: неизвестен метод нахождения исходных данных.

К сожалению, в ходе анализа настоящего стандарта выяснилось, что ни один из предложенных в ГОСТ методов не удовлетворяет полностью всем факторам, влияющим на выбор метода оценки рисков.

1.4.3 Обзор известных методов и средств автоматизации аудита информационной безопасности и расчета рисков нарушения ИБ

Применение средств автоматизации аудита информационной безопасности позволяет оценить степень защищенности информационной системы организации и существующие в системе риски нарушения ИБ. Необходимость проведения аудита информационной безопасности обуславливается возможностью оценить правильность выбора рационального набора средств защиты информации при соблюдении принципа разумной достаточности. Программные продукты, предлагаемые на рынке, условно могут быть разделены на две группы: программное обеспечение (ПО), ориентированное на базовый уровень информационной безопасности, и программное обеспечение полного анализа рисков [54].

ПО базового уровня информационной безопасности.

Применение каких-либо инструментальных средств не является обязательным для предприятия, однако оно позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время на рынке есть около десятка программных продуктов для анализа и управления рисками базового уровня безопасности.

Примером инструментария базового уровня является ***система COBRA*** (Consultative Objective and Bi-Functional Risk Analysis), разрабатываемая компанией Risk Associates.

Британская система *COBRA* представляет собой продукт, позволяющий аудитору провести проверку как на соответствие информационной системы требованиям международных стандартов, так и оценить риск нарушения информационной безопасности системы [55]. COBRA реализует методы количественной оценки рисков, а также позволяет формализовать и ускорить процесс проверки на соответствие режима информационной безопасности требованиям Британского стандарта BS 7799 (ISO 17799). Имеется несколько баз знаний: общие требования BS 7799 (ISO 17799) и специализированные базы, ориентированные на различные области применения [54].

Этот программный продукт может применяться при проведении аудита ИБ или для работы специалистов служб, ответственных за обеспечение информационной безопасности. Простота, соответствие международному стандарту, сравнительно небольшое число вопросов позволяют легко адаптировать этот метод для работы в отечественных условиях.

Недостатки метода:

- отсутствие возможности установки пользователем весов на каждое требование безопасности при расчете значения риска;
- отсутствие русскоязычной версии;
- возможна нестабильность системы при работе с отчетом под Win2000 и выше.

Еще один метод, условно относящийся к базовому уровню, − **RA Software Tool** − базируется на британском стандарте BS 7799, части 1 и 2, на методических материалах Британского института стандартов (BSI) PD 3002, PD 3003, PD 3005, а также стандарте ISO 13335, части 3 и 4.

Недостатки инструментального средства:

- возможность проверить систему лишь на соответствие стандартам, отсутствие возможности численного оценивания риска;
- аудит информационной безопасности системы проводится лишь в соответствии с международными британскими стандартами и другими нормативными документами зарубежных стран;
- отсутствие русскоязычной версии.

Средства полного анализа рисков нарушения ИБ.

Для автоматизации процедуры проведения аудита информационной безопасности с помощью оценки риска разработаны программные продукты, построенные с использованием структурных методов системного анализа. В настоящее время на рынке представлено несколько программных продуктов этого класса [56].

Метод и программное средство **CRAMM** – это универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач.

К **недостаткам** метода, реализованного в программном средстве CRAMM можно отнести следующее:

- использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора ИБ;
- CRAMM в гораздо большей степени подходит для аудита уже существующих ИС, находящихся на стадии эксплуатации, нежели чем для ИС, находящихся на стадии разработки;
- аудит по методу CRAMM – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора;

- программный инструментарий CRAMM генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;
- пользователи не имеют возможности внести дополнения в базу знаний, что вызывает *трудности при адаптации* метода к потребностям конкретной организации [58].

Программное обеспечение RiskWatch американской компании RiskWatch, Inc. является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности.

К **недостаткам** RiskWatch можно отнести:

- необходимость наличия на предприятии *достоверной статистики* по инцидентам в сфере ИБ;
- необходимость наличия *экспертов*, способных дать достоверные оценки объемов потерь от реализации угроз ИБ;
- в этом продукте *риски* в сфере *информационной* и *физической* безопасности компьютерной сети *рассматриваются совместно* [58].

Система **ГРИФ 2006** предоставляет возможность проводить анализ рисков при помощи анализа модели информационных потоков, а также, при помощи анализа модели угроз и уязвимостей - в зависимости от того, какие исходные данные есть в распоряжении аудитора, а также от того, какие данные аудита требуются для принятия решения о возможности успешного прохождения системой аудита ИБ.

Для оценки рисков информационной системы организации, согласно *модели анализа угроз и уязвимостей*, защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы [60].

Данный подход имеет ряд **недостатков**:

- нет возможности сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности;
- отсутствует возможность добавить специфичные для данной компании требования политики безопасности [61].

Второй из предложенных методов расчета риска – алгоритм *построения модели информационных потоков*. Анализ рисков нарушения информационной безопасности, согласно данному методу, осуществляется с помощью построения модели информационной системы организации [62].

Недостатки данной модели:

- учитывается лишь *наличие или отсутствие барьера* на пути распространения угроз, и нет возможности учесть как влияет то или иное СрЗ на величину риска нарушения информационной безопасности;
- при анализе информационного риска *не учитываются атаки*, осуществляемые пользователями *из других сегментов* [58].

В соответствии с предложенным в [63] методом оценки риска нарушения информационной безопасности был разработан программный комплекс **RiskAnalyzer** [64], реализующий алгоритм, описанный в [65].

Недостатком данного программного решения является необходимость вручную строить модель угроз в виде нечетких когнитивных карт, что требует высокой квалификации от аудитора ИБ.

Кроме того, можно отметить, что общими недостатками методов Гриф 2006, CRAMM, COBRA, RiskWatch, *MSAT* и программных продуктов, реализующих методы, а также программы *RiskAnalyzer* является *невозможность оценить значение уровня риска нарушения ИБ в реальном масштабе времени с учетом информации с датчиков событий*; в средствах Гриф 2006, CRAMM, COBRA, RiskWatch, *MSAT* отсутствует возможность учесть сведения о технических х*арактеристиках* используемых или планируемых средств защиты [63].

1.5 Основные научно-теоретические задачи, решаемые в диссертационной работе

Анализ особенностей информационной системы, построенной на основе технологии облачных вычислений, приведенный в разделе 1.1 показал, что обеспечение режима информационной безопасности ИСОТ является одной из самых серьёзных и актуальных проблем как для поставщика, так и для потребителя облачных услуг. На основе проведенного анализа литературы и известных публикаций, можно сделать вывод о том, что оценка степени соответствия компонентов системы обеспечения информационной безопасности (СОИБ) требованиям существующих стандартов в области ИБ, построение *модели угроз, оценка рисков* и разработка рекомендаций по их управлению осуществляются в ходе проведения *аудита информационной безопасности,* который обеспечивает получение и *оценку* объективных данных о текущем состоянии защищенности информационной системы.

Данной проблеме посвящены работы большого количества авторов, среди которых [1, 40-46, 48, 50, 52, 54-57, 59-61].

Проведенный в разделе 1.4 сравнительный анализ известных методов и средств автоматизации аудита информационной безопасности позволяет сделать следующие выводы: предлагаемые методы проведения аудита ИБ в большинстве случаев либо опираются на качественные экспертные оценки, либо не достаточно детализированы; в программных средствах отсутствует возможность оценить *оперативное* значение уровня риска нарушения информационной безопасности. Кроме того, существенным недостатком почти всех рассмотренных методов и программных средств является невозможность учесть специфику объекта защиты (что является одним из важнейших пунктов для проведения аудита в облачных средах), а также отсутствие возможности оценить эффективность конкретного набора средств защиты информации. Так как отчеты почти всегда формируются на основе

экспертных оценок и данных общего характера, они не могут быть использованы как основа для проведения объективного аудита ИБ.

Кроме того, аудит ИБ на соответствие требованиям существующих стандартов в области защиты информации, невозможно провести для ИСОТ, в силу того, что подходящие стандарты для облачных вычислений отсутствуют в нормативной правовой базе РФ или находятся в стадии разработки. Таким образом, единственным способом проведения аудита ИБ для облачных сред на сегодняшний день является использование численных методов оценки рисков нарушения ИБ.

Вместе с тем, потребитель, заключая договор на предоставление облачных услуг, должен требовать от поставщика внедрения средств мониторинга событий и управления инцидентами, что позволило бы оценить риск нарушения информационной безопасности ИСОТ в реальном масштабе времени, когда угроза проявляется по конкретному пути распространения к конкретному критичному объекту определенного потребителя.

Исходя из всего вышеперечисленного актуальной задачей является разработка методологии аудита информационной безопасности ИСОТ, основанной на расчете оперативного значения риска нарушения ИБ.

Метод оценки оперативного риска, применяемый для аудита ИБ ИСОТ, должен отвечать требованиям:

- применимости на стадии эксплуатации СЗИ в режиме реального времени;
- учета специфики объекта защиты, особенностей топологии сети облака, специфических средств защиты информации, применяемых в облачных технологиях;
- возможности получения количественных выходных данных;
- достаточной формализованности для реализации в качестве программного продукта.

Задачи, решаемые в диссертационной работе

Для достижения поставленной цели в настоящей диссертационной работе решаются следующие задачи:

1. Определение *перечня угроз* нарушения информационной безопасности, характерных для облачных вычислений, и *их источников*. Разработка *модели* преднамеренных *угроз* нарушения информационной безопасности с учетом особенностей ИСОТ.

2. Разработка методики частной политики безопасности СОбВ, основываясь на рекомендациях проектов государственных стандартов РФ в сфере облачных вычислений и учитывая специфику ИСОТ.

3. Разработка *метода проведения экспертного аудита информационной безопасности* систем, построенных на основе технологии облачных вычислений, основанного на получении численной оценки рисков нарушения ИБ, а также *функциональной модели IDEF0* аудита информационной безопасности ИСОТ.

4. Разработка *программного модуля автоматизации процесса экспертного аудита ИБ* информационной системы, реализующего предложенные модели и методы. Исследование адекватности предложенных моделей и методов на основе вычислительных экспериментов.

1.6 Выводы по первой главе

1. Изучение нормативной правовой документации и стандартов в области информационной безопасности облачных сред позволяет сделать вывод о перспективности исследований и разработок методов и средств проведения аудита информационной безопасности ИСОТ. Анализ различных публикаций показал, что аудит на соответствие требованиям существующих стандартов в области защиты информации невозможно провести для

информационных систем, построенных на основе вычислительного облака, в силу того, что подходящие стандарты для облачных вычислений отсутствуют в нормативной правовой базе РФ или находятся в стадии разработки. Конкретные же решения в области проведения аудита облачных вычислений также отсутствуют. Таким образом, необходимо разработать метод аудита ИБ ИСОТ, который позволял бы численно оценить значение уровня риска нарушения информационной безопасности облака в условиях отсутствия нормативной правовой базы по данному вопросу.

2. Обзор нормативных правовых документов и известных публикаций показал, что для успешного проведения аудита ИБ с помощью методов численной оценки риска нарушения информационной безопасности с последующим выбором рационального варианта реагирования на опасные события необходима *адекватная объекту защиты модель угроз*, которая учитывала бы все особенности инфраструктуры и специфику ИСОТ. Кроме того, построение модели угроз должно осуществляться на основе наиболее полного перечня угроз и их источников, а также на основе разработанной частной политики информационной безопасности для СОбВ. В настоящее время отсутствуют исследования, задачей которых было бы выявление угроз и их источников, характерных для облачных сред, разработка частной политики безопасности для облачных вычислений, а также отсутствуют подходы к построению моделей угроз, адекватных для ИСОТ.

3. Анализ современных литературных источников и нормативной правовой базы РФ показал, что для получения объективных результатов аудита системы защиты ИСОТ важно оценить не только значение уровня риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз, но и значение уровня риска, когда угроза проявляется по конкретному пути распространения в реальном времени. Однако, методы, которые позволили бы численно оценить риск нарушения информационной безопасности в реальном масштабе времени на основе сенсоров и датчиков опасных событий, в настоящее время отсутствуют.

4. В связи с необходимостью периодического проведения аудита информационной безопасности целесообразна разработка *программного модуля,* в котором реализованы результаты исследований, позволяющего обеспечивать воспроизводимость полученных результатов и сократить время проведения аудита ИБ. В связи с тем, что облачные технологии являются частью стратегии по повышению динамичности бизнес-процессов предприятия, а также, учитывая возможность реализации сложных сценариев атак, при разработке подобного программного модуля необходимо использовать современные интеллектуальные технологии, способные адаптироваться к данному объекту защиты и небольшим изменениям в условиях функционирования объекта. Примером такой интеллектуальной технологии является искусственная нейронная сеть (ИНС).

ГЛАВА 2. РАЗРАБОТКА ЧАСТНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ И МОДЕЛИ УГРОЗ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Предложена методика разработки частной политики информационной безопасности для облачных сред и разработана модель угроз в системе облачных вычислений на основе использования нечетких когнитивных карт.

В данной главе приводится описание угроз нарушения информационной безопасности и их источников, характерных для системы облачных вычислений – информационной системы, в которой взаимодействуют поставщик и конкретный потребитель облачных услуг, на основе абстрактно-алгебраического подхода формируется формализованное описание системы защиты СОбВ, а также разрабатывается модель политики информационной безопасности ИСОТ.

Результаты данной главы опубликованы в работах [21,103,104,107].

2.1 Разработка архитектуры системы облачных вычислений

В диссертационной работе рассматривается бизнес-модель продажи и использования *приложения как услуги (SaaS)*. Поставщик в этом случае разрабатывает web-приложение и предоставляет клиенту доступ к программному обеспечению через сеть «Интернет». Преимущество этой модели для потребителя заключается в отсутствии затрат на приобретение, установку, техническую поддержку оборудования и аппаратных платформ для развертывания приложений.

Предоставляемая поставщиком облачных услуг компьютерная инфраструктура включает: аппаратные средства, операционные системы, ПО

для управления облаками и средства виртуализации. Потребителю через web-интерфейс программное обеспечение предоставляется *в аренду*. *Программное обеспечение для управления облаками* предоставляет возможности мониторинга облачной инфраструктуры, предоставления ресурсов в нужном для потребителя объеме, обеспечения задачи безопасности облака, помогает подключать гипервизоры, создавать облачные хранилища.

Вычислительное облако представляет собой систему, построенную на основе клиент-серверной архитектуры. Модель клиент-серверного взаимодействия характеризуется наличием двух взаимодействующих самостоятельных процессов - клиента и сервера. Архитектура облачных вычислений является *более современной версией архитектур клиент-серверных взаимодействий*, которая обеспечивает развитие ИТ-технологий.

Как отмечается в [9] любая архитектура облака не является универсальной: все компоненты инфраструктуры, за исключением программного обеспечения управления облаками, являются опциональными для определенного потребителя облачных услуг, зависят от бизнес-процессов потребителя и оговариваются с поставщиком. Например, есть ряд задач, которые не требуют средств виртуализации, однако решение все равно будет считаться облачным. В каждом случае, для каждого конкретного потребителя, облачная архитектура может быть выполнена с использованием различных компонентов, которые зависят от конкретных бизнес-процессов, которые будут выполняться в облаке.

Облачным средам характерны *угрозы безопасности информации, связанные с потерей доверия*, которые связаны с закрытостью для пользователей применяемых поставщиком облачных технологий, программных решений, невозможностью дать оценку реализованного уровня защищенности информации, достигнутого поставщиком, отсутствием эталонных значений каких-либо параметров, которые необходимо обеспечить поставщику и пользователю облачных услуг для достижения определенного уровня безопасности, а также *угрозы, связанные с*

непрерывностью модернизации ИСОТ, когда система рассматривается как защищенная на этапе проектирования, а после ввода ее в эксплуатацию может обладать множеством уязвимостей, содержащихся в новом установленном ПО. В связи с этим, в рамках договора об оказании облачных услуг, необходимо проводить периодический независимый аудит информационной безопасности системы с целью определения актуального уровня защищенности СОбВ.

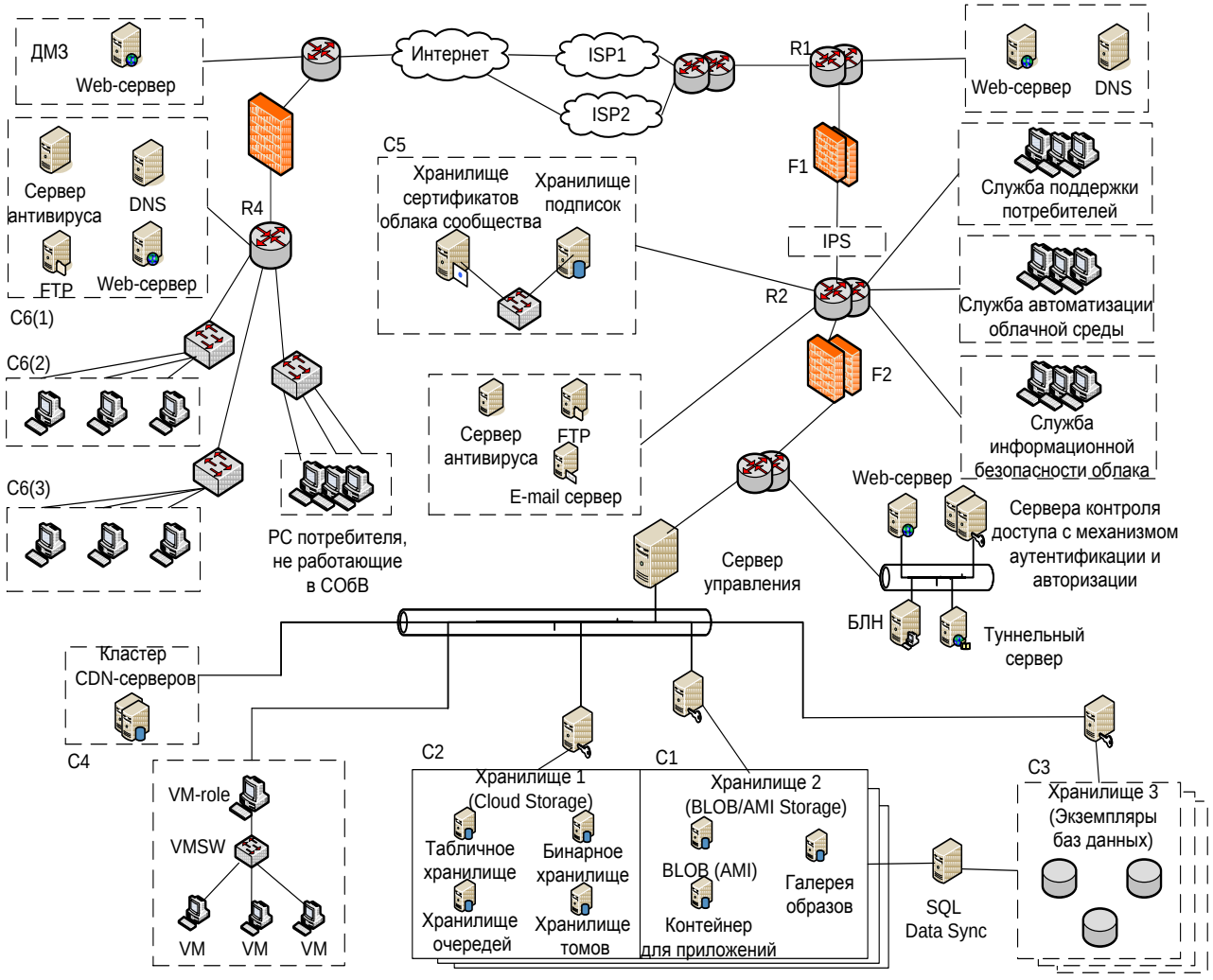


Рисунок 2.1 – Архитектура системы облачных вычислений

Провести аудит информационной безопасности и оценить уровень защищенности облачной системы в общем виде, без учета особенностей облачной инфраструктуры потребителя и поставщика облачных услуг

невозможно. Благодаря проведенному анализу возможных схем клиент-серверных взаимодействий, архитектуры облачного решения Azure [9] и изучения концепции вычислительного облака для обеспечения услуги SaaS (программное обеспечение как услуга), представленной в [2], в диссертационной работе предложена *архитектура системы облачных вычислений* для облака сообщества, представленная на рисунке 2.1.

При разработке инфраструктуры СОбВ учтены требования для типовой ИСОТ и требования архитектуры безопасности.

Согласно [2], в состав ИСОТ входят следующие компоненты:

- со стороны потребителя облачных услуг: рабочие станции сотрудников потребителя облачных услуг с удаленным рабочим столом, облачные периферийные устройства и ПО (облачный клиент), сетевое оборудование для осуществления межоблачного взаимодействия.
- со стороны поставщика облачных услуг: пограничный сервер для потребителя, функциональные серверы для обеспечения бизнес-процессов потребителя облачных услуг, хранилища данных (представлены в архитектуре тремя хранилищами), сетевое оборудование, включая сетевое оборудование для осуществления межоблачного взаимодействия.

Архитектура сети потребителя облачных услуг в архитектуре СОбВ представлена *минимальным* набором простейших элементов инфраструктуры, которые поддерживают в рабочем состоянии сеть потребителя.

Архитектура сети поставщика включает в себя *пограничный сервер* для связи с конкретным потребителем, реализованный в виде *IIS сервера*, серверы контроля доступа с механизмом аутентификации и авторизации для входа в рабочую часть вычислительного облака потребителя, *тремя службами потребителя облачных услуг,* а также служебными *серверами для выдачи и хранения сертификатов* членов облака сообщества *и данных о подписках* каждого потребителя. Весь трафик аутентификации и авторизации клиента, а также трафик, содержащий обрабатываемые в облаке критичные активы потребителя облачных услуг, шифруется с помощью туннельного

сервера, а доступность web-сервера гарантируется балансировщиком нагрузки (БЛН).

В рабочей области облака доступ к хранилищам и виртуальным машинам осуществляется с помощью *сервера управления* облаком. *Кластер CDN серверов (Content Delivery Network)* хранит контент сети доставки облака и является отдельно заказываемой функцией облака сообщества для обеспечения более быстрого доступа к наиболее часто используемым данным потребителя.

Администратор потребителя облачных услуг управляет всей сетью виртуальных машин (ВМ) с помощью специализированной ВМ – *VM-role*, к которой через *виртуальный коммутатор* подключены все виртуальные машины потребителя облачных услуг.

Доступ к *хранилищам системы облачных вычислений* осуществляется через БЛН с дополнительной аутентификацией и авторизацией сотрудника потребителя облачных услуг.

Хранилище 1 (*Cloud Storage)* – хранилище, в котором находятся неструктурированные данные потребителя (документы, видеофайлы, чертежи, схемы) и в том числе тома для подключения к вызываемому сотрудником потребителя образу виртуальной машины. Информация для аутентификации и авторизации пользователя для доступа к данному хранилищу прописана в учетной записи пользователя, под именем которого авторизовался в системе сотрудник потребителя облачных услуг.

Хранилище 2 (BLOB/AMI Storage) − хранилище образов виртуальных машин, которое также включает в себя галерею образов и контейнер для приложений. Информация для аутентификации и авторизации пользователя для доступа к данному хранилищу имеет несколько уровней. При низком уровне доступа сотрудник потребителя имеет доступ только к образу виртуальной машины, с которым ему положено работать по бизнес-процессам. Однако уровень сотрудника можно повысить и получить доступ к галерее образов, содержащей «чистые» образы виртуальных машин, а также к

контейнеру приложений, в котором находятся все заказанные потребителем облачных услуг приложения, готовые к установке в образ ВМ. Повышение уровня доступа ко второму хранилищу регламентируется политикой безопасности потребителя облачных услуг и находится в юрисдикции компании потребителя облачных услуг.

Хранилище 3 служит для хранения *экземпляров баз данных* потребителя облачных услуг. Для доступа в хранилище также нужно пройти процедуру аутентификации, которая определит конкретный экземпляр базы/баз данных, которые должны быть доступны сотруднику потребителя облачных услуг в соответствии с бизнес-процессами.

Совокупность пограничного сервера, функциональных серверов и хранилищ данных, а также сетевое оборудования для поддержки серверов, представляет собой *типовой облачный сервер ИСОТ*.

Уровень оборудования представлен маршрутизаторами, коммутаторами и серверами, *уровень управления* – сервером управления и сервисами безопасности, такими как, например, межсетевые экраны, IPS, туннельные серверы шифрования трафика и серверы контроля доступа с механизмами аутентификации и авторизации потребителя облачных услуг. *Уровень оркестровки* на данной архитектуре не отражен, но учтен в составленной по данной архитектуре модели угроз нарушения информационной безопасности.

Типовая архитектура *демилитаризованной зоны* поставщика облачных услуг включает в себя: публичный web-сервер, DNS-сервер, сервер приложений для управления информационными ресурсами web-портала. В демилитаризованной зоне должна храниться и обрабатываться только общедоступная открытая информация, что отражено в варианте архитектуры СОбВ.

Чтобы минимизировать риски потребителя и поставщика в процессе реализации облачных сервисов, внутренний web-сервер для клиент-серверного взаимодействия (например, IIS-сервер) размещен в другом сетевом сегменте, как и CDN-сервер, обеспечивающий временное хранение ресурсов клиентов

облачных сервисов и позволяющий уменьшить время доступа пользователей к кэшированным данным. То есть следует обеспечить сегрегацию этих серверов от общедоступных, располагая их во внутренней защищенной подсети поставщика облачных услуг (во внутренней рабочей области облака).

2.2 Описание угроз нарушения информационной безопасности, характерных для систем облачных вычислений, и их источников

При построении системы обеспечения информационной безопасности системы облачных вычислений (СОбВ) необходимо принимать во внимание угрозы нарушения информационной безопасности *конкретному* объекту защиты. В рамках данной диссертационной работы составлен перечень угроз в системе облачных вычислений (СОБВ) на основе модели предоставления услуг SaaS с учетом рекомендаций, представленных в [2].

1. Угрозы безопасности информации для *потребителя* облачных услуг.

- Угрозы безопасности информации, связанные с неопределённостью ответственности. Данные угрозы появляются в связи с отсутствием чёткого *разделения ответственности* в части обеспечения информационной безопасности между потребителем и поставщиком услуг SaaS, что является причиной невыполнения некоторых мер по защите информации. Необходимо четкое и однозначное составление договора об оказании услуги и соблюдение всех *пунктов частной политики безопасности*, как поставщиком, так и потребителем.

- Угрозы безопасности информации, связанные с потерей управления. Использование облачных услуг подразумевает передачу потребителем облачных услуг части *функций управления* своей ИС

поставщику облачных услуг. В частности, при оказании услуги SaaS поставщику дополнительно делегируются функции по управлению операционными системами и прикладным ПО. Это приводит к тому, что поставщик облачных услуг может задать параметры информационной системы потребителя облачных услуг в соответствии со сложившейся у него практикой. В свою очередь, потребитель облачных услуг не имеет возможности полностью контролировать значения заданных параметров и, следовательно, не в состоянии в полной мере самостоятельно обеспечить защищённость своей информации. Здесь у администратора поставщика возникает возможность получить доступ к критичным активам потребителя.

- Угрозы безопасности информации, связанные с потерей доверия. В общем случае пользователи облачных услуг *не могут* достоверно *оценить уровень доверия к поставщику* облачных услуг, в связи с закрытостью для пользователей применяемых поставщиком облачных технологий и программных решений. Не известны эталонные значения каких-либо параметров, которые надо обеспечить поставщику и пользователю облачных услуг для достижения определённого уровня безопасности. Кроме того, пользователи облачных услуг не обладают возможностью дать оценку реализованного уровня защищённости информации, достигнутого поставщиком. В данном случае необходимо *проведение экспертного аудита СОбВ* с последующим предоставлением результатов потребителю в качестве гаранта сохранности его критичных активов.

- Угрозы безопасности информации, связанные с *осуществлением несанкционированного доступа (НСД)* со стороны *потребителей* облачных услуг. Так как облачные ресурсы предоставляются удалённо, то на облачный сервер могут быть проведены атаки, связные с уязвимостями сети потребителя облачных услуг. Это позволяет сделать вывод о необходимости разработки и *внедрения частной политики безопасности* в сегменте потребителя и использования сервисов безопасности, призванных

гарантировать защиту пользовательских рабочих мест на стороне потребителя облачных услуг.

- Угрозы, связанные с общедоступностью инфраструктуры. Так как потребители облачных услуг (в том числе все потребители облака сообщества) делят *одну и ту же инфраструктуру поставщика*, то возникают угрозы нарушения безопасности данных путём осуществления *прямого доступа* к защищаемым данным *другого потребителя облачных услуг*.

- Угрозы безопасности информации, связанные с недостатком управления облачными ресурсами. Данная угроза обусловлена сложностью *определения* логического и физического *местоположения облачных ресурсов*, недостаточностью физического *контроля доступа к хранилищам* данных, надёжностью *резервного копирования* и др. Кроме того, существуют угрозы потребителям облачных услуг, связанные с передачей защищаемой информации поставщикам облачных услуг, являющихся резидентами других стран со своими особенностями законодательства в области защиты информации.

- Угрозы, связанные со злоупотреблениями со стороны потребителей облачных услуг. В связи с тем, что потребитель облачных услуг может устанавливать собственное ПО на облачный сервер, то для достижения своих неправомерных целей потребитель облачных услуг может *установить вредоносное ПО*, с помощью которого осуществлять рассылку спама, НСД к виртуальным машинам других клиентов.

2. Угрозы безопасности информации для поставщиков облачных услуг.

- Угрозы, связанные с неопределённостью при распределении ответственности. В облаке могут быть определены такие роли, как провайдер облачных услуг, пользователь облачных услуг, администратор клиентской информационной системы, владелец информации и т. д. При этом существуют угрозы, связанные с *неопределённостью при распределении ответственности между различными ролями* в части владения данными,

контроля доступа, поддержки инфраструктуры и т. п. Организация безопасности информации от таких угроз затруднена тем, что её реализация способна привести к существенным разногласиям между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей. Для устранения этой угрозы поставщику облачных услуг необходимо *тщательно прорабатывать политику безопасности*, и уделять особое внимание *проработке ролей*.

- Угрозы, связанные с *несогласованностью политик безопасности*. Вследствие децентрализованности архитектуры системы облачных вычислений, у поставщика и потребителя облачных услуг могут быть реализованы различные политики безопасности для одних и тех же средств защиты. Такая несогласованность политик безопасности различных средств защиты может быть использована злоумышленником в интересах нарушения информационной безопасности.

- Угрозы, связанные с *непрерывной модернизацией* ИСОТ. Одним из преимуществ использования облачных услуг является возможность осуществления выбора и изменения *первоначального состава ПО* уже после ввода системы облачных вычислений в эксплуатацию. Однако в этих условиях система, рассматриваемая как защищённая на этапе проектирования, после ввода её в эксплуатацию может обладать множеством уязвимостей, содержащихся в новом ПО. Таким образом, можно сделать вывод о необходимости проведения периодического независимого аудита информационной безопасности на основе оценки уровня риска нарушения ИБ, чтобы оценить защищенность системы *в реальном масштабе времени*.

- Угрозы, связанные с осуществлением незащищённого администрирования облачных услуг. Использование средств администрирования в СОбВ, может являться причиной угроз вследствие *недостаточности внимания*, уделённого контролю вводимых пользователями облачных услуг данными (в том числе аутентификационных данных).

- Угрозы, связанные с использованием технологий виртуализации. В большинстве случаев основой для создания облачной инфраструктуры являются технологии виртуализации. При этом один физический сервер, его вычислительные ресурсы и ресурсы памяти делятся между множеством виртуальных машин.

В данном перечне угроз *не рассматривались* технические сбои коммуникационного оборудования и программного обеспечения поставщика и потребителя облачных услуг, ошибки администраторов и пользователей системы рассматриваются как уязвимости.

В соответствии с приведенными в диссертационной работе угрозами нарушения информационной безопасности системы облачных вычислений был сформирован перечень источников угроз, характерных для СОбВ, представленный в таблице 2.1.

Таблица 2.1 − Источники угроз ИБ в системах облачных вычислений

№ п/п	Источник угроз	Описание источника угроз	Возможности источника угрозы	Особенности источника угроз в СОбВ
1	2	3	4	5
1.	Потребитель облачных услуг или запущенный им процесс [ПОТ]	Является внутренним нарушителем по отношению к системе облачных вычислений	Несоблюдение требований информационной безопасности при работе с СОбВ, игнорирование прав и правил, описанных в политике безопасности, может позволить субъекту получить несанкционированный доступ к критичной информации, хранящейся в облаке	Воздействие источника угроз аналогично традиционным ИС

Окончание таблицы 2.1

1	2	3	4	5
2.	Сотрудник (администратор) поставщика облачных услуг или запущенный им процесс [ПОС]	Является внутренним нарушителем по отношению к системе облачных вычислений	Теоретически обладает неограниченным доступом к компонентам СОбВ, которые на практике должны быть *ограничены частной политикой безопасности*, может реализовывать угрозы ИБ, связанные с несанкционированным доступом к информации потребителя	В связи с переносом части информационных активов потребителя в облака, возможности сотрудника поставщика при доступе к данным активам расширяются
3.	*Другой потребитель облачных услуг или запущенный им процесс* [ДР_КЛ]	Является внешним нарушителем по отношению к системе облачных вычислений	Может реализовывать угрозы нарушения ИБ по отношению к информационным активам и ресурсам других потребителей СОбВ	Наличие данного источника угроз обусловлено динамической масштабируемостью и консолидацией вычислительных ресурсов, а также возможностью самообслуживания потребителей.
4.	Злоумышленник или запущенный им процесс [ЗЛ]	Является внешним нарушителем по отношению к системе облачных вычислений	Не является потребителем облачных услуг. Может получить несанкционированный доступ к информационным активам и ресурсам СОбВ, используя те или иные программно-аппаратные средства.	Воздействие источника угроз аналогично традиционным ИС.

На рисунке 2.2 представлена схема процесса распространения угроз в СОбВ посредством эксплуатации уязвимостей компонентов инфраструктуры

облака и с учетом рекомендованных в [2] особенностей ИСОТ. Схема разработана в соответствии с дополненным перечнем источников угроз.

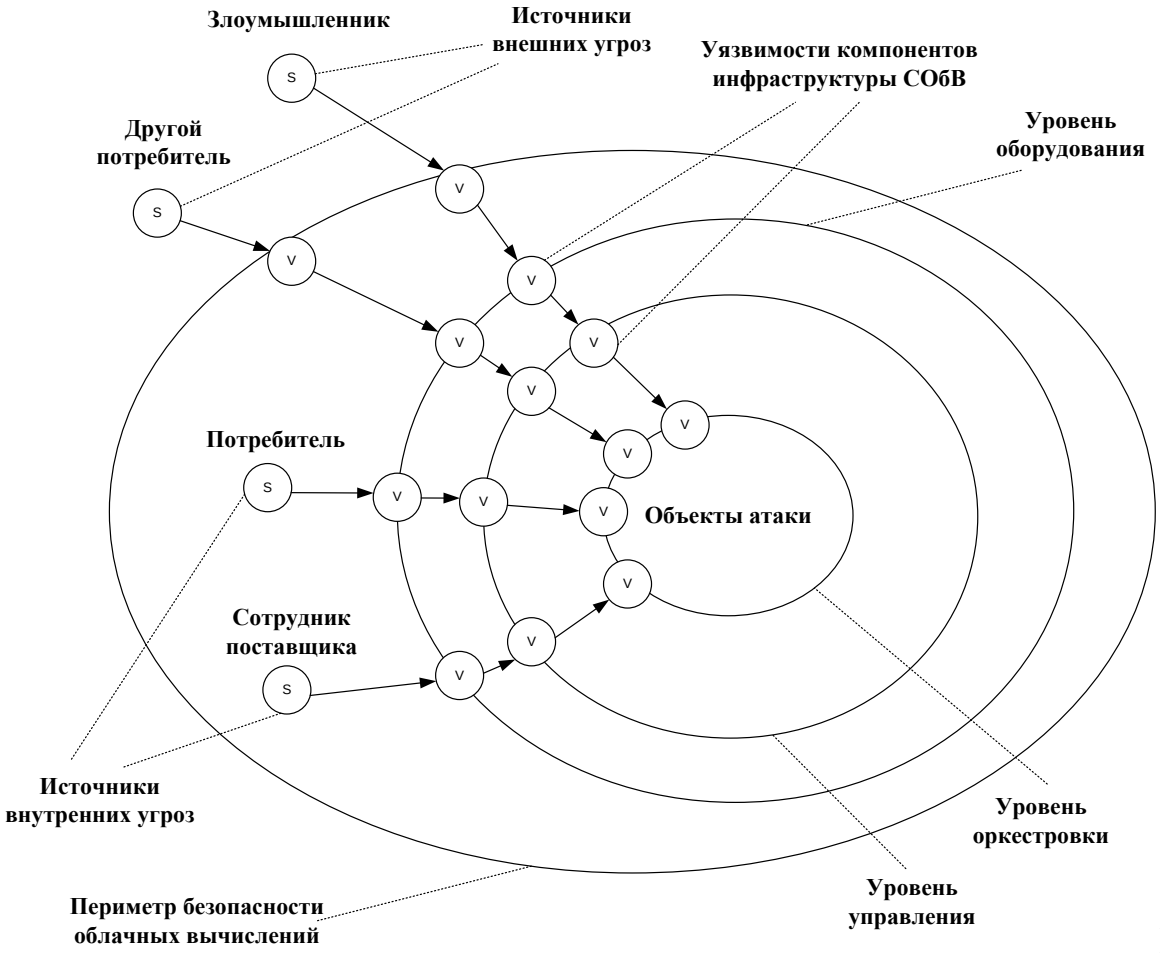


Рисунок 2.2 – Схема процесса распространения угроз в СОбВ

Поскольку в диссертационной работе под СОбВ понимается информационная система взаимодействия конкретного потребителя с поставщиком облачных услуг, при использовании облачных вычислений, *периметр ИСОТ* охватывает не только корпоративную сеть потребителя, но и сеть поставщика [66], обслуживающую определенного потребителя. Архитектура поставщика, созданная или эксплуатируемая другим потребителем в инфраструктуре поставщика, не является частью СОбВ.

Периметр безопасности облачных вычислений является ключевой концепцией компьютерной безопасности облаков [48]. Периметр безопасности выполняет роль барьера в отношении операций *доступа к СОбВ*: *субъекты*, которые находятся внутри периметра являются

внутренними по отношению к облаку пользователями, которые осуществляют доступ к ресурсам облака в соответствии с *частной политикой безопасности, принятой поставщиком и потребителем облачных услуг*; *субъекты*, которые находятся за периметром безопасности облачных вычислений, не имеют права так или иначе получить доступ к ресурсам системы, если только это не разрешено средствами контроля границ (например, периметровым межсетевым экраном) на основе применения соответствующих политик доступа. Контроль периметра безопасности облачных вычислений является важным элементом построения безопасных облачных систем [48].

Уровень оборудования является первым уровнем архитектуры ИСОТ, на котором выполняются функции, возложенные на аппаратное обеспечение, в там числе на аппаратные сервисы безопасности, входящее в состав такой системы. Уровень оборудования включает в себя все пограничные серверы поставщика, серверы для хранения информации потребителя, а также коммуникационное оборудование потребителя и поставщика облачных услуг.

Уровень управления включает в себя управление виртуальными машинами и виртуальным сетевым оборудованием, централизацию всех ресурсов СОбВ и обеспечение отказоустойчивости элементов распределенной вычислительной сети СОбВ.

Уровень оркестровки включает в себя специализированное ПО для управления облачными серверами ИСОТ, программные средства обеспечения ИБ в облачных средах, а также ПО, которое будет установлено потребителями облачных услуг в случае реализации услуги SaaS.

2.3 Формализованное описание системы защиты информации СОбВ на основе абстрактно-алгебраического подхода

Процесс защиты информации характеризуется большим количеством и многообразием факторов, влияющих на его результат, воздействие которых часто не удается однозначно выявить и описать строго математически. В связи с этим проблема защиты информации относится к числу *сложных слабоструктурированных* и *слабоформализуемых* проблем [42].

Существует несколько подходов к математическому описанию сложных слабоструктурированных проблем, позволяющих не только понять особенности и специфику исследуемого объекта защиты, но и выработать рациональную стратегию действий, опирающуюся на количественные оценки. Для применения количественных методов исследования требуется математическая модель исследуемого объекта или процесса, в которой они упрощаются, схематизируются и представляются с использованием некоторого математического аппарата. Для более детальной проработки и учета особенностей ИСОТ необходимы абстрактные модели, которые позволили бы использовать компактные символические системы для описания системы защиты информации СОбВ. В диссертационной работе предлагается использовать в качестве аппарата для формализации системы защиты информации СОбВ *абстрактно-алгебраический* подход к описанию систем [67,68].

Система защиты информации в соответствии с [69] представляет собой *совокупность* органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, *организованную и функционирующую* по правилам и нормам, установленным соответствующими документами в области защиты информации.

Предлагается описание системы защиты информации (СЗИ) СОбВ в виде восьмерки пространств:

$$Q = \{O, I, M, T, S, P_a, L, F\},$$

где O – пространство информационных ресурсов, объектов атаки: виртуальные машины и приложения потребителя, объекты Cloud Storage,

экземпляр базы SQL, контент сети доставки облака, управляющая информация СОбВ, данные о подписках и сертификаты потребителей, информационные ресурсы, обрабатываемые на стороне потребителя облачных услуг;

I – пространство компонентов инфраструктуры системы облачных вычислений;

M – пространство средств защиты информации и сервисов безопасности СОбВ;

T – пространство нормативных правовых документов в сфере защиты информации, принятых в СОбВ, включая частную политику безопасности облачных вычислений;

S – пространство источников угроз: сотрудник-нарушитель компании потребителя облачных услуг, злоумышленник – субъект, не являющийся потребителем облачных услуг (или запущенные им процессы), сторонний нарушитель – субъект являющийся другим потребителем облачных услуг (или запущенные им процессы), сотрудник (администратор) поставщика облачных услуг (или запущенные им процессы);

P_a – пространство вероятностей активизации источников угроз;

L – пространство состояний СОбВ;

F – пространство событий перехода системы из безопасного состояния в небезопасное и наоборот.

Пространство вероятностей активизации источников угроз $p_a \in P_a$ и пространство источников угроз нарушения безопасности СОбВ $s \in S$ будем называть наборами *существенных свойств* системы в каждый конкретный момент времени, а пространство информационных ресурсов $o \in O$ и пространство компонентов инфраструктуры $i \in I$ будем называть *операционными свойствами* системы в каждый конкретный момент времени.

В целях анализа информационной безопасности для каждого состояния системы введем четыре атрибута для пространства вероятностей активизации

источников угроз: $p_a^{зл}$ – вероятность активизации источника угроз – злоумышленника, $p_a^{адм}$ – вероятность активизации сотрудника поставщика облачных услуг; $p_a^{внш}$ – вероятность активизации стороннего нарушителя, являющегося другим потребителем облачных услуг; $p_a^{кл}$ – вероятность активизации сотрудника-нарушителя компании потребителя облачных услуг, такие что $p_a^{зл}, p_a^{адм}, p_a^{внш}, p_a^{кл} \in [0,1]$. Состояние СОбВ, при котором $(p_a^{зл}, p_a^{адм}, p_a^{внш}, p_a^{кл}) = (0,0,0,0)$ будем называть безопасным состоянием, любое же, отличное от этого, небезопасным.

Тогда, пространство безопасных состояний можно описать следующим соотношением:

$$L^+ = \{l \in L | (p_a^{зл}, p_a^{адм}, p_a^{внш}, p_a^{кл}) = (0,0,0,0)\}$$

Состояние, при котором хотя бы один из атрибутов будет отличен от нуля, будем называть небезопасным, и описываться оно будет соотношением:

$$L^- = \{l \in L | \exists \forall l \in \{p_a^{зл}, p_a^{адм}, p_a^{внш}, p_a^{кл}\}, l \neq 0\}$$

Причем, пространство состояний СОбВ может описываться данным соотношением:

$$L^- \cup L^+ = L$$

Событием безопасности H^- в СОбВ назовем переход системы от безопасного состояния в небезопасное.

$$H^- = f \mid f \in F, f : L^+ \to L^-$$

Переход системы из небезопасного состояния в безопасное обозначим H^+.

$$H^+ = f \mid f \in F, f : L^- \to L^+$$

Событие безопасности H^- может привести к увеличению значения уровня риска нарушения информационной безопасности R. Система защиты информации должна создавать такие условия для системы, чтобы уровень

риска снижался (стремился к допустимому), то есть, снижалась вероятность перехода из безопасного состояния в небезопасное:

$$Q \Leftrightarrow (R \to 0) \coloneqq r : H^{+} \mid r : H^{-} \to H^{+}$$

На основании абстрактно-алгебраического подхода угроза безопасности информации СОбВ может быть представлена пятеркой пространств:

$$U = \{O, I, S, W, N\},$$

где W – пространство уязвимостей компонентов инфраструктуры СОбВ;

N – пространство способов реализации угроз от конкретного источника к конкретному объекту атаки.

Уязвимость $w \in W$ СОбВ – это слабое место (брешь) в барьере или отсутствие барьера на пути распространения атаки, существование которой в определенном состоянии системы облачных вычислений при наличии источника угрозы может привести к реализации атаки на ресурс ИСОТ:

$$W = \{w \mid w = m \wedge l \mid s \wedge l \Rightarrow H^{-}\}$$

Пространство угроз нарушения информационной безопасности – совокупность объекта атаки и субъекта атаки, при которой СОбВ переходит из безопасного состояния в небезопасное:

$$U = \{u \in n \mid u = o \wedge l \mid s \wedge l \Rightarrow L^{-}\}$$

Предложенная в диссертации математическая модель может быть применена к традиционным информационным системам, однако, характерные особенности ИСОТ обуславливают расширение пространств *O*, *I, S,* P_a по сравнению с традиционными информационными системами. В свою очередь, расширение этих пространств повлияет на изменение пространств *W* и *N* и, следовательно, способствует расширению всей модели угроз нарушения информационной безопасности СОбВ.

В диссертационной работе в качестве *результата действий* нарушителей и злоумышленника рассматривается получение доступа к

образу виртуальной машины потребителя облачных услуг и данным в хранилищах облака. Это обусловлено тем, что при перехвате информации во время осуществления межоблачного взаимодействия, нарушитель (злоумышленник) получает доступ лишь к некоторому объему информации, передаваемой из облака в сегменты сети потребителя облачных услуг, в то время как получение доступа к образу виртуальной машины потребителя облачных услуг и данным в хранилищах облака позволяет заинтересованному субъекту ознакомиться в полной мере со всем объемом критичной информации потребителя.

Каждое действие нарушителя и злоумышленника направлено на достижение частных целей, при этом для реализации атаки им необходимо активизировать или использовать уязвимости компонентов СОбВ, а также, в случае, например, злоумышленника, получить доступ за периметр безопасности облачных вычислений. То есть, для успешной реализации атаки необходимо определить слабые места – уязвимости компонентов инфраструктуры СОбВ. Кроме того, для получения количественных характеристик исследуемых угроз и возможности дальнейшего использования этих параметров в процессе анализа рисков нарушения информационной безопасности необходимо опираться на модель угроз, учитывающую особенности инфраструктуры ИСОТ.

Поскольку преднамеренная угроза – это действие, связанное с нарушением политики безопасности, построению модели угроз должна предшествовать разработка частной политики безопасности для СОбВ.

2.4 Метод разработки частной политики информационной безопасности системы облачных вычислений

2.4.1 Модель частной политики информационной безопасности для СОбВ

Многими экспертами отмечается, что потребитель облачных услуг имеет тот уровень защищенности в облачной среде, который обеспечивается поставщиком [8,48]. Однако для гарантии защиты пользовательских рабочих мест на стороне потребителя облачных услуг особое внимание необходимо уделить разработке политики безопасности всей системы облачных вычислений (СОбВ), под которой понимается информационная система взаимодействия поставщика и потребителя облачных услуг [70].

Политика информационной безопасности организации — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации [69].

Политика информационной безопасности любой организации зависит от конкретной технологии обработки информационных активов предприятия и от используемых в данной системе информационных потоков, реализующих деловые процессы предприятия. При составлении политики безопасности, необходимо учитывать, какая именно услуга предоставляется потребителю (SaaS, PaaS, IaaS или иная услуга) и какая именно модель облачного размещения реализуется в конкретном случае (частное, публичное, общественное облако, облако сообщества или иная модель) [69]. Критически важно, чтобы поставщики не пользовались и не навязывали универсальный подход в обеспечении информационной безопасности для всех моделей и для всех потребителей. Для устранения угроз, связанных с неопределённостью при распределении ответственности, поставщику облачных услуг необходимо тщательно прорабатывать политику безопасности.

Как отмечается в [71], политика безопасности любой информационной системы при разработке информационно-безопасных технологий состоит из множества *частных политик*, направленных на конкретные аспекты

безопасности ИС. Частные политики безопасности, детализирующие положения политики ИБ, формируются на основе принципов, требований и задач, определенных в политике информационной безопасности, с учетом дополнительной классификации активов и угроз, определения владельцев критичных активов, анализа, оценки рисков и возможных последствий реализаций угроз в границах области действия регламентируемой области или технологии [72].

Актуальность разработки частных политик информационной безопасности объясняется необходимостью планирования и управления ИБ на всех этапах жизненного цикла информационной системы. В случае разработки частной политики безопасности ИСОТ, необходимо учитывать специфику межоблачных взаимодействий между поставщиком и потребителем облачных услуг. С помощью правильно составленной политики ИБ можно обеспечить безопасное, доверенное и адекватное управление системой облачных вычислений, поддержку непрерывности межоблачного взаимодействия, повышение уровня доверия потребителя к поставщику облачных услуг и, как следствие, минимизировать риски нарушения информационной безопасности в СОбВ.

Таким образом, для обеспечения безопасного функционирования СОбВ необходимо создание частной политики информационной безопасности, которая должна неукоснительно соблюдаться как поставщиком, так и потребителем облачных услуг.

В диссертационной работе предлагается модель политики безопасности, которая учитывает особенности услуги SaaS в соответствии с [2]. Обеспечение информационной безопасности СОбВ при реализации услуги SaaS требует уделить особое внимание защите всех основных объектов ИСОТ. Требования, которые предлагается внести в политику безопасности ИСОТ, представлены в виде модели политики информационной безопасности на рисунке 2.3.

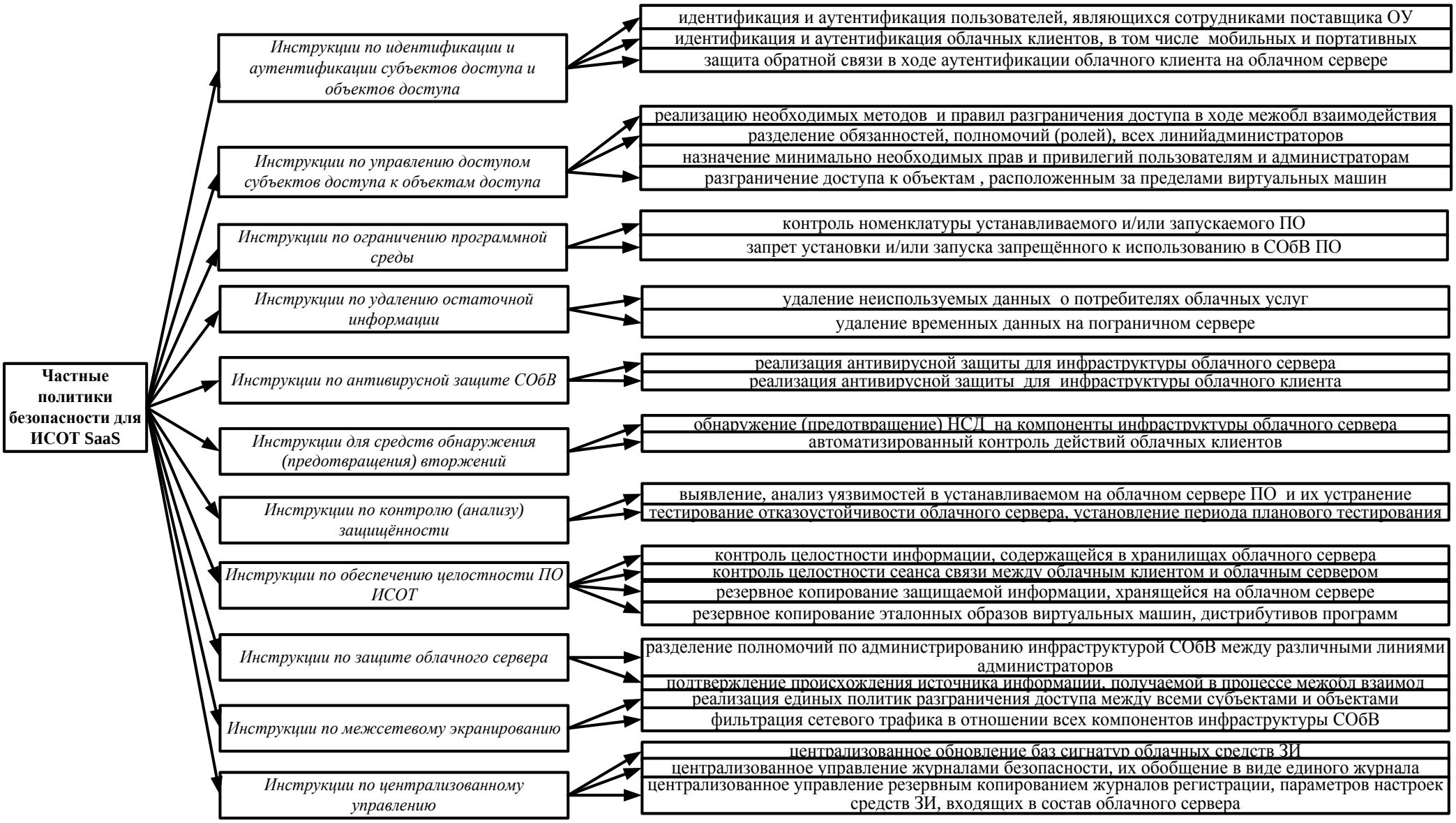


Рисунок 2.3 – Модель политики информационной безопасности СОбВ

Таким образом, соблюдение дополнительных требований к политике информационной безопасности СОбВ, предложенных в диссертационной работе, позволит существенно снизить риски использования облачных вычислений как со стороны поставщика, так и со стороны потребителя облачных услуг и, как следствие, позволит увеличить доверие потенциальных потребителей к ИСОТ.

2.4.2 Методика разработки частной политики информационной безопасности для СОбВ

В диссертационной работе предлагается модернизированная методика разработки частной политики безопасности применительно к СОбВ с использованием формальной модели, основанной на математической модели ролевого разграничения доступа, которая описана в [1,73,74].

Модель ролевого разграничения доступа – многообещающая технология контроля доступа для современной компьютерной среды. В ролевой политике разрешения ассоциированы с ролями, и пользователи соотносятся с соответствующими ролями, таким образом, получая разрешения ролей. Это упрощает управление всей СОбВ в целом. Кроме того, ролевая политика безопасности позволяет избежать угроз информационной безопасности, связанных с неопределенностью ответственности в системе облачных вычислений. Организация безопасности информации от таких угроз затруднена тем, что её реализация способна привести к существенным разногласиям между поставщиком и потребителем облачных услуг по вопросам, связанным с определением их прав и обязанностей. Для устранения этой угрозы поставщику облачных услуг необходимо не только *тщательно прорабатывать политику безопасности*, но и уделять особое внимание *проработке иерархии ролей и иерархии административных ролей*.

Роли задаются для различных должностей в облаке, и пользователи соотносятся к ролям, основанным на ответственности и профессионализме. Пользователи могут быть переназначены на другую роль. Роли могут наделяться новыми разрешениями по мере подключения новых приложений и заказе потребителем новых услуг, разрешения могут отбираться у ролей, когда это необходимо потребителю или поставщику услуг.

Основными элементами математической модели ролевого разграничения доступа являются [1,73,74]:

U – множество пользователей;

R – множество ролей;

P – множество прав доступа к объектам СОбВ;

S – множество межоблачных сессий пользователей;

(L, ≤) – решетка уровней конфиденциальности информации;

PA: $R \rightarrow 2^P$ – функция, определяющая для каждой роли *множество прав доступа*, при этом для каждого $p \in P$ существует $r \in R$ такая, что $p \in PA(r)$;

UA: $U \rightarrow 2^R$ – функция, определяющая для каждого пользователя *множество ролей*, на которые он может быть авторизован в облаке;

user: $S \rightarrow U$ – функция, определяющая для каждой межоблачной сессии *пользователя*, от имени которого она авторизована;

roles: $U \rightarrow 2^R$ – функция, определяющая для каждого пользователя *множество ролей*, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s))$;

c: $U \rightarrow L$ – функция уровня доступа пользователя;

c: $O \rightarrow L$ – функция уровня конфиденциальности объекта облака;

A = {read, write} – виды доступа;

AR – множество административных ролей ($AR \cap R = \varnothing$);

AP – множество административных прав доступа ($AP \cap P = \varnothing$);

ARA: AR $\rightarrow$ 2^{AP} – функция, определяющая для каждой административной роли *множество административных прав доступа*, при этом для каждого p $\in$ AP существует r $\in$ R такая, что p $\in$ ARA(r);

AUA: U $\rightarrow$ 2^{AR} – функция, определяющая для каждого пользователя *множество административных ролей*, на которые он может быть авторизован;

roles: S $\rightarrow$ 2^{R} $\cup$ 2^{AR} – функция, определяющая для пользователя *множество ролей*, на которые он авторизован в данной межоблачной сессии, при этом в каждый момент времени для каждого s $\in$ S выполняется условие roles(s) $\subseteq$ UA(user(s)) $\cup$ UA(user(s)).

Модель контролирует назначение пользовательской роли посредством отношения *can-assign* $\subseteq$ARxCRx2^{R}.

Отношение can-assign (***x***, ***y***, {***a***, ***b***, ***c***}) означает, что член административной роли ***x*** (или член административной роли, которая является старшей для ***x***), может назначать пользователя, текущее членство (или отсутствие членства) которого в постоянных ролях удовлетворяет условию необходимой предпосылки ***y***, членом постоянных ролей ***a***, ***b*** или ***c***.

Для реализации модели ролевого разграничения доступа в СОбВ необходимо установить уровни конфиденциальности, а также определить множество специфических для СОбВ объектов доступа и сформировать множество возможных субъектов доступа.

Установим для информационных объектов в СОбВ следующие уровни конфиденциальности: ОИ – открытая информация, К – конфиденциально, СК – строго конфиденциально

В результате исследований, проводимых в диссертационной работе, разработано и предложено множество информационных объектов доступа для системы облачных вычислений (таблица 2.2).

Таблица 2.2 – Множество информационных объектов доступа СОбВ

Обозн.	Наименование	Ур. конф.
1	2	3
o1	Сайт поставщика облачных услуг	ОИ
o2	Множество логинов и паролей личных кабинетов сотрудников потребителя облачных услуг	К
o3 (1)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту 1	СК
…		
o3 (*i*)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту i	СК
o4 (1)	Информационные ресурсы по проекту 1, хранящиеся в облачном хранилище	СК
…		
o4 (*i*)	Информационные ресурсы по проекту i, хранящиеся в облачном хранилище	СК
o5	Файлы СОбВ, относящиеся к конфигурированию собственных виртуальных машин конкретным потребителем облачных услуг	СК
o6 (1)	Файлы СОбВ, относящиеся к управлению внутриоблачным пространством поставщиком облачных услуг	СК
o6 (2)	Файлы СОбВ, относящиеся к сервисам безопасности поставщика облачных услуг	СК
o7	Данные о серверном времени, скорости доступа и обработки данных, объем хранимых в хранилище данных	К
o8	Данные о фактическом распределении доступа в едином пуле облака	СК
o9	Объем предоставленных потребителю услуг	К

Окончание таблицы 2.2

1	2	3
o10 (1)	Информационные ресурсы по проекту 1, хранящиеся на стороне потребителя облачных услуг	К
…		
o10 (*i*)	Информационные ресурсы по проекту i, хранящиеся на стороне потребителя облачных услуг	К
o11 (1)	Экземпляры отдела, работающего по проекту 1, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК
…		
o11 (*i*)	Экземпляры отдела, работающего по проекту i, запускаемые в физической операционной среде (физическом кластере поставщика облачных услуг)	СК

Множество ролей пользователей (субъектов доступа) системы облачных вычислений, разработанное в ходе исследований, представлено в таблице 2.3.

Таблица 2.3 – Множество субъектов доступа в СОбВ

Обозн.	Наименование	Ур. дост.
1	2	3
L1	Технический директор поставщика облачных услуг	СК
LT1	Сотрудник первой линии техподдержки поставщика облачных услуг	К
LT2	Сотрудник второй линии техподдержки поставщика облачных услуг	СК
LT3	Сотрудник третьей линии техподдержки поставщика облачных услуг	К
S1	Руководитель службы автоматизации ИСОТ	СК
S2	Главный специалист по ИСОТ	СК

Продолжение таблицы 2.3

1	2	3
S3	Администратор инфраструктуры ИСОТ	К
S4	Эксперт по виртуализации в облачных вычислениях	К
AV1	Начальник службы безопасности облачного поставщика	СК
AV2	Специалист по защите программного обеспечения и платформ поставщика услуги SaaS	К
AV3	Специалист по защите облачной инфраструктуры поставщика услуги SaaS	К
AV4	Специалист по защите кластера физических серверов поставщика	К
P1	Технический директор потребителя облачных услуг	СК
P2, P3	Руководители подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами	СК
A1	Начальник отдела автоматизации и безопасности потребителя	СК
A2	Администратор безопасности потребителя облачных услуг	СК
A3	Работник, осуществляющий интеграцию и сопровождение SaaS ИСОТ (менеджер ИСОТ)	СК
A4	Администратор штатных средств защиты потребителя	К
P4, P5	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия	К
P6, P7	Сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия	К

Окончание таблицы 2.3

1	2	3
P8, P9	Сотрудники подразделений потребителя облачных услуг, работающие по проектам 1 и 2 соответственно, не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ
P10	Сотрудник подразделения потребителя облачных услуг, не работающие по проектам 1 и 2, и не имеющие права эксплуатировать СОбВ в соответствии с бизнес-процессами	ОИ

Так как система облачных вычислений – это система, в которой взаимодействуют поставщик и потребитель облачных услуг, в диссертационной работе предложено модифицировать ролевую модель разграничения доступа таким образом, что каждая из представленных сторон (потребитель и поставщик) имеет свою максимальную роль в иерархии, в отличие от известной ролевой модели разграничения доступа, где максимальная роль в иерархи может быть только одна. Для поставщика облачных услуг максимальной ролью является роль технического директора поставщика (L1), для потребителя, соответственно, − технического директора потребителя облачных услуг (P1).

В общем случае иерархия ролей потребителя будет многоуровневой и распределенной. На рисунке 2.4 представлена разработанная иерархическая структура ролей для множества информационных субъектов и объектов для случая, когда $i=2$.

В примере, проиллюстрированном иерархией ролей на рисунке 2.4, потребитель облачных услуг имеет два подразделения, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами. В каждом из подразделений минимальная роль отводится сотрудникам потребителя облачных услуг, не имеющим права эксплуатировать СОбВ в соответствии с

бизнес-процессами (P8, P9, P10), а максимальная − руководителям подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами (P2, P3). Кроме того, в иерархии учтено, что два подразделения потребителя могут выполнять работу в СОбВ над разными проектами (проекты 1 и 2), которые, в соответствии с бизнес-процессами, не имеют общих и пересекающихся ресурсов и активов. Таким образом, сотрудники подразделения, работающего по проекту 1, не имеют доступ к информационным ресурсам и активам СОбВ подразделения, работающего по проекту 2, и наоборот.

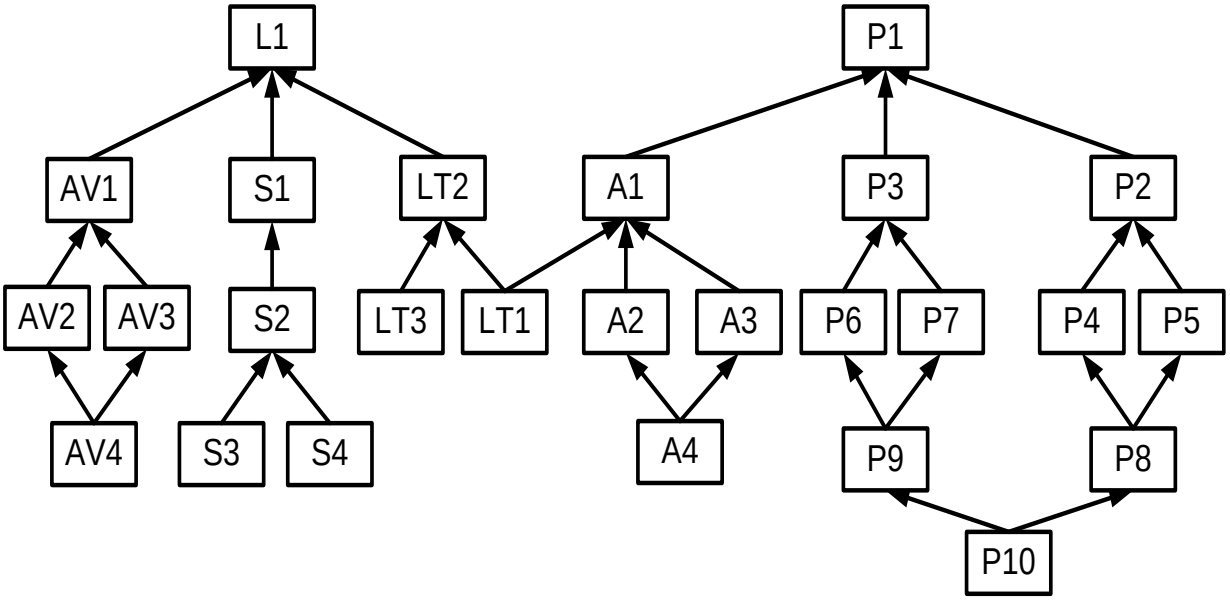


Рисунок 2.4 – Иерархическая структура ролей в СОбВ

В иерархии потребителя облачных услуг, помимо двух подразделений, работающих по проектам 1 и 2, есть третье подразделение, отвечающее за автоматизацию и информационную безопасность компании. Максимальная роль в этом подразделении отводится начальнику отдела автоматизации и безопасности потребителя облачных услуг (A1), а минимальная – администратору штатных средств защиты (A4), под которыми понимаются традиционные средства защиты, не входящие в систему безопасности облачной среды потребителя.

Иерархия поставщика облачных услуг, где максимальная роль отведена техническому директору поставщика (L1), состоит из трех служб-

отделов: служба поддержки потребителей облачных услуг, службы автоматизации облачной среды и службы информационной безопасности поставщика облачных услуг.

Служба поддержки потребителей состоит из трех линий (LT1, LT2, LT3) поддержки, которые взаимодействуют напрямую с потребителями облачных услуг и помогают конкретному поставщику решать возникающие вопросы и проблемы в реальном масштабе времени. В ходе исследований были выделены три возможные линии технической поддержки облаков [75]:

- сотрудники *первой линии* техподдержки поставщика облачных услуг (LT1), которые при обращении к ним потребителя ликвидируют технические сбои в инфраструктуре, влияющие на предоставляемые пользователям сервисы; данные сотрудники не обладают высокими привилегиями в СОбВ;
- сотрудники *второй линии* техподдержки поставщика облачных услуг (LT2) –группа специалистов высокого профиля, которая обладает достаточной компетенцией и способна решать проблемы как с инфраструктурой СОбВ, так и с ее сервисами;
- сотрудники *третьей линии* техподдержки поставщика облачных услуг (LT3) являются сотрудниками разработчика и производителя технологии облачных вычислений (Amazon, Google, Microsoft).

Служба автоматизации облачной среды ответственна за разработку и процесс интеграции в SaaS облачных вычислений со стороны потребителя облачных услуг; сотрудники службы занимаются вопросами оптимального управления облачными сервисами в условиях существующих ограничений сети потребителя облачных услуг. Максимальной ролью в данной службе будет обладать руководитель службы автоматизации ИСОТ (S1), а минимальными ролями будут обладать администратор инфраструктуры ИСОТ (S3) и эксперт по виртуализации в облачных вычислениях (S4).

Служба информационной безопасности поставщика облачных услуг отвечает за безопасность облачной среды со стороны поставщика облачных услуг. В данной службе роли распределены на три составляющие защиты

облака: защита программного обеспечения и платформ поставщика услуги SaaS (роль AV2), защита облачной инфраструктуры поставщика услуги SaaS (роль AV3) и защита кластера физических серверов поставщика облачных услуг (роль AV4). Максимальной в данной службе будет роль начальника службы безопасности облачного поставщика (AV1), а минимальной − специалист по защите кластера физических серверов поставщика облачных услуг (AV4).

Иерархия ролей пользователей СОбВ задает на множестве R отношение частичного порядка «≤», при котором выполняется условие: для u ∈ U, если r_i, r_j ∈ R, r_j ∈ UA(u) и $r_i \leq r_j$, то r_i ∈ UA (u). При этом для $r_i \leq r_j$ выполняется одно из условий: 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, $x_j \leq x_i$ [1,73,74].

Для иерархии ролей пользователей СОбВ выполняются следующие ограничения[1,73,74]:

- ограничение функции UA – для каждого пользователя u ∈ U роль x_read = ⊕ (UA(u) ∩ {y_read | y ∈ L}) UA(u) (здесь x = c(u)) и x_write = ⊕{y_write | y ∈ L} ∈ UA(u) (здесь x = ⊗L);

- ограничения функции roles – для каждой сессии s ∈ S множество ролей roles(s) = {x_read, x_write};

- ограничения функции PA – должно выполняться:

  – для каждого x ∈ L доступ (o, read) ∈ PA(x_read) тогда и только тогда, когда доступ (o, write) ∈ PA(x_write);

  – для каждого доступа (o, read) существует единственная роль x_read: (o, read) ∈ PA(x_read) (здесь x = c(o)).

Поставщик облачных услуг ни в коем случае не должен обладать какими-либо правами доступа к информации, которую обрабатывает потребитель в облаке. К такой информации относятся образы виртуальных машин потребителя, информационные ресурсы, хранящиеся в облачном хранилище, информационные ресурсы, хранящиеся на стороне потребителя

облачных услуг и экземпляры, запускаемые в физической операционной среде (физическом кластере поставщика). Кроме того, администраторы безопасности потребителя облачных услуг конфигурируют собственные виртуальные машины и конфигурационные файлы, относящиеся к конкретному потребителю, должны быть скрыты от служб поставщика. Таким образом, в СОбВ используются IP-адреса, каждый из которых ассоциируется с учетной записью клиента, а не с конкретным экземпляром виртуальной машины. Для запуска виртуальной машины ей должен быть присвоен атрибут, указывающий, какие учетные записи облачного web-сервиса имеют право запускать конкретную виртуальную машину.

Одновременно с этим, поставщик обладает правами на управление и конфигурирование внутриоблачного пространства и собственных сервисов безопасности, чтобы осуществить защиту данных конкретного потребителя не только от злоумышленников, но и от других потребителей услуг облака.

Таким образом, руководитель подразделения и сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 1 в соответствии с бизнес-процессами предприятия могут читать образы виртуальных машин (о3) по проекту 1 и имеют полный доступ на собственные экземпляры, запускаемые в физической операционной среде (о11). Соответственно, руководитель подразделения и сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по проекту 2 в соответствии с бизнес-процессами предприятия могут читать образы виртуальных машин (о3) по проекту 2 и имеют полный доступ на собственные экземпляры, запускаемые в физической операционной среде (о11). Вносить изменения в настройки конфигурационных файлов образов виртуальных машин и экземпляров, запускаемых в физической операционной среде, обоих проектов могут администратор безопасности потребителя облачных услуг и менеджер ИСОТ. Начальник отдела автоматизации и безопасности потребителя облачных услуг и технический

директор обладают полными правами по отношению к образам и экземплярам проектов своей организации.

Информационные ресурсы по проектам, хранящиеся в облачном хранилище (o4), и информационные ресурсы по проектам, хранящиеся на стороне потребителя облачных услуг (o10), доступны с полными правами руководителю соответствующего подразделения и сотрудникам потребителя облачных услуг, осуществляющие эксплуатацию СОбВ по соответствующему проекту в соответствии с бизнес-процессами предприятия, а также техническому директору потребителя облачных услуг.

К файлам СОбВ, относящимся к конфигурированию собственных виртуальных машин конкретным потребителем облачных услуг (o5), имеют полные права менеджер ИСОТ, начальник отдела автоматизации и безопасности потребителя и технический директор потребителя.

Правами на чтение множества логинов и паролей личных кабинетов сотрудников потребителя облачных услуг (o2) обладают сотрудники потребителя облачных услуг, осуществляющие эксплуатацию СОбВ в соответствии с бизнес-процессами предприятия. Данное множество доступно для специалиста по защите программного обеспечения и платформ и начальника службы безопасности облачного поставщика с правом вносить правки. Полными правами на доступ ко множеству логинов и паролей обладают руководители подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, начальник отдела автоматизации и безопасности потребителя и технический директор потребителя.

Чтение сайта поставщика облачных услуг (o1) могут осуществить все сотрудники потребителя облачных услуг без исключения. Кроме того, только правами на чтение сайта обладают следующие сотрудники поставщика облачных услуг: эксперт по виртуализации, специалист по защите кластера физических серверов, специалист по защите облачной инфраструктуры, администратор инфраструктуры ИСОТ, специалисты первой и третьей линии

техподдержки потребителя облачных услуг, специалист по защите программного обеспечения и платформ, начальник службы безопасности облачного поставщика. Полными правами на доступ к сайту обладают главный специалист ИСОТ, руководитель службы автоматизации ИСОТ, сотрудник второй линии техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг.

Данные об объеме предоставленных потребителю услуг (о9) доступны по чтению руководителям подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, сотрудникам службы автоматизации ИСОТ и техническому директору потребителя. Кроме того, прочесть эти данные могут специалист по защите облачной инфраструктуры, начальник службы безопасности облачного поставщика, сотрудник первой линии техподдержки, сотрудники службы автоматизации ИСОТ. Правами на чтение и на внесение правок в объем предоставленных потребителю услуг имеют только сотрудник второй линии техподдержки, руководитель службы автоматизации ИСОТ и технический директор поставщика облачных услуг.

Данные о серверном времени, скорости доступа и обработки данных, а также объем хранимых в облачном хранилище данных (о7) доступны по чтению руководителям подразделений потребителя, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами, администратору штатных средств защиты потребителя и администратору безопасности потребителя. Со стороны поставщика эти данные доступны по чтению для специалиста по защите облачной инфраструктуры, начальнику службы безопасности облачного поставщика, главному специалисту ИСОТ, администратору инфраструктуры ИСОТ и эксперту по виртуализации в облачных вычислениях. Полный доступ к объекту 7 имеют менеджер ИСОТ, начальник отдела автоматизации и безопасности потребителя облачных услуг и технический директор потребителя, а также руководитель службы автоматизации облачной среды, сотрудники первой и второй линии

техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг.

Данные о фактическом распределении доступа в едином пуле облака (о8) доступны по чтению со стороны поставщика специалисту по защите облачной инфраструктуры, начальнику службы безопасности облачного поставщика и эксперту по виртуализации в облачных вычислениях. Полный доступ к этим данным имеет руководитель и главный специалист службы автоматизации ИСОТ, сотрудники первой и второй линии техподдержки потребителя облачных услуг и технический директор поставщика облачных услуг. Так как начальник отдела автоматизации и безопасности потребителя, а также технический директор потребителя, наследуют все права сотрудника первой линии техподдержки, который в свою очередь является сотрудником поставщика облачных услуг, то они также имеют полный доступ к данным о фактическом распределении доступа в едином пуле облака.

Конфигурационные файлы внутриоблачного пространства и файлы поставщика, отвечающие за конфигурирование собственных средств безопасности поставщика (о6), должны быть закрыты для доступа любому сотруднику потребителя облачных услуг в целях повышения защищенности всей системы облачных вычислений. Вносить правки в файлы СОбВ, относящиеся к управлению внутриоблачным пространством поставщиком облачных услуг, может сотрудник третьей линии техподдержки потребителя, а по чтению они доступны специалисту по защите программного обеспечения и платформ поставщика и начальнику отдела безопасности поставщика. Полным доступом к файлам управления внутриоблачным пространством обладают сотрудники службы автоматизации (руководитель, главный специалист, администратор инфраструктуры и эксперт по виртуализации), сотрудники второй линии техподдержки и технический директор поставщика облачных услуг.

К файлам СОбВ, относящимся к сервисам безопасности поставщика облачных услуг, имеют полный доступ все сотрудники службы безопасности

поставщика облачных услуг (начальник службы, специалист защите ПО и платформ, специалист по защите инфраструктуры и специалист по защите кластера физических серверов), а также технический директор поставщика облачных услуг.

С учетом приведенных выше условий и ограничений в диссертационной работе разработана матрица доступа ролей пользователей (субъектов доступа) СОбВ к множеству объектов доступа, представленная в таблице 2.4.

Таблица 2.4 – Матрица прав доступа ролей пользователей СОбВ

	o1	***o2***	***o3 (1)***	***o3 (2)***	***o4 (1)***	***o4 (2)***	***o5***	***o6 (1)***	***o6 (2)***	***o7***	***o8***	***o9***	***o10 (1)***	***o10 (2)***	***o11 (1)***	***o11 (2)***
L1	rw	w	-	-	-	-	-	rw	rw	rw	rw	rw	-	-	-	-
LT2	rw	w	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
LT1	r	-	-	-	-	-	-	-	-	rw	rw	r	-	-	-	-
LT3	r	-	-	-	-	-	-	w	-	-	-	-	-	-	-	-
S1	rw	-	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
S2	rw	-	-	-	-	-	-	rw	-	r	rw	r	-	-	-	-
S3	r	-	-	-	-	-	-	rw	-	r	-	r	-	-	-	-
S4	r	-	-	-	-	-	-	rw	-	r	r	r	-	-	-	-
AV1	r	w	-	-	-	-	-	r	rw	r	r	r	-	-	-	-
AV2	r	w	-	-	-	-	-	r	rw	-	-	-	-	-	-	-
AV3	r	-	-	-	-	-	-	-	rw	r	r	r	-	-	-	-
AV4	r	-	-	-	-	-	-	-	rw	-	-	-	-	-	-	-
P1	r	rw	rwe	rwe	rw	rw	rw	-	-	rw	rw	r	rw	rw	rw	rw
A1	r	rw	rw	rw	-	-	rw	-	-	rw	rw	-	-	-	rw	rw
A3	r	rw	-	w	-	-	rw	-	-	rw	-	-	-	-	w	w
A2	r	rw	-	w	-	-	-	-	-	r	-	-	-	-	w	w
A4	r	rw	-	-	-	-	-	-	-	r	-	-	-	-	-	-
P2	r	rw	re	-	rw	-	-	-	-	r	-	r	rw	-	rw	-
P4,5	r	r	re	-	rw	-	-	-	-	-	-	-	rw	-	rw	-
P8	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P3	r	rw	-	re	-	rw	-	-	-	r	-	r	-	rw	-	rw
P6,7	r	r	-	re	-	rw	-	-	-	-	-	-	-	rw	-	rw
P9	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Полученные в виде матрицы разграничения доступа результаты разработки частной политики безопасности системы облачных вычислений

применяются при настройке средств контроля доступа в системе облачных вычислений и для определения полномочий прав пользователей (или запущенных ими процессов) на осуществление тех или иных процедур над защищенными данными. В СОбВ используются IP-адреса, каждый из которых ассоциируется с учетной записью клиента облачных вычислений. Для запуска виртуальной машины каждому IP-адресу должны быть присвоены соответствующие атрибуты, указывающие, какие учетные записи облачного web-сервиса имеют право запускать ту или иную конкретную виртуальную машину.

В таблице 2.5 представлено разработанное в диссертационной работе множество административных ролей СОбВ.

Таблица 2.5 − Множество административных ролей в СОбВ

Обозначение	***Наименование***
arv1	**Администратор *облачного сервера***
arv2	Администратор безопасности *облачного сервера*
arv3	Администратор *ИСОТ*
arv4	Администратор *службы автоматизации ИСОТ*
arv5	Администратор *технической поддержки ИСОТ*
ark1	**Администратор *облачного клиента***
ark2	Администратор *безопасности облачного клиента*
ark3	Администратор конфигурационных файлов *проекта 1*
ark4	Администратор конфигурационных файлов *проекта 2*

Проведенные в диссертационной работе исследования показали невозможность создания иерархии административных ролей, которая включала бы административные роли как потребителя, так и поставщика облачных услуг. Связанно это с тем, что при объединении административных ролей поставщика и потребителя в одну иерархию создаются пользователи, получающие по иерархии права суперпользователей, которые могут напрямую обращаться к результирующим потокам данных потребителя

облачных услуги управлять всеми конфигурационными файлами системы облачных вычислений.

Исходя из вышесказанного, в диссертационной работе было разработано две иерархические структуры в проекции на множество административных ролей, представленные на рисунке 2.5.

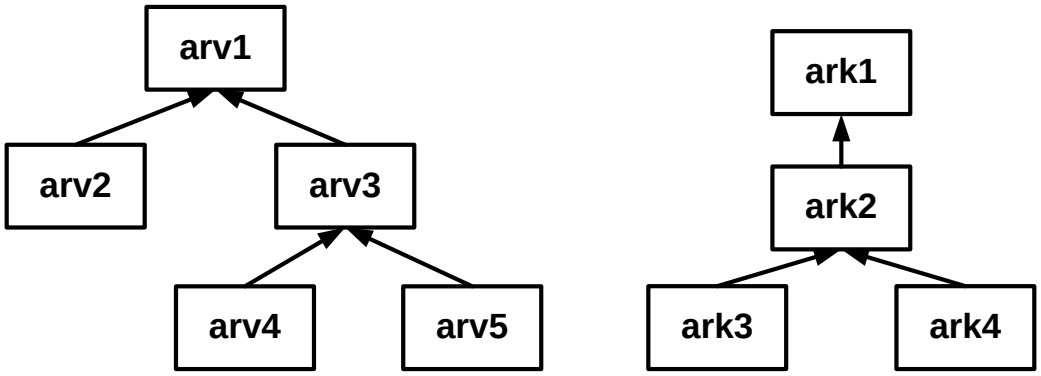


Рисунок 2.5 − Иерархии административных ролей в СОбВ

Для администрирования множеств авторизованных ролей пользователей на множестве административных ролей задаются следующие функции [1,73,74]:

• can-assign(): AR →CR ×2R – функция, определяющая для каждой административной роли множество ролей, которые могут быть включены в множество авторизованных ролей пользователя с использованием данной административной роли при выполнении заданных предварительных условий;

• can-revoke(): AR → 2^R– функция, определяющая для каждой административной роли множество ролей, которые могут быть исключены из множества авторизованных ролей пользователя с использованием данной административной роли.

В диссертационной работе разработаны значения функций can-assign() для административных ролей СОбВ, представленные в таблице 2.6.

Таблица 2.6 − Функции can-assign() для административных ролей

Административная роль	***Предварительное условие***	***Диапазон ролей функции can-assign***
arv1	AV, S	L1
arv2	AV and (not S1) and (not LT2)	AV1
	AV	AV2,AV3,AV4
arv3	S and (not LT2)	S1
	LT and not (S1)	LT2
arv4	S	S2,S3,S4
arv5	LT	LT3,LT1
ark1	A and (not (P3 or P2))	A1
	P10	P1
ark2	A	A2,A3,A4
	P10 and (not (A1 or P3))	P2
	P10 and (not (A1 or P2))	P3
ark3	P9	P6,P7,P9
ark4	P8	P4,P5,P8

В таблице 2.7 представлены разработанные функция can-revoke() для административных ролей в системе облачных вычислений.

Таблица 2.7 − Функция can-revoke() для административных ролей

Административная роль	***Диапазон ролей функции can-revoke***
1	2
arv1	L1
arv2	[AV1…AV4], L1
arv3	S1,LT2, L1
arv4	[S1..S4]

Окончание таблицы 2.7

1	2
arv5	[LT1…LT3]
ark1	P1
ark2	[A1…A4], P2,P3
ark3	P6,P7,P9
ark4	P4,P5,P8

Метод администрирования множества прав доступа аналогичен методу администрирования множества административных ролей. Для администрирования множеств прав доступа на множестве административных ролей задаются следующие функции:

• can-assign: AR →CR ×2R – функция, определяющая для каждой административной роли множество ролей, которые могут быть включены в множество прав доступа с использованием данной административной роли при выполнении заданных предварительных условий;

• can-revoke: AR → 2^R– функция, определяющая для каждой административной роли множество ролей, которые могут быть исключены из множества авторизованных ролей пользователя с использованием прав доступа данной административной роли.

Таблицы 2.8 и 2.9 показывают значения функций can-assign() и can-revoke() для прав доступа в частной политике безопасности СОбВ.

Таблица 2.8 − Функции can-assign() для прав доступа

Административная роль	***Предварительное условие***	***Множество ролей***
1	2	3
arv2	AV2 or AV3 and (not AV1)	AV4
	AV1 and (not AV2)	AV3
	AV1 and (not AV3)	AV2

Окончание таблицы 2.8

1	2	3
arv3	L1 and (not LT2)	S1
	L1 and (not S1)	LT2
arv4	S2 and (not S4)	S3
	S2 and (not S3)	S4
	S1	S2
arv5	LT2 and (not LT1)	LT3
	LT2 and (not LT3)	LT1
ark2	P1 and (not P3)	P2
	P1 and (not P2)	P3
	A1 and (not A3)	A2
	A1 and (not A2)	A3
ark3	P3 and (not P7)	P6
	P3 and (not P6)	P7
ark4	P2 and (not P5)	P4
	P2 and (not P4)	P5

Таблица 2.9 − Функция can-revoke() для прав доступа

Административная роль	***Множество ролей***
arv1	[AV1…AV4], [LT1…LT3], [S1...S4]
arv2	[AV2…AV4]
arv3	S1,LT2
arv4	[S2...S4]
arv5	LT1,LT3
ark1	[A1…AV4], [P2…P8]
ark2	A2,A3,P3,P2
ark3	P6,P7
ark4	P4,P5

В таблице 2.10 сформированы перечни возможностей для субъектов и объектов системы облачных вычислений, которые должны составлять основу для написания частной политики безопасности в СОбВ.

Таблица 2.10 – Перечень возможностей в СОбВ

№	*Обозначение*	*Наименование*
Права доступа		
1.	read	Право чтения
2.	write	Право записи
Возможности, связанные с сайтом потребителя /поставщика облачных услуг		
3.	o1_read	Просмотр содержания сайта
4.	o1_write	Изменение содержания сайта
Возможности, связанные с логинами и паролями от личных кабинетов		
5.	o2_read_own	Просмотр собственных логина и пароля
6.	o2_write_own	Изменение собственных логина и пароля
7.	o2_read_all	Просмотр всей базы логинов и паролей
8.	o2_write_all	Изменение всей базы логинов и паролей
Возможности, связанные с образами виртуальных машин		
9.	o3_read_own	Чтение образа ВМ
10.	o3_write_own	Запись в образ ВМ
Возможности, связанные с информационными ресурсами облачного хранилища		
11.	o4_read_own	Просмотр собственных ресурсов ОХ
12.	o4_write_own	Изменение собственных ресурсов ОХ
13.	o4_read_all	Просмотр всей базы ресурсов ОХ
Возможности, связанные с конфигурационными файлами СОбВ		
14.	o5_read_v	Просмотр конфигурационных файлов поставщика
15.	o5_read_own	Просмотр конфигурационных файлов потребителя
16.	o5_write_v	Изменение конфигурационных файлов поставщика
17.	o5_write_own	Изменение конфигурационных файлов потребителя
Возможности, связанные с данными серверном времени, скорости доступа и обработки данных, объема хранимых в хранилище данных		
18.	o6_read_own	Просмотр данных, связанных с конкретным потребителем облачных услуг
19.	o6_write_own	Изменение данных, связанных с конкретным потребителем облачных услуг
Возможности, связанные с данными о фактическом распределении доступа в едином пуле облака		
20.	o7_read	Просмотр данных
21.	o7_write	Изменение данных

Окончание таблицы 2.10

№	*Обозначение*	*Наименование*
Возможности, связанные с данными об объеме предоставленных потребителю услуг		
22.	o8_read	Просмотр данных
23.	o8_write	Изменение данных
Возможности, связанные с информационными ресурсами, хранящимися на стороне потребителя облачных услуг		
24.	o9_read	Просмотр информационных ресурсов
25.	o9_write	Изменение информационных ресурсов
Возможности, связанные с экземплярами физических серверов		
26.	o10_read	Просмотр сведений об экземплярах
27.	o10_write	Изменение экземпляров
28.	o10_write_all	Моментальный снимок экземпляра
29.	o11_write_own	Запуск собственного экземпляра физического сервера

Достоинством предложенной в диссертационной работе методики разработки частной политики информационной безопасности системы облачных вычислений с использованием формальной модели, основанной на математической модели ролевого разграничения доступа, является возможность *исключения* пользователей, получающих по иерархии ролей права *суперпользователей*, которые могут напрямую обращаться к результирующим потокам данных потребителя облачных услуг, а также управлять всеми конфигурационными файлами системы облачных вычислений. В методике предлагается ввести в иерархию две максимальные роли: одну со стороны поставщика потребителя облачных услуг (роль технического директора поставщика облачных услуг) и одну со стороны потребителя облачных услуг (роль технического директора потребителя облачных услуг), которые имели бы одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества, и *минимально необходимую роль* для поддержки бизнес-процессов СОбВ.

Соблюдение требований частной политики безопасности СОбВ позволит существенно снизить риски использования облачных вычислений, как со стороны поставщика, так и со стороны потребителя облачных услуг и,

как следствие, позволит увеличить доверие потенциальных потребителей к ИСОТ.

2.5 Разработка модели угроз в системе облачных вычислений на основе построения нечетких когнитивных карт с учетом инфраструктуры объекта защиты

2.5.1 Описание подхода когнитивного моделирования применительно к СОбВ

Научная проблема проведения аудита информационной безопасности на основе расчета рисков, заключающаяся в выявлении функциональной зависимости значения уровня риска от характеристик компонентов инфраструктуры с учетом сетевой топологии объекта защиты, от параметров имеющихся барьеров, а также от ценности обрабатываемой информации, была решена в работе [76].

Для потребителя облачных услуг уровень риска нарушения ИБ зависит от вероятностей реализации угроз информационным активам, которые обрабатываются в исследуемый период времени в среде инфраструктуры поставщика, а также от вероятностей угроз информационным ресурсам ограниченного доступа на стороне потребителя.

В диссертационной работе предложенная в [76] методология используется применительно к системе облачных вычислений для расчетов *прогнозируемых* численных значений уровней рисков в СОбВ в процессе проведения аудита информационной безопасности системы.

В диссертационной работе построена модель угроз СОбВ в виде нечетких когнитивных карт (НКК). Данный подход к построению модели угроз был впервые описан в [76].

Нечеткие когнитивные карты задаются в виде ориентированного графа и представляют моделируемую систему в виде множества концептов $\{K_1, K_2..K_o\}$, существенных для понимания исследуемой проблемы и связанных между собой отношениями влияния, отражающими причинно-следственные связи и показывающими степень влияния одного концепта на другой $w_{ij} \in W$ [77]. Термин «нечеткие» введен для обозначения того, что причинные связи могут принимать значения из диапазона действительных чисел $[0,1]$.

Как отмечается в [78], процесс составления НКК может рассматриваться как перевод знаний эксперта о проблемной ситуации на математический язык, таким образом, язык когнитивных карт является формализованным представлением практических знаний эксперта.

Согласно [77] путь между входным концептом {s} – источником угрозы и выходным концептом {o} – объектом атаки нечеткой когнитивной карты определяется следующим образом:

$$K_s \to K_o, \left(K_s, K_{z_1}, K_{z_2}, K_{z_3} ... K_{z_n}, K_o\right)_j, \tag{2.7}$$

где $n \in [1, n]$ – номер пути между входным K_S и выходным K_O концептами;

K_{z_n} – промежуточные концепты, соответствующие компонентам инфраструктуры (сервисы безопасности, коммуникационное оборудование, программное обеспечение);

$n \in [1, N]$– количество промежуточных концептов.

На рисунке 2.6 представлена обобщенная модель угроз в СОбВ в виде нечеткой когнитивной карты, в которой приведены начальные и конечные уязвимости компонентов инфраструктуры системы облачных вычислений на пути распространения атак.

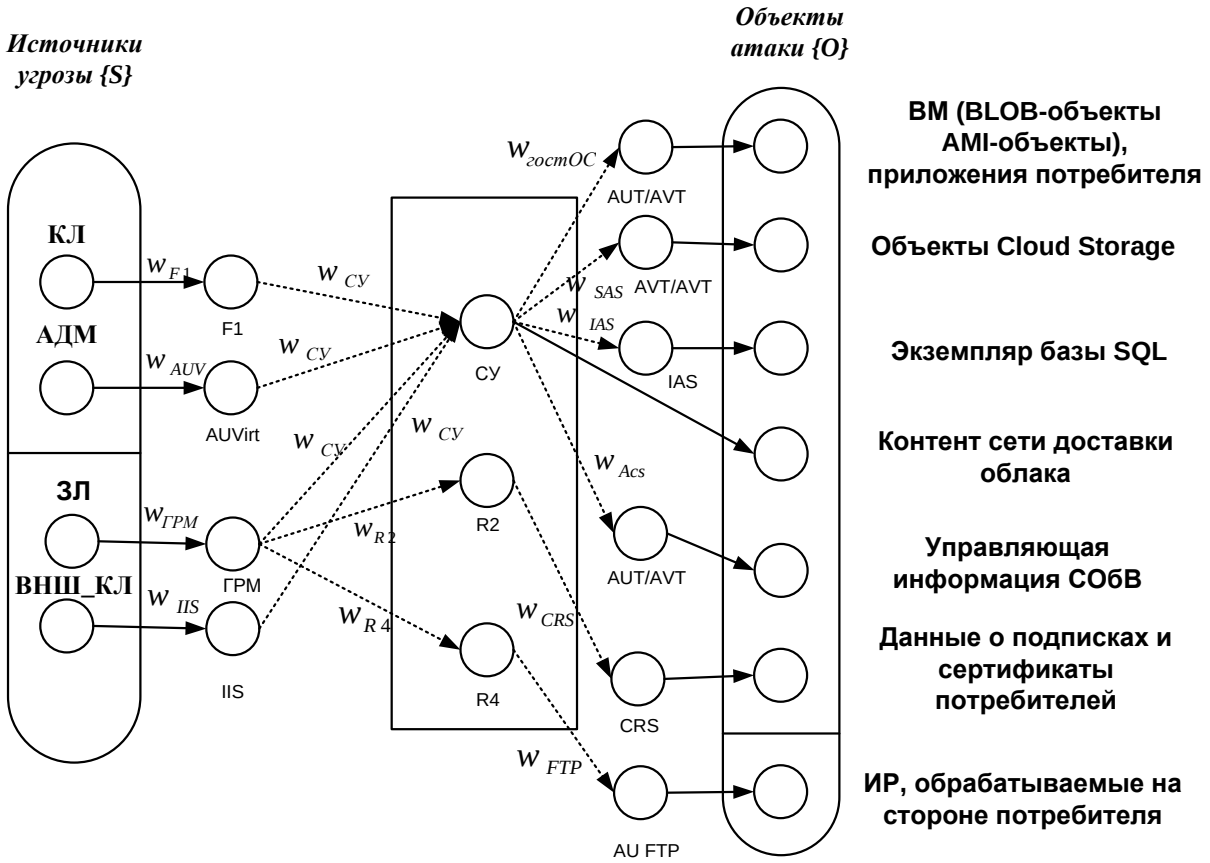


Рисунок 2.6 – Обобщенная модель угроз в виде НКК

На рисунке 2.6: КЛ – субъект доступа: сотрудник-нарушитель политики разграничения доступа компании потребителя облачных услуг; АДМ – субъект доступа: сотрудник службы поставщика облачных услуг; ВНШ_КЛ – субъект доступа: сторонний нарушитель – субъект являющийся другим потребителем облачных услуг облака сообщества (или запущенные им процессы); ЗЛ – субъект доступа: злоумышленник – субъект, не являющийся потребителем облачных услуг (или запущенные им процессы); w – соответствует уровням уязвимостей компонентов инфраструктуры СОбВ – промежуточным концептам; R – маршрутизатор; IIS – пограничный сервер; AUVirt, AUT, AVT, IAS – серверы аутентификации облака; FTP – файловый сервер; СУ – сервер управления. Оценки уровней уязвимостей получены с использованием методики CVSS и международной базы данных уязвимостей (NVD) [79].

Использование нечетких когнитивных карт позволяет произвести моделирование процессов распространения угроз информационной системе

через используемые уязвимости ее компонентов. При этом полученная модель обладает свойством *наглядности* и простотой *понимания и перевода* содержательного знания эксперта на математический язык.

Анализ визуализированных путей реализации угроз служит основой для обоснования выбора средств защиты – барьеров на пути реализации угроз, снижающих значение риска нарушения ИБ до приемлемого уровня.

2.5.2 НКК1 – модель угроз несанкционированного доступа, реализуемого злоумышленником и другим потребителем облачных услуг, НКК2 – модель угроз несанкционированного доступа, реализуемого администратором поставщика и нарушителем со стороны потребителя облачных услуг

Нечеткая когнитивная карта *отражает* процесс реализации угроз *через уязвимости* компонентов инфраструктуры, реализуемых на уровнях оборудования, управления и оркестровки ИСОТ .

При увеличении уровня уязвимости промежуточного концепта упрощается переход от одного барьера к другому на пути реализации угрозы, и тем самым понижается уровень защищенности соответствующих информационных ресурсов.

Для построения модели угроз необходимо располагать сведениями об уязвимостях сетевой инфраструктуры и используемых в СОбВ сервисах безопасности. В диссертационной работе каждому компоненту инфраструктуры соответствует значение его уязвимости, из базы данных уязвимостей National Vulnerability Database [79].

После определения входных данных – сведении об уязвимостях сетевой инфраструктуры и используемых в СОбВ сервисах безопасности, а также источниках и объектах атаки, необходимо определить *все* возможные пути реализации угроз.

На рисунке 2.7 с учетом установленных сервисов безопасности и компонентов инфраструктуры составлена нечеткая когнитивная карта (НКК) − модель угроз несанкционированного доступа злоумышленника, с целью проникновения с удаленного компьютера внутрь защищаемой системы облачных вычислений и модель угроз несанкционированного доступа, реализуемого сотрудником-нарушителем другого потребителя облачных услуг, удаленно имеющим определенные права в системе облачных вычислений и пытающимся превысить уровень своих полномочий.

На рисунке 2.8 приведена НКК – модель внутренних угроз, реализуемых сотрудником (администратором) поставщика облачных услуг и сотрудником-нарушителем компании потребителя облачных услуг, соответственно.

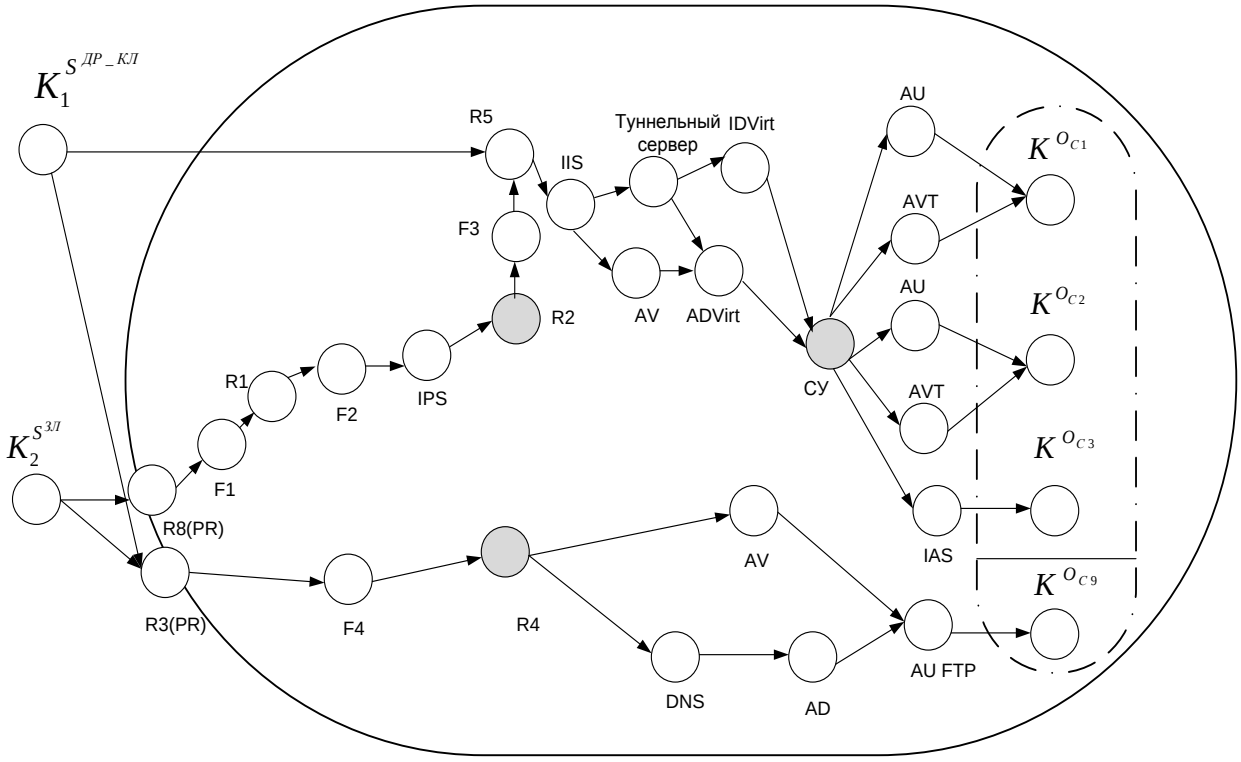


Рисунок 2.7 − НКК1 – модель угроз несанкционированного доступа, реализуемого злоумышленником и другим потребителем облачных услуг

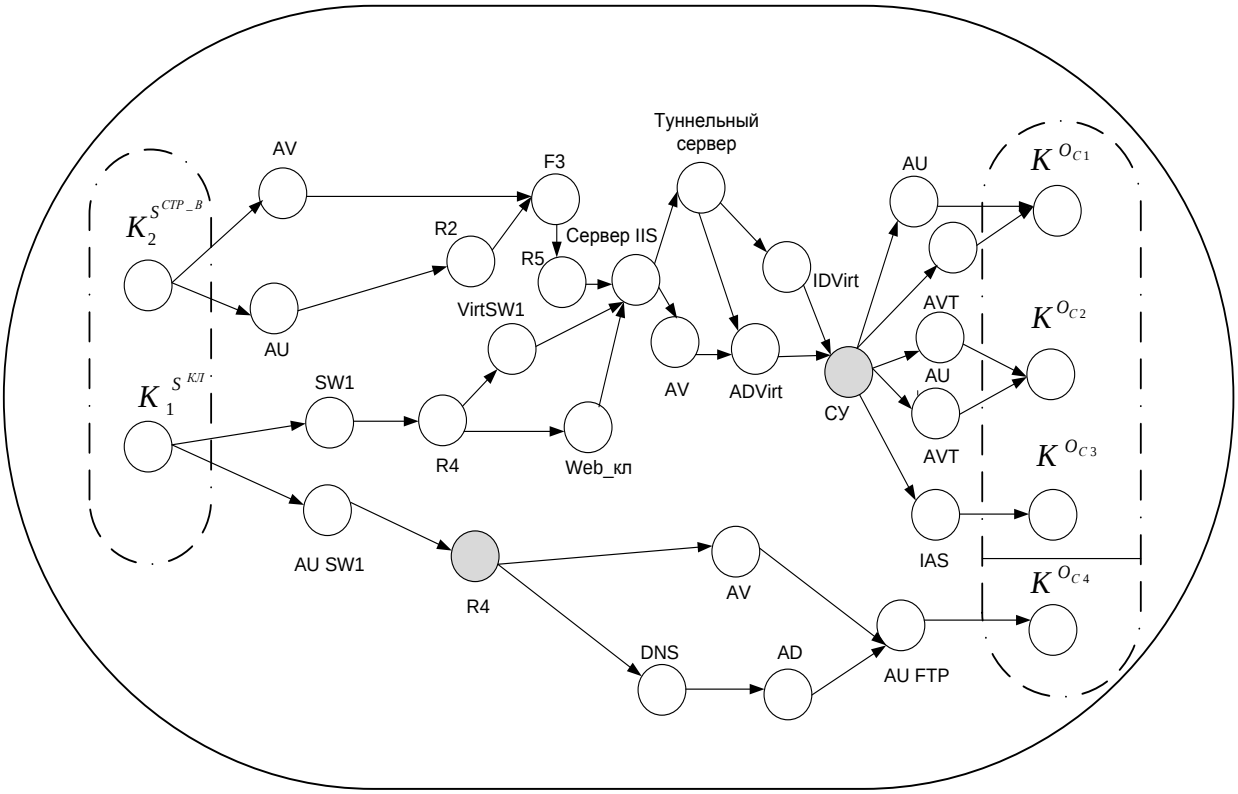


Рисунок 2.8 – НКК2 – модель угроз несанкционированного доступа, реализуемого администратором поставщика и нарушителем со стороны потребителя облачных услуг

На рисунках: $K_i^{ВНШ\_КЛ}$ – субъект доступа: сторонний нарушитель – субъект являющийся другим потребителем облачных услуг (или запущенные им процессы); $K_i^{ЗЛ}$ – субъект доступа: злоумышленник – субъект, не являющийся потребителем облачных услуг (или запущенные им процессы); $K_i^{адм}$ – субъект доступа: администратор поставщика облачных услуг; $K_i^{КЛ}$ – субъект доступа: сотрудник-нарушитель компании потребителя облачных услуг; K_y^{C1} – объект атаки: виртуальные машины и облачные приложения потребителя; K_y^{C2} – объект атаки: объекты cloud Storage; K_y^{C3} – объект атаки: экземпляр базы SQL; K_y^{C4} – объект атаки: информационные ресурсы, обрабатываемые на стороне потребителя облачных услуг; PR – граничный маршрутизатор; AV –антивирус; F – межсетевой экран; R – маршрутизатор; IIS – внутренний web-сервер для клиент-серверного межоблачного взаимодействия; FTP – файловый сервер; VirtSW – виртуальный коммутатор; СУ – сервер управления.

Когнитивная карта иллюстрирует возможные пути угроз, реализуемых потенциальным злоумышленником и нарушителем, позволяет провести анализ несанкционированного проникновения к информационным ресурсам: показывает, откуда проводится атакующее воздействие, какие объекты могут являться целями проведения атак, какими средствами защищена информационная система, какие уязвимости могут быть использованы во время атаки.

Модель угроз в СОбВ, разработанная на основе построения нечетких когнитивных карт, *адекватна* объекту защиты, потому что позволяет обеспечить оценку угроз нарушения информационной безопасности на всех уровнях ИСОТ. Преимуществом использования НКК в данном приложении в сравнении с какими либо другими методами является возможность учесть инфраструктуру потребителя и поставщика облачных услуг, уязвимости функциональных и пограничных серверов, а также облачных хранилищ данных, формализовать численно неизмеримые факторы, такие как вероятности угроз.

2.6 Выводы по второй главе

1. Разработана архитектура системы облачных вычислений для облака сообщества и концепции вычислительного облака для обеспечения услуги SaaS, в которой учитываются требования для типовой информационной системы, построенной на основе технологии облачных вычислений, и требования архитектуры безопасности сетей.

2. На основе абстрактно-алгебраического подхода, сформированного в диссертационной работе перечня потенциально возможных угроз СОбВ и их источников, с *учетом особенностей* технологии

облачных вычислений предложено формализованное описание системы защиты информации СОбВ.

3. Предложены *модель политики* информационной *безопасности* ИСОТ и *методика разработки частной политики безопасности* СОбВ, *позволяющие назначить* несколько максимальных ролей, которые имеют одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества, и *минимально необходимую роль* для поддержки бизнес-процессов СОбВ и *исключить* из иерархии ролей роль *суперпользователя*, имеющего полномочия напрямую обращаться к результирующим потокам данных, *управлять* всеми конфигурационными файлами СОБВ, и *увеличить* доверие потенциальных потребителей к ИСОТ.

4. Разработана модель преднамеренных (целенаправленных) угроз нарушения информационной безопасности в системе облачных вычислений, основанная на построении нечетких когнитивных карт, которая позволяет учесть угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, а также учесть такой источник угроз как другой потребитель облачных услуг, который, являясь клиентом облака сообщества, должен обслуживаться поставщиком изолированно от потребителя облачных услуг.

ГЛАВА 3. МЕТОД ПРОВЕДЕНИЯ ЭКСПЕРТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

В данной главе разрабатывается метод проведения экспертного аудита ИБ системы облачных вычислений на основе использования искусственной нейронной сети.

Доказана возможность использования искусственной нейронной сети для проведения экспертного аудита на основе численного оценивания оперативного значения риска нарушения ИБ в СОбВ, формализованы условия достаточности множества данных обучающей выборки для хорошей натренированности ИНС с учетом требований репрезентативности, сформировано множество данных обучающей выборки для обучения ИНС на основе прогнозируемых значений уровня риска нарушения ИБ для СОбВ, выбрана архитектура нейронной сети и оценены возможные алгоритмы обучения ИНС для решения поставленной задачи, разработана функциональная модель, наглядно иллюстрирующая предложенный в диссертационной работе метод проведения экспертного аудита ИБ в СОбВ.

Результаты данной главы опубликованы в работах [42,70,105,106,107].

3.1 Проведение аудита информационной безопасности с точки зрения системного анализа

Аудит информационной безопасности (ИБ) – один из аспектов управления ИБ. Аудит целесообразно проводить после разработки системы обеспечения информационной безопасности (СОИБ) для оценивания результатов проектирования; аудит проводится периодически в ходе

эксплуатации информационной системы (ИС) для оценки эффективности существующих мер защиты, активный аудит проводится при расследовании важности инцидентов ИБ в режиме реального времени.

Качество аудита безопасности зависит от адекватности информации об объекте оценки: сведений о топологии сети, сведений об инфраструктуре информационной системы, об установленных средствах защиты, об используемой политике информационной безопасности, программном обеспечении, схеме информационных потоков.

Аудит нарушения ИБ обеспечивает получение и *оценку* объективных данных о текущем состоянии защищенности информационной системы. Необходимость осуществления аудита безопасности связана со сложностью инфраструктуры современных ИС, множеством используемых приложений, обрабатываемым объемом данных, сложностью реализации системы информационной безопасности, необходимостью учета всего спектра потенциально возможных угроз.

Существует множество определений аудита информационной безопасности представленных в [2,69,80,81,82,83,84].

В диссертационной работе под аудитом безопасности ИС понимается экспертиза состояния защищенности, включающая *получение объективных данных* о параметрах и условиях функционирования системы, которые могут влиять на защищенность, *и их анализ*. В результате эксперт выявляет, насколько рационально решены вопросы безопасности информации и контроля доступа, как минимизировать риски при обработке в ИС конфиденциальной информации заказчика, выявляет локализацию слабых мест в системе обеспечения информационной безопасности и выдает рекомендации о путях решения существующих проблем.

Для осуществления процедуры анализа исходных данных аудитор может применить методику, которая позволила бы оценить соответствие используемых в системе обеспечения информационной безопасности механизмов защиты требованиям существующих стандартов

информационной безопасности. Однако на сегодняшний день такие методики отсутствуют [1], а стандарты информационной безопасности для облачных сред находятся в процессе разработки [82].

Другой подход к проведению анализа в ходе аудита основан на *оценке рисков*. В этом случае должны быть идентифицированы все возможные угрозы, выявлены и оценены уязвимости. Эксперт в аудиторском отчете указывает используемый им при анализе метод расчета информационных рисков.

Учитывая, что угрозы нарушения ИБ характеризуются многоаспектностью происходящих событий и альтернативностью сценариев, а на процесс проведения аудита с использованием метода оценки рисков нарушения информационной безопасности оказывает влияние большое количество и многообразие факторов, влияющих на результат экспертизы, воздействие которых часто не удается однозначно выявить и описать строго математически, то проблему проведения экспертного аудита ИБ можно отнести к числу *сложных слабоструктурированных* и *слабоформализуемых* проблем.

В науке имеется опыт по решению подобных слабоформализуемых проблем – это *системный анализ* объектов исследования [86]. Его конструктивность обусловлена тем, что он является методом, позволяющим учесть при решении проблемы все существенные факторы [87].

Методы системного анализа – декомпозиция, анализ и синтез системы, снимающей или ослабляющей проблему практики. В процессе исследования используются основные принципы системного анализа, сформулированные в [87] применительно к процессу проведения аудита ИБ.

В диссертационной работе *сформирован* следующий вариант декомпозиции проведения аудита информационной безопасности:

- анализ проблемы обеспечения ИБ в облачных средах (1 глава);
- разработка формализованного описания системы защиты информации СОбВ (2 глава);

- разработка частной политики безопасности для СОбВ (2 глава);
- разработка модели угроз нарушения ИБ с использованием нечетких когнитивных карт (2 глава);
- обучение ИНС и получение численных значений оперативного уровня риска нарушения информационной безопасности.

Для решения последней задачи необходимо:

- сформировать множество данных обучающей выборки для настройки параметров искусственной нейронной сети (ИНС) (3 глава);
- осуществить выбор эффективного алгоритма обучения искусственной нейронной сети (3 глава);
- разработать программный модуль для получения численных значений оперативного уровня риска нарушения ИБ с помощью нейронной сети.

Результаты исследования и поэтапного решения проблемы проведения аудита ИБ приводятся в диссертационной работе.

3.2 Разработка метода и структурной схемы, реализующей метод проведения экспертного аудита информационной безопасности в системе облачных вычислений

Система облачных вычислений является информационной системой взаимодействия потребителя и поставщика облачных услуг. С точки зрения информационной безопасности в процессе обеспечения выполнения бизнес-процессов такой системы могут возникнуть угрозы ИБ, связанные с потерей доверия потребителя к поставщику СОбВ. Эти угрозы возникают по причине отсутствия достоверного оценивания уровня доверия к поставщику облачных услуг в связи с закрытостью для собственных пользователей применяемых поставщиком облачных технологий и программных решений. Кроме того,

пользователи облачных услуг не обладают возможностью дать оценку реализованного уровня защищённости информации, достигнутого поставщиком.

В данном случае необходимо проведение *независимого аудита СОбВ* с последующим предоставлением результатов потребителю в качестве гаранта сохранности его критичных активов.

Одним из преимуществ использования облачных услуг является возможность осуществления выбора и изменения *первоначального состава ПО* уже после ввода системы облачных вычислений в эксплуатацию. Однако в этих условиях система, рассматриваемая как защищённая на этапе проектирования, после ввода её в эксплуатацию может обладать множеством уязвимостей, содержащихся в новом ПО. Таким образом, можно сделать вывод о необходимости проведения *периодического* независимого аудита информационной безопасности СОбВ.

Проведение аудита ИБ на сегодняшний день становится все более востребованной на рынке услуг информационной безопасности не только в облачных средах, но и в традиционных ИС.

Аудит ИБ является совокупностью трех важнейших составляющих: методологии аудита, включающей в себя модели, средства и методы проведения аудита; результат проведения аудита (качественный или количественный); эталонная система обеспечения ИБ, с которой сравниваются результаты проверки информационной системы. Взаимосвязь этих трех компонентов аудита ИБ представлена на рисунке 3.1.

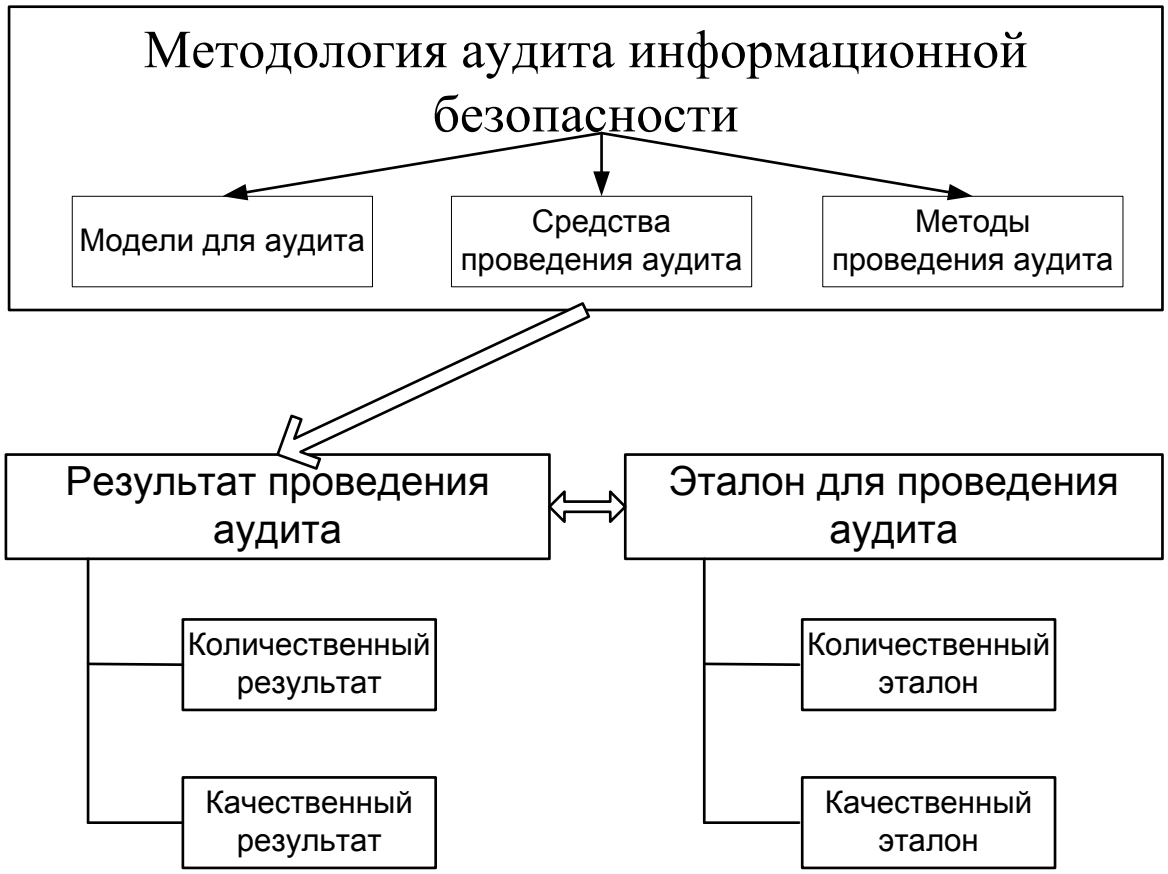


Рисунок 3.1 – Составляющие аудита ИБ

Качество проводимого аудита безопасности во многом зависит от полноты и точности информации, которая была получена в процессе сбора исходных данных. Поэтому информация должна включать в себя: существующую организационно-распорядительную документацию, касающуюся вопросов информационной безопасности, сведения о программно-аппаратном обеспечении системы, а также информацию о средствах защиты, установленных в ИС.

Различают следующие виды аудита ИБ систем:

● инструментальный (активный) аудит – выявление уязвимостей программного и аппаратного обеспечения систем средствами автоматизированной проверки. Результатом активного аудита является информация об уязвимостях системы защиты информации, степени их критичности, а также, в ряде случаев, методах устранения. По окончании активного аудита выдаются рекомендации по модернизации системы защиты

информации, которые позволяют устранить уязвимости системы защиты информации и тем самым повысить уровень защищенности информационной системы в целом. *В качестве недостатка* активного аудита в ряде источников, таких как [84, 88], отмечают то, что без проведения других видов аудита эти рекомендации могут оказаться недостаточными для создания максимально эффективной системы защиты информации;

● *экспертный аудит* информационной безопасности – подразделяется на *аудит соответствия отечественным стандартам* информационной безопасности, при котором состояние информационной безопасности сравнивается с неким абстрактным описанием, приводимым в стандартах, и на экспертный аудит, целью которого является исследовать уровень защищенности системы.

Основным *недостатком* и *открытым вопросом* при проведении *аудита ИБ на соответствие стандартам* является вопрос о стандартах безопасности, проверку на соответствие которому будет выполнять аудитор [89]. Кроме того, если стандарты в области ИБ отсутствуют или находятся на стадии разработки, то провести аудит на соответствие стандартам становится невозможным. В таком случае единственным способом проведения экспертного аудита является исследование *уровня защищенности системы*, при этом аудитор должен использовать *методологию*, позволяющую провести *оценку рисков нарушения информационной безопасности* системы.

Как уже отмечалось в диссертационной работе ранее, аудит ИБ на соответствие требованиям существующих стандартов в области защиты информации, невозможно провести для ИСОТ, в силу того, что подходящие стандарты для облачных вычислений отсутствуют в нормативной правовой базе РФ или находятся в стадии разработки

Для проведения аудиторской проверки поставщиком облачных услуг с целью увеличения доверия потенциальных потребителей к ИСОТ, а также с целью обосновать выбор барьеров на пути реализации угроз, снижающих значение риска нарушения ИБ облака сообщества до приемлемого уровня

необходима объективная оценка степени защищенности данных потребителя облачных услуг в облачной инфраструктуре поставщика.

В результате аудита информационной безопасности ИСОТ можно выявить, насколько рационально решены вопросы безопасности информации и контроля доступа в облачной среде, определить, как минимизировать риски при обработке в ИСОТ конфиденциальной информации потребителя облачных услуг, локализовать слабые места в системе обеспечения информационной безопасности и сформулировать рекомендации о путях решения существующих проблем безопасности в системе. Кроме того, потребитель заинтересован в определении поставщиком конкретного объективного механизма для оценки качества предлагаемой облачной услуги.

В международных и российских стандартах в области информационной безопасности сформированы требования к *методологии оценивания рисков* нарушения ИБ [23]. Методология должна обеспечивать получение *численных значений* уровня риска, помогать осуществлять внутренний аудит для обоснования *выбора корректирующих действий в процессе менеджмента* защиты информации, обеспечивать способность к *быстрой адаптации* при изменении компонентов инфраструктуры, должна гарантировать, что метод оценки рисков дает *сравнимые* и *сопоставимые* результаты.

На сегодняшний день отсутствует методология экспертного аудита ИБ, которая удовлетворяла бы всем перечисленным выше требованиям [84]. Что касается рекомендаций и методик экспертного аудита ИБ в системе облачных вычислений, то они отсутствуют не только в нормативной базе РФ, но и в законодательных актах других стран [85].

Разработанная методология аудита информационной безопасности системы должна *учитывать* множественность субъектов и объектов атаки, флюктуируемость системы облачных вычислений, должна *обеспечивать* наиболее вероятные численные результаты проведения аудита даже при возможном *отсутствии некоторых необходимых для расчетов входных данных*. На сегодняшней день наиболее эффективным инструментом для

решения подобных задач являются современные интеллектуальные системы, среди которых можно выделить *искусственные нейронные сети*.

В диссертационной работе разработан метод проведения экспертного аудита СОбВ, удовлетворяющий всем перечисленным выше требованиям к методологии оценивания рисков нарушения ИБ [90] и адаптирующий известные возможности искусственных нейронных сетей для создания программного модуля, который реагировал бы в реальном масштабе времени на любые изменения данных с датчиков событий, а также выдавал бы объективные численные результаты расчета риски нарушения ИБ СОбВ даже при отсутствии части необходимых для расчета входных данных.

Искусственная нейронная сеть (ИНС) − это самообучающаяся интеллектуальная информационная система, которая строит ассоциативную сеть понятий (нейронов) для параллельного поиска решений с помощью обучения на множестве данных обучающей выборки

В результате обучения строятся математические решающие функции (передаточные функции или функции активации), которые определяют зависимости между входными и выходными сигналами нейронной сети.

Искусственный нейрон – это элементарный преобразовательный элемент, имеющий непустое множество входов, на которые поступают сигналы (входные данные). Функционирует нейрон в два такта, на первом такте в суммирующем блоке вычисляется величина возбуждения полученного нейроном. Другими словами, в нейрон от других нейронов приходит какое-то число сигналов, обработав их, нейрон передает выходной сигнал далее, другому нейрону. На втором такте суммарное возбуждение пропускается через активационную (преобразующую) функцию в результате чего получается выходной сигнал нейрона. Обобщенная структура нейрона представлена на рисунке 3.2

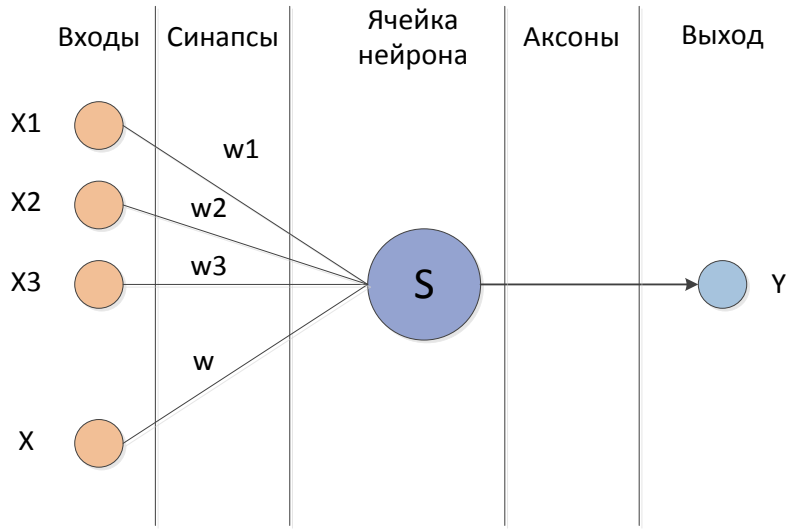


Рисунок 3.2 – Структура нейрона

На рисунке 3.2:

− синапс − однонаправленная входная связь нейрона, соединенная с выходом другого нейрона, которая имеет свой вес;

− аксон − единственный отросток биологического нейрона, по которому он передает свой выходной сигнал.

Обучение нейронной сети сводится к определению связей (синапсов) между нейронами и установлению силы этих связей (весовых коэффициентов). Алгоритмы обучения нейронной сети упрощенно сводятся к определению зависимости весового коэффициента связи двух нейронов от числа примеров, подтверждающих эту зависимость.

Достоинство нейронных сетей перед такой интеллектуальной системой как *индуктивный вывод* заключается в решении не только классифицирующих задач, но и задач поиска закономерностей в массивах данных. Возможность нелинейного характера функциональной зависимости выходных и входных признаков позволяет расширить диапазон решаемых задач с помощью данной интеллектуальной системы.

Сам процесс решения задач в силу проведения матричных преобразований проводится очень быстро и достаточно точно, что является несомненным *достоинством нейронных сетей по сравнению с абдуктивными системами*. В искусственной нейронной сети фактически

имитируется параллельный процесс прохода по нейронной сети в отличие от последовательного в индуктивных и абдуктивных системах. Кроме того, нейронные сети легко могут быть *реализованы в виде программного модуля* с ассоциативной памятью, что позволяет автоматизировать решаемые задачи.

Таким образом, в качестве инструмента для создания методологии экспертного аудита ИБ в диссертационной работе была выбрана именно искусственная нейронная сеть.

Разработанная методология использует теорию искусственных нейронных сетей, а также множество данных обучающей выборки, созданное на основе расчетных данных по методу оценки рисков, предложенного в [76,91].

При решении проблемы оценивания рисков нарушения ИБ в диссертационной работе предложено использовать *два* различных *подхода* для определения риска: оценивание *прогнозируемого* значения и *оперативного* значения уровня риска нарушения ИБ. Это обуславливается тем, что при определении соответствия системы защиты СОбВ требованиям потребителя облачных услуг, важно оценить не только значение уровня риска нарушения информационной безопасности с учетом наиболее полного перечня потенциально возможных угроз, но и *оперативное* значение риска, когда угроза проявляется по конкретному пути распространения в реальном масштабе времени.

Оценка *прогнозируемого* значения риска связана со *стратегией* безопасности, которая разрабатывается для СОбВ заблаговременно. В ходе мониторинга безопасности системы обеспечивается получение информации о состоянии сетевых устройств в облаке, о событиях, нарушающих безопасность, в *реальном масштабе времени*. При проявлении атаки или обнаружении таких событий в СОбВ необходимы *тактические* действия. Тактические действия должны быть результатом организованного взаимодействия систем мониторинга и управления устройствами сетевой безопасности. Принять решение о том, какие именно тактические действия

необходимо применять в данный конкретный момент времени, поможет численное *оперативное* значение уровня риска. Взаимосвязь понятий прогнозируемого и оперативного риска показана на рисунке 3.3.

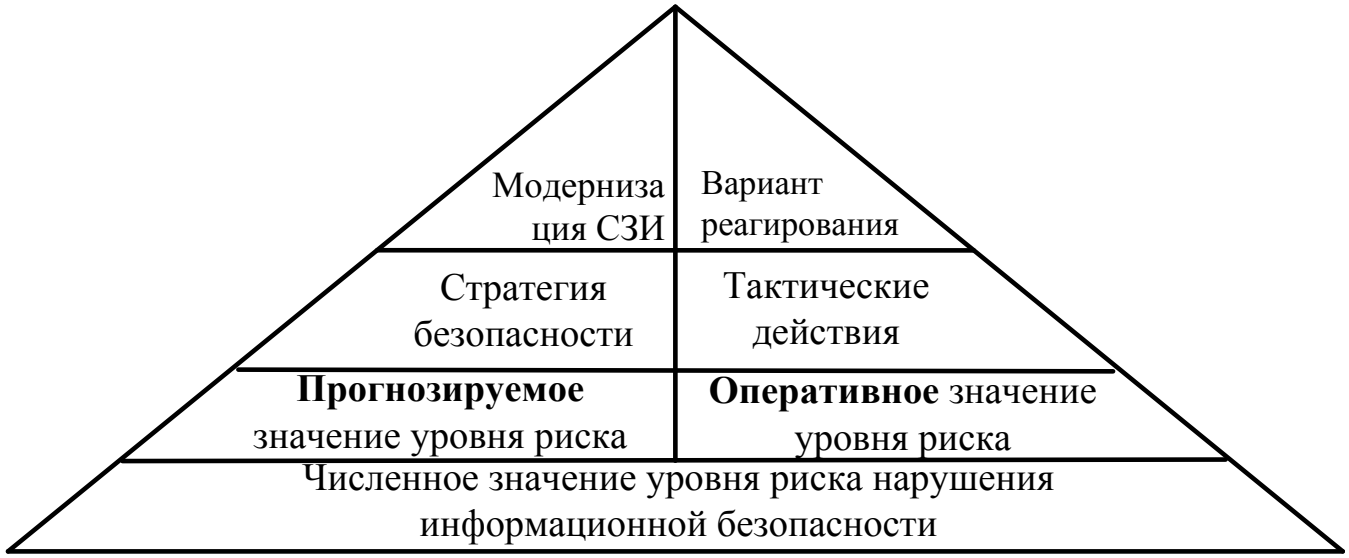


Рисунок 3.3 – Взаимосвязь прогнозируемого и оперативного значения уровня риска нарушения информационной безопасности

Результаты расчетных прогнозируемых значений риска было предложено использовать в качестве множества данных обучающей выборки для ИНС. На выходах нейронной сети аудитор получит оперативное значение риска в реальном масштабе времени.

Таким образом, метод экспертного аудита, предложенный в диссертационной работе, включает в себя следующие этапы:

- построение модели угроз в виде нечеткой когнитивной карты;
- расчет прогнозируемых значений уровня риска нарушения информационной безопасности системы облачных вычислений;
- формирование множества данных обучающей выборки для обучения искусственной нейронной сети, настройка и обучение ИНС;
- определение оперативного значения уровня риска аудитором в реальном масштабе времени на основе данных с датчиков событий;
- формирование отчета аудитора на основе полученных значений уровня риска.

Разработанный в диссертационной работе метод экспертного аудита ИБ, применительно к системе облачных вычислений, показан на рисунке 3.4.

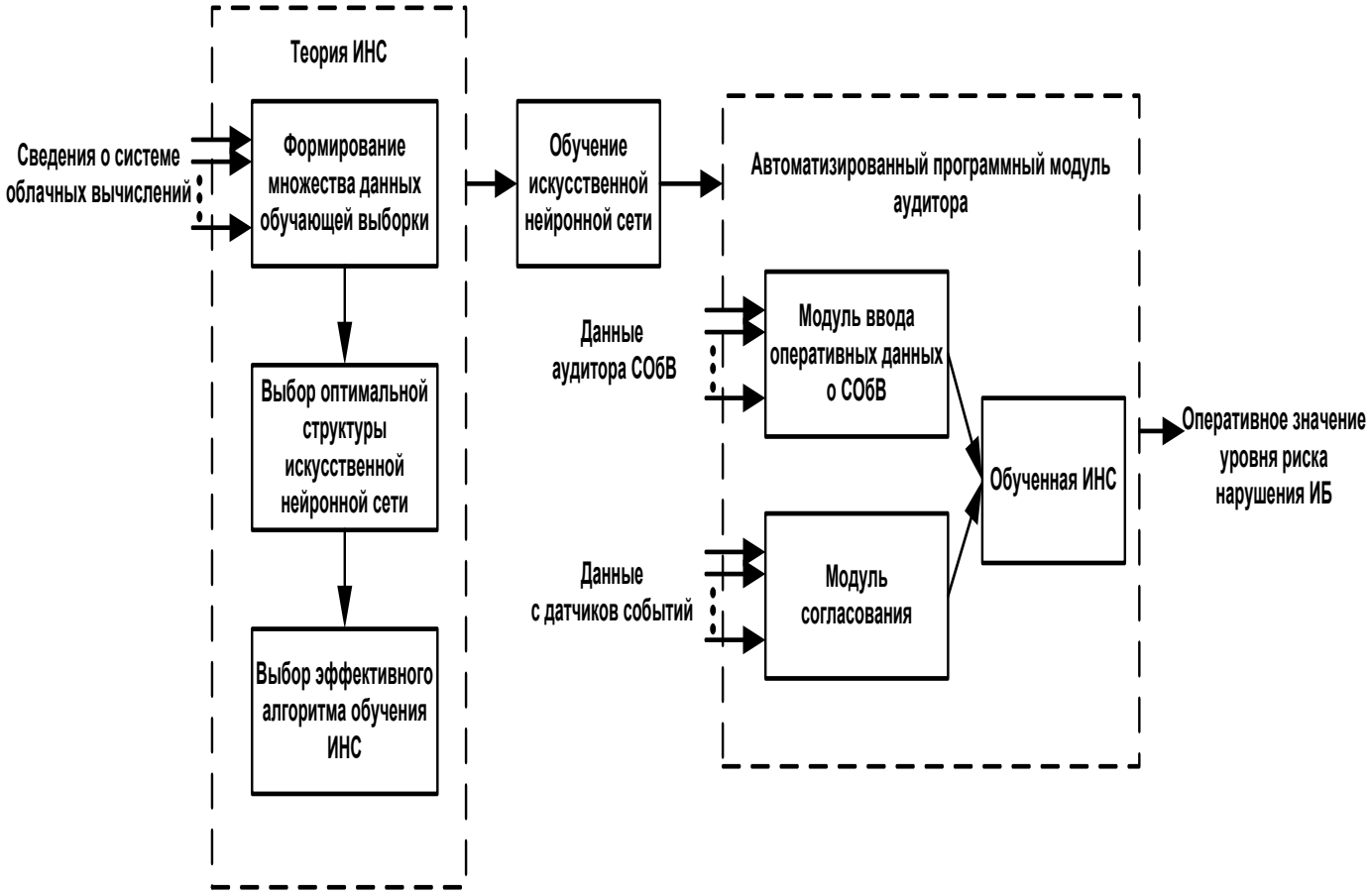


Рисунок 3.4 – Схема, иллюстрирующая метод проведения экспертного аудита СОбВ

Для успешного использования нейронных сетей аудитором ИБ необходимо сформировать множество данных обучающей выборки, исходя из текущих сведений о рассматриваемой системе. Далее производится выбор оптимальной структуры нейронной сети и выбор эффективного по своим параметрам алгоритма обучения ИНС, в которых будет учитываться специфика обучающей выборки. После успешного обучения и тестирования нейронной сети на контрольных примерах, необходимо загрузить сведения о синапсах между нейронами и весовые коэффициенты в автоматизированный программный модуль, который использует специалист для проведения аудита ИБ СОбВ.

После обучения ИНС в составе системы управления ИБ обеспечит получение оперативного значения риска нарушения информационной безопасности с учетом актуальных данных, полученных в процессе мониторинга инфраструктуры СОбВ датчиками событий, и данных о системе облачных вычислений, находящихся в распоряжении аудитора. На вход обученной ИНС подается информация с выхода модуля ввода оперативных данных о СОбВ и с модуля согласования данных, в котором на основе оперативных данных (полученных с сенсоров систем обнаружения вторжений, антивирусов, с межсетевых экранов и других компонентов инфраструктуры), выявляется источник актуальной угрозы. На выходе автоматизированного программного модуля аудитора формируется оперативное значение риска нарушения ИБ.

Результаты расчетов рисков нарушения ИБ в СОбВ при проведении экспертного аудита могут быть использованы поставщиком облачных слуг при обсуждении с потребителем применяемых стратегий безопасности для обоснования своих возможностей по обеспечению защищенности критичной информации потребителя облачных услуг и предоставления ему гарантируемых поставщиком показателей. Также, оценка риска нарушения ИБ в реальном масштабе времени позволит осуществить выбор рационального варианта реагирования на возможные инциденты, возникающие в системе облачных вычислений.

3.3 Решение проблемы формирования множества данных обучающей выборки и выбора архитектуры искусственной нейронной сети

Одной из главных проблем практического использования искусственных нейронных сетей является формирование множества данных

обучающей выборки. Качество обучения ИНС напрямую зависит от количества и качества примеров в обучающей выборке, а также от того, насколько полно эти примеры описывают задачу, с которой имеет дело нейронная сеть.

По своей организации и функциональному назначению искусственная нейронная сеть с определенным количеством входов и выходов выполняет некоторое преобразование входной сенсорной информации в выходные управляющие сигналы. Число входов нейронной сети равно *n*, а число выходов *m*. Совокупность всевозможных входных векторов размерности n образует векторное пространство *X*, которое называется признаковым пространством ИНС. Аналогично, выходные вектора также формируют признаковое пространство, которое будет обозначаться *Y*. Состояние, при котором нейронная сеть выполняет требуемую функцию, называют обученным состоянием сети W. Таким образом, обучающая выборка ИНС – определенное количество примеров, которые иллюстрируют примеры соответствий между признаковыми пространствами X и Y.

Обучающая выборка является множеством пар векторов, причем в каждой паре один вектор соответствует *стимулу* или входу нейронной сети, а второй – требуемой *реакции* или выходу нейронной сети. Процесс обучения нейронной сети представляет собой в приведение всех векторов стимулов из обучающей выборки требуемым реакциям путем выбора *весовых коэффициентов* нейронов. Процесс обучения с математической точки зрения является процессом поиска некоторого минимума функции.

При составлении множества данных обучающей выборки искусственной нейронной сети важно обеспечить репрезентативность выборки [92].

Репрезентативность – соответствие характеристик выборки характеристикам популяции или совокупности данных в целом [93]. Репрезентативность входных и выходных данных заключается в достаточности количества обучающих примеров, отражающих правила и

закономерности, которые должны быть обнаружены нейронной сетью в процессе ее обучения [94]. Детализация свойства репрезентативности обучающей выборки ИНС показана на рисунке 3.5.

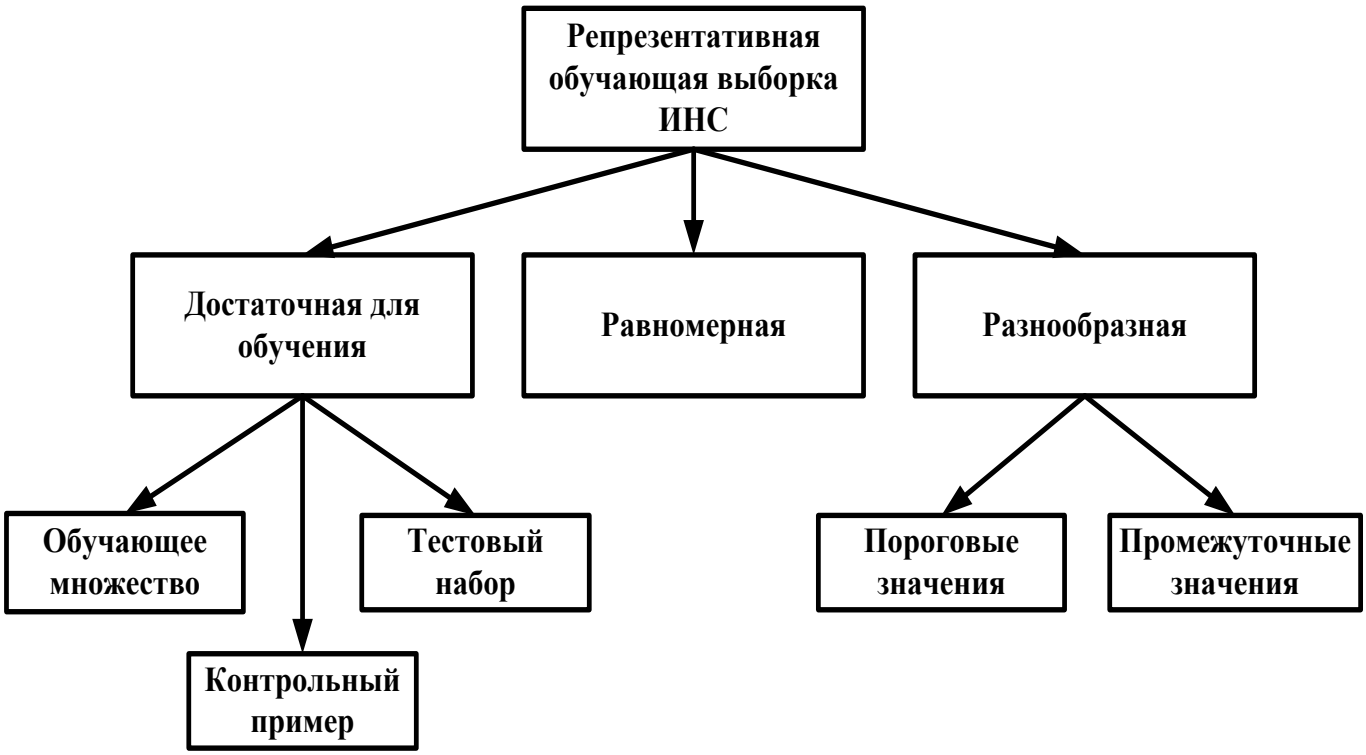


Рисунок 3.5 – Детализация свойства репрезентативности множества данных обучающей выборки искусственной нейронной сети

Репрезентативная выборка должна удовлетворять трем условиям:

− достаточность — число обучающих примеров в выборке должно быть *достаточным для обучения*. Для обучения нейронной сети очень важно, чтобы число обучающих примеров было в несколько раз больше, чем число весов межнейронных связей, в противном случае выборка считается недостаточной для обучения. Кроме того, размер выборки должен быть достаточным для формирования обучающего множества, выделения из обучающего множества тестового набора, а также отдельного формирования контрольного примера, не входящего в обучающее множество;

− равномерность обучающей выборки — примеры различных данных должны быть представлены в обучающей выборке примерно в *одинаковых*

пропорциях и с примерно *одинаковым шагом дискретизации*, что упростит обучение нейронной сети и уменьшит время обучения;

− разнообразие — в обучающей выборке должно присутствовать *большое число разнообразных комбинаций* вход-выход в обучающих примерах. Необходимая среднеквадратичная ошибка не будет достигнута за конечное время обучения, если число примеров в выборке достаточное, но она не содержит *пороговые значения*, возможные при использовании обученной нейронной сети на практике, либо не содержит *промежуточные значения с достаточным шагом дискретизации*, характерные для множества данных обучающей выборки.

В диссертационной работе на основе абстрактно-алгебраического подхода сформированы условия достаточности множества данных обучающей выборки для обучения искусственной нейронной сети.

1. Обучающая выборка должна включать в себя определенное количество примеров, иллюстрирующих соответствие между признаковыми пространствами *X* и *Y*, таких чтобы сеть достигала обученного состояния *W*:

$$W = \{X(x_1 \dots x_n) \leftrightarrow Y(y_1 \dots y_m)\} \tag{3.1}$$

2. Обучающая выборка должна быть достаточной для обучения, и представлена двойкой пространств − пространство обучающих примеров *D*, пространство тестовых наборов T, − а также включать в себя контрольный пример K, не входящий в обучающее множество:

$$W = \{D(X,Y), T(X,Y) | K(x,y)\} \tag{3.2}$$

3. Для упрощения обучения, сокращения количества итераций и времени на обучение множество данных обучающей выборки должно включать примеры различных данных, которые удовлетворяют условию (3.3).

$$w = \{w \in W | (w_1 \dots w_n) \propto (w_1 \dots w_n) | y_{qw} = const\}, \quad (3.3)$$

где: n – количество примеров в множестве данных обучающей выборки;

y_{qw} – шаг дискретизации обучающей выборки.

4. Обучающая выборка должна включать в себя пороговые значения, возможные при использовании обученной нейронной сети на практике, и промежуточные значения с достаточным шагом дискретизации. Число комбинаций «вход-выход» в обучающей выборке должно быть достаточно большим и разнообразным для обучения ИНС:

$$W = \{w_1, w_n | (w_2 \dots w_n) \approx ((w_1 + y_{qw}) \dots (w_{n-1} + y_{qw}) | N \gg 1\} \quad (3.4)$$

Для успешного обучения ИНС необходимо сформировать множество данных обучающей выборки искусственной нейронной сети исходя из этих условий. Если данные условия выполнятся для обучающей выборки ИНС, то нейронная сеть будет *хорошо натренирована*.

Таким образом, чтобы использовать искусственную нейронную сеть для проведения аудита информационной безопасности СОбВ необходимо сформировать множество данных обучающей выборки, которая удовлетворяла бы всем вышеперечисленным требованиям. Кроме того, при построении выборки обучающей нейронная сеть нужно отталкиваться от того, что ИНС работает только с *числовыми входными данными*. В диссертационной работе предлагается использовать в качестве числовых входных данных для формирования репрезентативного множества данных для обучения искусственной нейронной сети *результаты расчета прогнозируемого значения риска* нарушения информационной безопасности СОбВ.

Для расчета прогнозируемых значений уровня риска нарушения ИБ в системе облачных вычислений был использован метод, предложенный в [76,91]. В ходе оценивания прогнозируемого значения риска вычисляются

значения рисков нарушения информационной безопасности активов, обрабатываемых в сегментах инфраструктуры поставщика и потребителя облачных услуг, в зависимости от ценности обрабатываемой информации и оценки значимости угроз от множества источников к сегментам по следующей схеме:

- значения уровней угроз на путях распространения от одного источника к одному объекту атаки определяются как произведение вероятности активизации угрозы и полученных нормированием приведенных в международной базе данных величин уязвимостей компонентов инфраструктуры поставщика и потребителя облачных услуг и барьеров:

$$P_j = P_a \cdot \prod_{z \in Z} W_{nocm,z,z+1} \cdot \prod_{z \in Z} W_{nomp,z,z+1}, \qquad (3.5)$$

где $W_{nocm,z,z+1}$ – значения уязвимостей компонентов облачной инфраструктуры поставщика услуг и барьеров на пути распространения атаки;

$W_{nomp,z,z+1}$ – значения уязвимостей компонентов облачной инфраструктуры потребителя услуг и барьеров на пути распространения атаки;

P_a – вероятность активизации угрозы;

- выявляется максимальное значение уровня угрозы от источника к объекту атаки:

$$P_S^u(K_i \to K_y) = \max_{j=1}^{J} P_j, \qquad (3.6)$$

где J – число путей от одного источника к одному объекту;

- аналогичные вычисления проводятся для всех возможных источников угроз совокупности активов на стороне поставщика и на стороне потребителя облачных услуг;
- для вычисления результирующего значения уровня угрозы информационным объектам СОбВ используем формулу:

$$\mathrm{P}_{\Sigma}^{u} = 1 - \prod_{s}\left(1 - \mathrm{P}_{S}^{u}\right), \tag{3.7}$$

- расчеты проводятся для поставщика и для потребителя облачных услуг;
- значение уровня риска нарушения ИБ объектам СОбВ:

$$\overline{R}_n = \sum_{s=1}^{S} P_{\Sigma}^{u} \cdot \begin{bmatrix} Ц(C_{пост}), \\ Ц(C_{потр}). \end{bmatrix} \Big| Ц(C_{пост}) + Ц(C_{потр}) = 1 \quad ,(3.8)$$

где S – число источников угроз;

Ц ($C_{пост}$) – ценность информационных активов поставщика облачных услуг;

Ц ($C_{потр}$) – ценность информационных активов потребителя облачных услуг.

- результирующее значение риска нарушения ИБ в СОбВ определяется по формуле:

$$\overline{R} = \sum_{n=1}^{N} \overline{R}_n, \tag{3.9}$$

где N – число критичных объектов СОбВ.

Метод позволяет получить оценку значения уровня риска нарушения ИБ для *наихудшего случая*, когда одновременно активизируются все возможные источники угроз. В диссертационной работе предлагается пример расчета прогнозируемого значения риска нарушения информационной безопасности. Результаты расчетов представлены в таблице 3.1.

Таблица 3.1 − Расчет прогнозируемых значений риска нарушения ИБ

Сегм	Цен	Pu_зл	Pu_др кл	Pu_пос	Pu_пот	Рез уровень угроз	Уровень риска R
С1	0,5	0,064	0,064	0	0,136	0,244	0,122
С2	0,4	0,003	0,164	0,219	0,014	0,3572	0,143
С3	0,1	0,003	0,164	0,219	0,014	0,3572	0,036
							0,3

В таблице 3.1 значения вероятностей угроз, реализуемых: $P^{зл}$ – злоумышленником; $P^{др\_кл}$ − другим потребителем облачных услуг; $P^{пос}$ – сотрудником поставщика облачных услуг; $P^{пот}$ − внутренним сотрудником потребителя (нарушителем политики безопасности).

Результаты расчетного примера показали применимость метода расчета прогнозируемых рисков для системы облачных вычислений. При проектировании системы обеспечения ИБ или в процессе планирования полученные результаты оценивания прогнозируемого значения уровня риска нарушения ИБ позволяют определить, в какой степени может быть достигнута поставленная цель защиты.

Используя результаты *количественной* оценки прогнозируемых значений рисков нарушения информационной безопасности, рассчитанных для СОбВ, можно сформировать репрезентативный массив данных обучающей выборки для настройки ИНС. Сложность решения рассматриваемой проблемы обусловлена также необходимостью учета изменяющегося параметра «ценность» информации. В диссертационной работе для преодоления этой сложности обоснована целесообразность настройки ИНС по значениям этого параметра. В таблице 3.2 приведен фрагмент множества данных для обучения ИНС. Полное множество данных обучающей выборки приведено в приложении диссертационной работы

Значение оперативного уровня риска нарушения ИБ является функцией ценности активов, обрабатываемых в СОбВ. Следует заметить, что значение параметра «ценность» информации не может быть получено путем какого-либо объективного измерения. Ценность информации может быть задана потребителем или поставщиком облачных услуг и определяется степенью полезности или важности для них какого-либо информационного актива СОбВ. Для определения ценности информационных активов сегмента должен использоваться метод, позволяющий учесть объективные сведения об обрабатываемых информационных активах.

Поэтому при формировании множества данных обучающей выборки для ИНС в качестве входного параметра необходимо использовать кроме вероятности активизации угрозы *Ра* параметр «ценность информации». Схема формирования множества данных обучающей выборки для определения рисков ИНС представлена на рисунке 3.6.

Таблица 3.2 – Фрагмент множества данных обучающей выборки

Ра_ЗЛ	Ра_ДР_КЛ	Ра_ПОС	Ра_ПОТ	С1	С2	С3	С4	R
0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0.3	0.7	0,008
0	0	0	1	0	0.1	0.3	0.6	0,0288
0	0	0	1	0.1	0.1	0.3	0.5	0,041
0	0	0	1	0.2	0.1	0.3	0.4	0,054
0	0	0	1	0.3	0.1	0.3	0.3	0,066
0	0	0	1	0.4	0.1	0.3	0.2	0,079
0	0	0	1	0.5	0.1	0.3	0.1	0,091
0	0	0	1	0.6	0.1	0.3	0	0,1
0	0	0	1	0.7	0	0.3	0	0,095
0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0.3	0.7	0,15
0	0	1	0	0	0.1	0.3	0.6	0,13
0	0	1	0	0.1	0.1	0.3	0.5	0,11
0	0	1	0	0.2	0.1	0.3	0.4	0,088
0	0	1	0	0.3	0.1	0.3	0.3	0,066
0	0	1	0	0.4	0.1	0.3	0.2	0,044
0	0	1	0	0.5	0.1	0.3	0.1	0,22
0	0	1	0	0.7	0	0.3	0	0,15

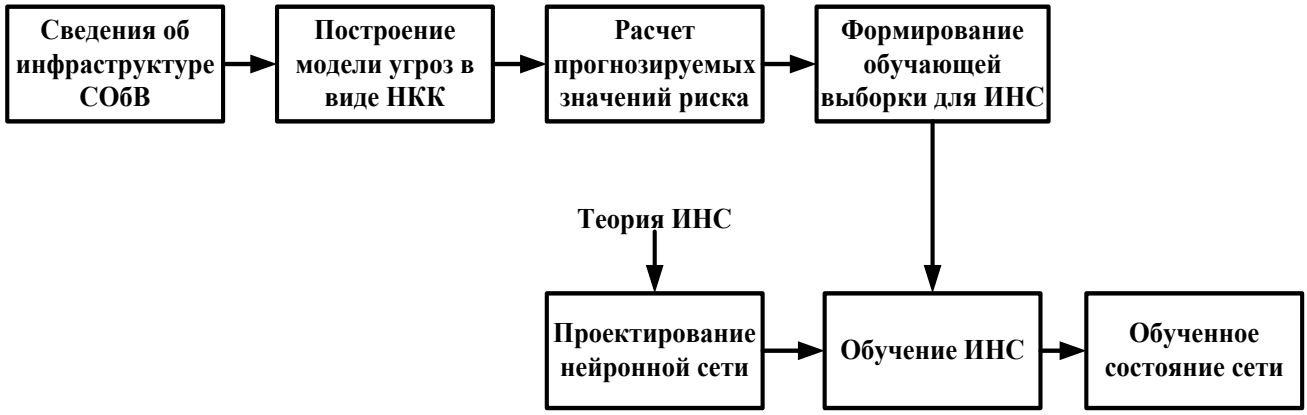


Рисунок 3.6 – Схема формирования множества данных обучающей выборки

В ходе численного эксперимента выявлено, что сформированное в диссертационной работе репрезентативное множество данных обучающей выборки вырабатывает у выходных сигналов нечувствительность к вариациям входных величин при условии, что эти вариации находятся в допустимых границах [0,1]. Также выходы ИНС не зависят от шага дискретизации, который будет использован для натренированной нейронной сети. Кроме того, аналогичные входные сигналы вызывают аналогичные реакции даже в случае, если они не входили в состав обучающего множества.

После решения проблемы формирования обучающей выборки ИНС необходимо выбрать оптимальную структуру (архитектуру) нейронной сети, адекватную поставленной задаче.

Подбор количества нейронов во входном слое обусловлен размерностью входного векторного пространства признаков *X*. Число выходов зависит от размерности выходного векторного пространства признаков Y. Оба эти пространства можно рассчитать исходя из множества данных обучающей выборки. В соответствии с этим, для нейронной сети, используемой в диссертационной работе для проведения аудита ИБ, количество входов будет равно семи, а количество выходов единице.

Так как процесс использования нейронной сети для аудита ИБ в диссертационной работе сводится к задаче поиска закономерностей в массиве данных, то были проведены исследования нескольких архитектур

нейронных сетей, которые являлись бы оптимальными для решения поставленной задачи.

Сеть Хопфилда. Нейронная сеть Хопфилда – нейронная сеть с симметричной матрицей связей [95]. В процессе работы динамика таких сетей сходится к одному из *положений равновесия*. Эти положения равновесия являются локальными минимумами функционала, называемого *энергией сети.*

Недостатком нейронной сети Хопфилда является *невозможность задать* нужное *количество эпох* обучения. Вместо этого сети Хопфилда используют понятие *«равновесие»*: следующее состояние сети в точности равно предыдущему, начальное состояние является входным образом, а при равновесии получают выходной образ [96]. Однако устойчивое состояние сети *не гарантирует* хорошую натренированность. Это обусловлено, что сеть может сойтись к *ложным аттракторам*, которые склеены из фрагментов различных данных обучающей выборки.

Кроме того, сеть Хопфилда имеет относительно *небольшой объем памяти*, что может привести к утрате способности проведения аудита ИБ с использованием механизма ИНС при добавлении аудитором дополнительных данных (примеров) в обучающую выборку. Сеть Хопфилда имеет еще одну особенность: размерности входных и выходных данных сети *обязательно должны совпадать*. Это накладывает некоторые ограничения для использования данной сети и не позволяет обучить сеть на сформированном в диссертационной работе множестве данных обучающей выборки.

Самоорганизующаяся карта Кохонена. Карта Кохонена является нейронной сетью с обучением без учителя. Помимо задач визуализации и кластеризации, применяется также в задачах моделирования, прогнозирования и поиска закономерностей в больших массивах данных [95].

Хотя карты Кохонена имеют ряд преимуществ, однако окончательный результат работы нейронных сетей сильно зависит от начальных установок

сети. При обучении карт Кохонена обучающая выборка должна состоять только из значений входных переменных, в процессе обучения *нет сравнения выходов с эталонными значениями*. Поэтому карты Кохонена чаще применяют для решения задач кластеризации. Применение же такой структуры ИНС для решения задачи проведения аудита ИБ, с учетом *заданного* множества данных обучающей выборки, затруднено.

Персептрон. Персептрон состоит из двух слоёв независимых нейронов. Первый слой состоит из рецепторов, второй из ассоциативных нейронов. Каждый нейрон первого слоя соединен со всеми нейронами последующего, но между нейронами одного и того же слоя связи отсутствуют. В современной терминологии такая сеть называется однослойной − по количеству слоёв ассоциативных нейронов [97]. Общий вид персептрона представлен на рисунке 3.7.

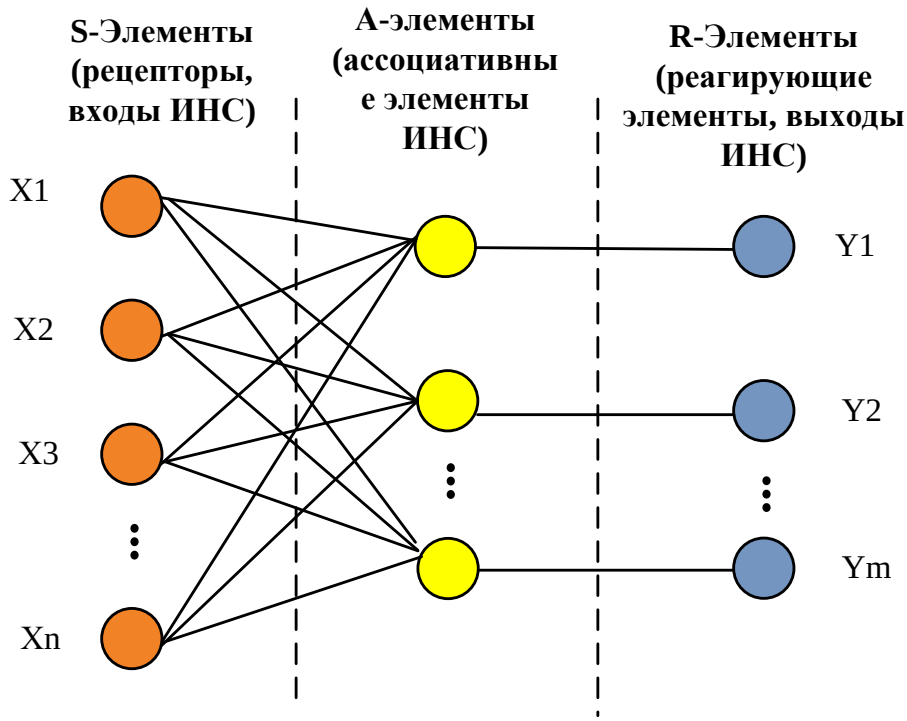


Рисунок 3.7 – Персептрон с одним скрытым слоем

Многослойный персептрон представляет собой сеть, состоящую из нескольких последовательно соединенных слоев нейронов. Входной слой состоит из сенсоров, задача которых состоит в приеме и распространении по сети входной информации. Далее располагается один скрытый слой; каждый

нейрон на скрытом слое имеет несколько входов и один выход. Алгоритмы функционирования персептрона зависят от алгоритмов обучения данной сети, однако, можно выделить несколько основных этапов, общих для всех обученных персептронов. Основные этапы функционирования персептрона представлены на рисунке 3.8.

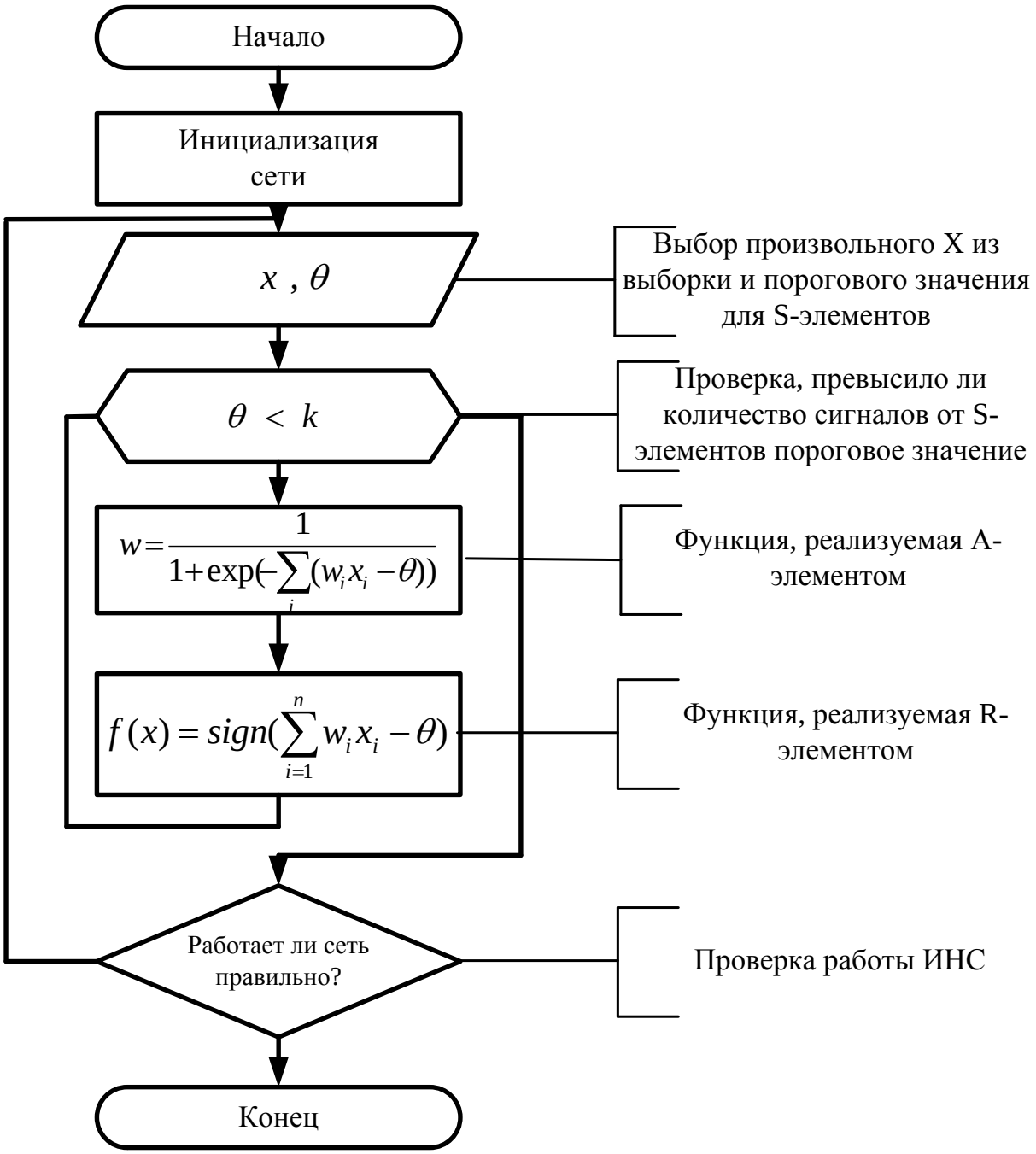


Рисунок 3.8 – Общий алгоритм функционирования персептрона

К достоинствам персептрона можно отнести достаточно простые и производительные алгоритмы обучения, а также то, что размерности входа и выхода нейронной сети ограничены при программной реализации только возможностями вычислительной системы, на которой моделируется нейронная сеть, при аппаратной реализации − технологическими возможностями [98].

Таким образом, из многообразия рассмотренных архитектур ИНС для проведения аудита ИБ на основе оценки риска был выбран персептрон с одним скрытым слоем, позволяющий решать простейшие задачи поиска закономерностей в массиве данных.

Персептрон, использующийся в диссертационной работе для аудита информационной безопасности представлен на рисунке 3.9.

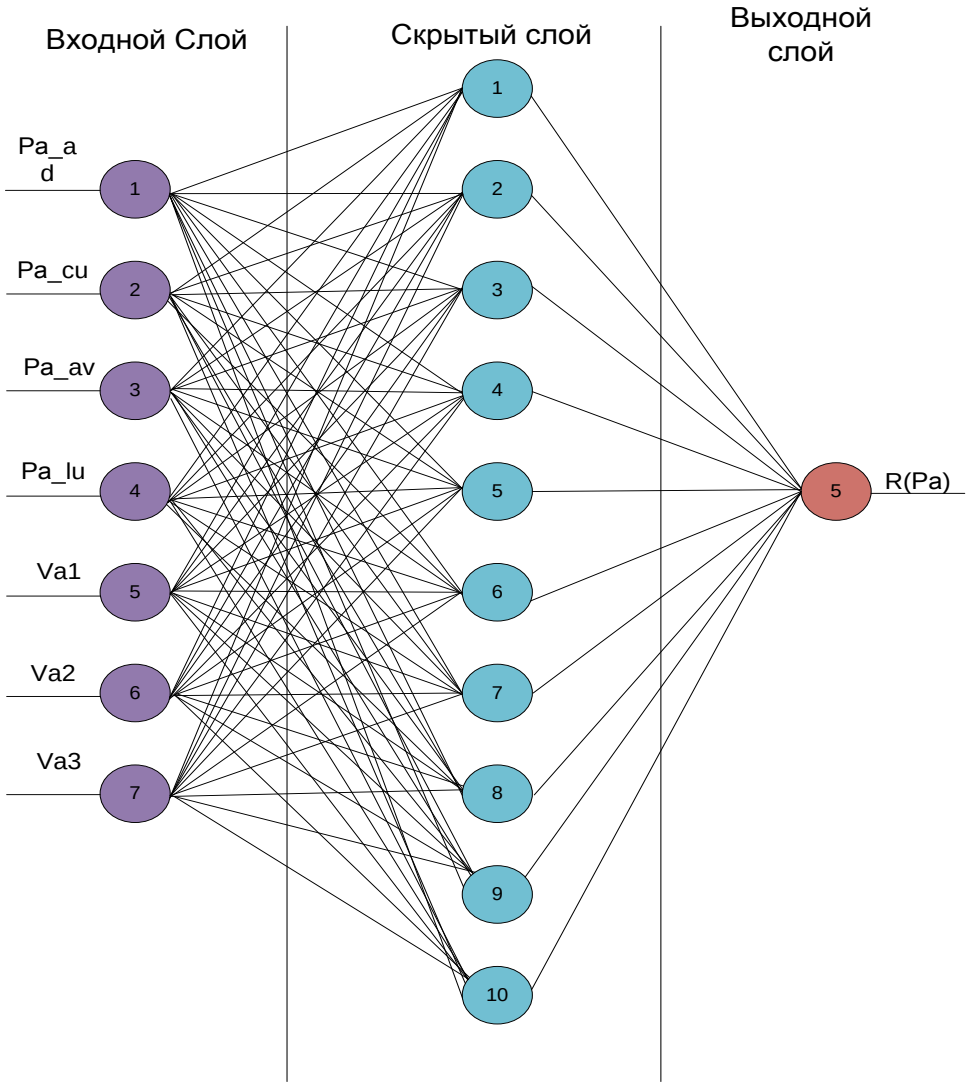


Рисунок 3.9 – Персептрон с одним скрытым слоем для аудита ИБ

При исследовании возможности использования персептрона с большим числом скрытых слоев для решения задачи, поставленной в диссертационной работе, наблюдался рост контрольной ошибки, связанный с *переобучением сети*. После проведения серии экспериментов и уменьшения количества скрытых элементов и слоев ИНС, лучший результат показала сеть с минимальным количеством скрытых слоев, что соответствует архитектуре персептрона с одним скрытым слоем.

3.4 Решение проблемы выбора эффективного алгоритма обучения искусственной нейронной сети для сформированного множества данных обучающей выборки

Для правильной работы нейронной сети важно подобрать эффективный алгоритм, по которому можно обучить нейронную сеть, обладающую определенной структурой. Любой алгоритм обучения ИНС – это совокупность математических действий, которая позволяет с помощью векторов ошибок вычислить такие поправки для весов нейронной сети, чтобы суммарная квадратичная ошибка уменьшилась до определенного уровня. Таким образом осуществляется «подстройка» коэффициентов нейронной сети, которая в конечном счете сводит среднюю квадратичную ошибку для пар «входы-выходы ИНС» до нуля или приемлемого малого уровня. Такая нейронная сеть считается обученной и готова к применению на новых, заранее неизвестных данных.

Обучение персептрона относится к способу машинного обучения, называемого «обучением с учителем» в ходе которого испытуемая система принудительно обучается с помощью примеров «стимул-реакция»[95].

Общий вид алгоритма обучения с учителем представлен на рисунке 3.10.

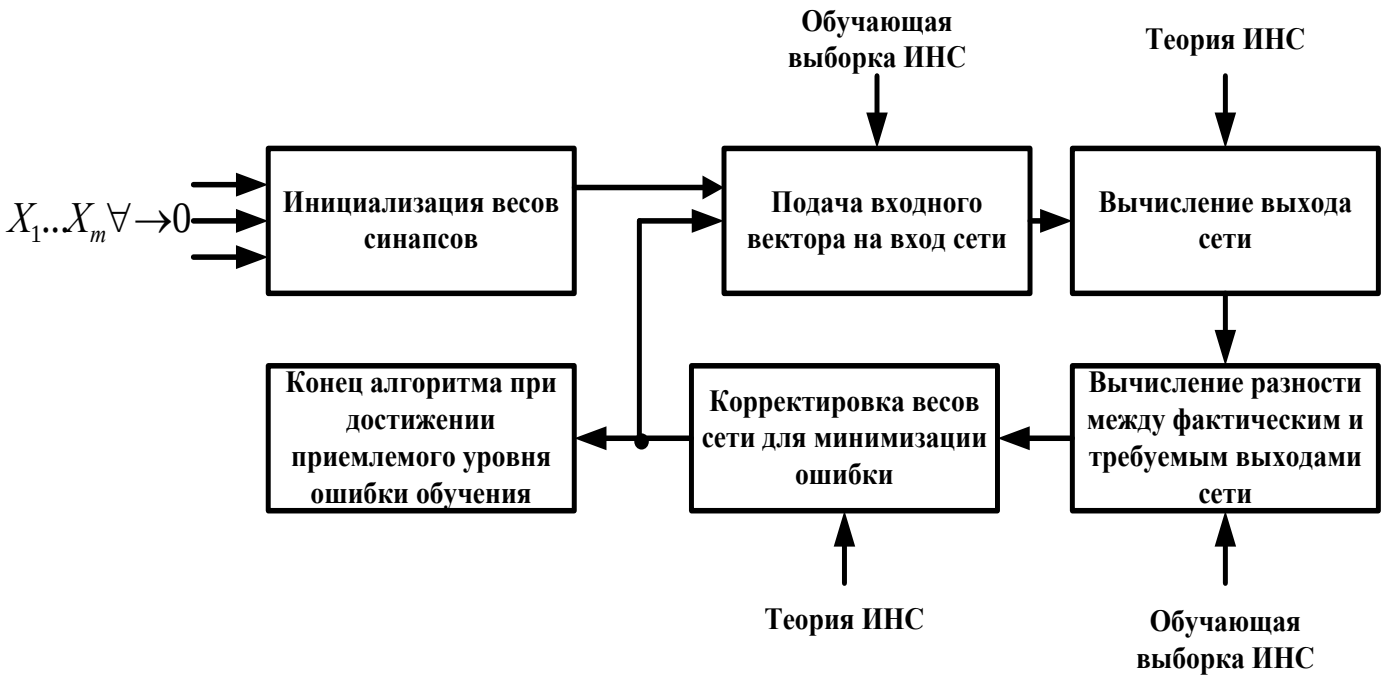


Рисунок 3.10 – Алгоритм обучения с учителем

Теория ИНС включает в себя множество разновидностей алгоритмов обучения, которые определяют каким образом нужно корректировать веса для минимизации средней квадратичной ошибки.

В диссертационной работе проводились исследования нескольких алгоритмов обучения персептрона с одним скрытым слоем, которые теоретически могли быть эффективными для данной архитектуры сети и показывали бы приемлемые результаты при обучении на заданном множестве данных обучающей выборки. Эксперименты с персептроном проводились в среде Matlab Neural Network.

Метод сопряженных градиентов. Метод построен на нахождении локального минимума функции на основе информации о ее значениях и ее градиенте. Обучение осуществляется с указанием количества эпох для обучения, при вычислении целевой функции предъявляются все примеры обучающей выборки и вычисляется средний квадрат функции ошибки [97]. При вычислении градиента используется суммарный градиент по всему обучающему набору.

В ходе исследований после проведения экспериментов в среде MatLab были выявлены следующие недостатки метода сопряженных градиентов:

● если при обучении сети, одним из примеров обучающей выборки ИНС был *локальный минимум* (вероятность активизации всех источников угроз СОбВ и ценность всех ресурсов равнялась нулю), то сеть не сможет найти *глобальный минимум*, что увеличивает возможность ложных срабатываний обученной сети при работе с ней, однако локальный минимум является обязательным условием для создания репрезентативного множества данных обучающей выборки;

● невозможность задать порог ошибки обучения в качестве сигнала выхода из цикла обучения;

● процесс обучения стремится к точке стабильности очень медленно;

● изменение подмножества выборки разрушает сопряженность направления поиска в процессе итераций, что не позволяет реагировать на динамическую масштабируемость системы облачных вычислений.

Дельта-правило. Дельта-правило является методом обучения персептрона по принципу градиентного спуска по поверхности ошибки. Основой для данного алгоритма является правила Хебба. Данный метод базируется на непрерывном изменении синаптических весов для уменьшения разности между значением желаемого и текущего выходного сигнала нейрона (средней квадратичной ошибки сети). Погрешность, полученная в выходном слое ИНС распространяется назад на предыдущие слои для коррекции синаптических весов. Процесс обратного распространения погрешностей движется вплоть до первого слоя сети.

К недостаткам данного метода обучения можно отнести:

● плохие экспериментальные показатели на данных, не заданных в обучающую выборку, что не позволяет аудитору учесть сложные сценарии атак на СОбВ;

● очень быстрое переобучение сети на сформированном в диссертационной работе множестве данных обучающей выборки, что не

позволит использовать все репрезентативное множество данных обучающей выборки, сформированное в диссертационной работе, для обучения ИНС и поведет за собой ухудшение показателей при тестировании нейронной сети на данных, не входящих в множество;

- скорость обучения или количество эпох, прохождение которых необходимо для достижения приемлемого уровня средней квадратичной ошибки обучения, намного больше, чем у других рассмотренных методов обучения.

Метод обратного распространения ошибки. Данный метод базируется на распространении сигналов ошибки от выходов сети к ее входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы сети. На каждой итерации алгоритма весовые коэффициенты нейронной сети модифицируются так, чтобы улучшить решение одного примера. Таким образом, в процессе обучения циклически решаются однокритериальные задачи оптимизации[98].

Метод обратного распространения ошибки является улучшенным вариантом Дельта-правила и экспериментально показал отличные результаты на тестовом и контрольных наборах, а также хорошую скорость работы и отсутствие переобучения сети на предложенном множестве данных обучающей выборки. Среднекваратичная ошибка при обучении с помощью данного алгоритма составила примерно 10^{-2} мсэ, что позволяет сделать вывод, что данный алгоритм является наиболее подходящим для решения задачи, поставленной в диссертационной работе.

Кроме того, используя метод обратного распространения ошибки, в качестве сигнала выхода из цикла обучения можно задать порог ошибки обучения и таким образом сократить количество итераций и, соответственно, время обучения сети.

3.5 Разработка IDEF0 модели проведения экспертного аудита информационной безопасности на основе использования искусственной нейронной сети

Экспертный аудит в системе облачных вычислений – сложный процесс, в ходе которого во внимание должно быть принято большое количество факторов и особенностей СОбВ, в том числе принятая частная политика безопасности поставщика и потребителя облачных услуг, архитектура СОбВ, набор специализированных средств защиты для облачных сред. Описание метода проведения экспертного аудита с помощью нейронной сети в виде текста достаточно громоздко, что в некоторой степени затрудняет понимание последовательности взаимосвязанных действий. Это обусловливает необходимость представления экспертного аудита ИБ в четком, наглядном виде, что, несомненно, позволит проанализировать и эффективно применить на практике предложенный метод. В данной диссертационной работе сделана попытка детализировать процесс проведения экспертного аудита информационной безопасности системы облачных вычислений, создав, таким образом, иерархическую структурную модель исследуемого процесса.

IDEF0 модель позволяет рассматривать системы (процесс) как набор взаимосвязанных действий, с последующей их детализацией. Такое представление процессов позволяет последовательно представлять детали исследуемого процесса, обеспечивая при этом, гарантированное понимание изображенного на диаграмме и полноту приведенной существенной информации, относящейся к предметной области [99]. Таким образом, целью использования IDEF0 модели является не только возможность выявления и графического представления *последовательности действий* в процессе проведения экспертного аудита ИБ в соответствии с предложенным в диссертационной работе методом, но и выработка *руководства* по обучению

экспертов−аудиторов – сотрудников отделов информационной безопасности поставщика, потребителя облачных услуг или третьей стороны, в компетенцию которых входит проведение аудита системы облачных вычислений.

Основополагающим принципом методологии функционального моделирования IDEF0 является представление функций реального объекта как преобразование входного потока информации или материальных предметов в выходной посредством воздействия преобразовывающего механизма (исполнителя) в соответствии с управляющей документацией. Эти основные аспекты отражены ролью каждой из четырех сторон функционального блока. Проектирование IDEF0-моделей выполнено с помощью программы IDEF-design 3.5. На рис. 3.11 представлена контекстная диаграмма IDEF0−модели экспертного аудита ИБ СОбВ.

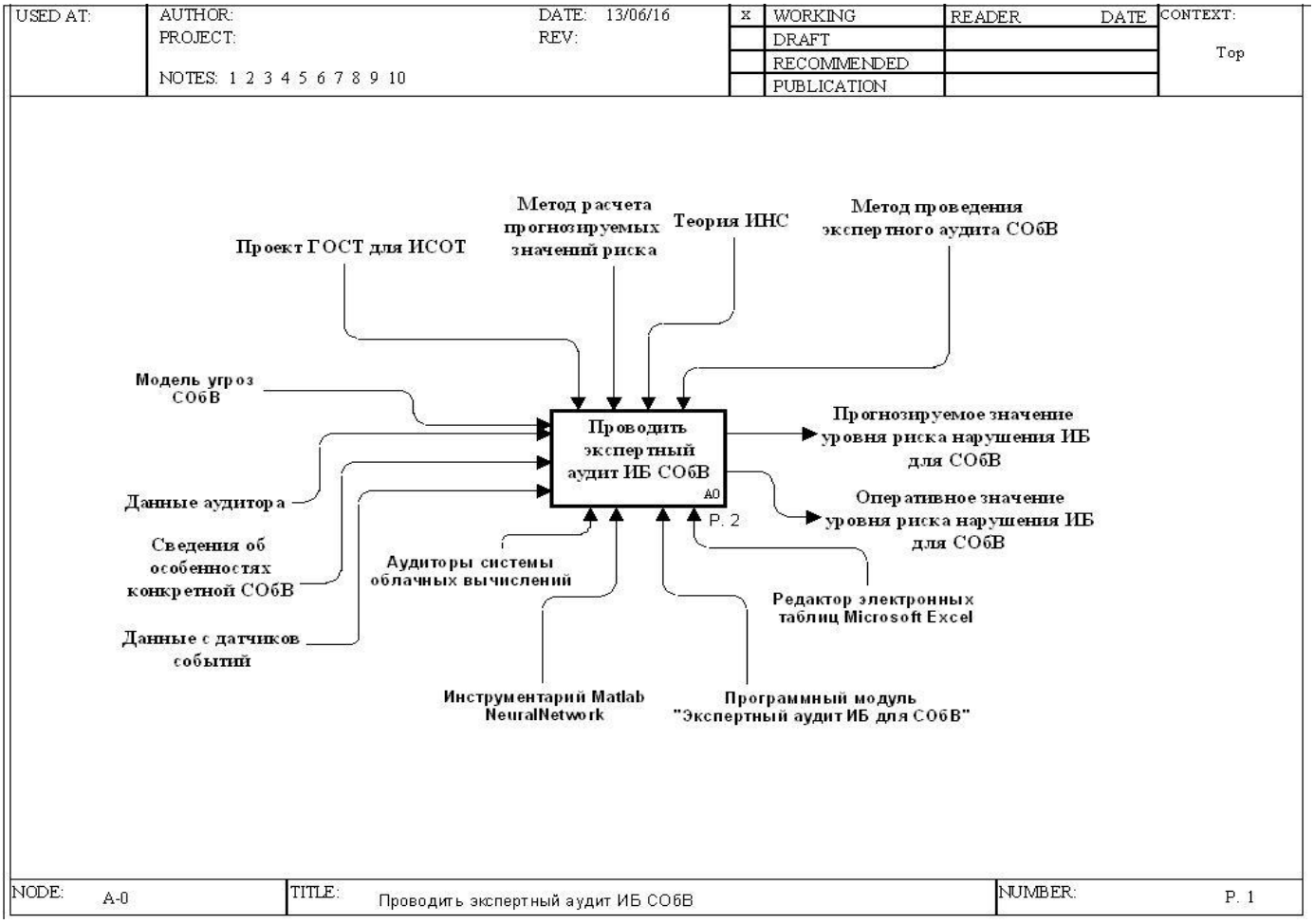


Рисунок 3.11 – Контекстная диаграмма IDEF0-модели экспертного аудита ИБ СОбВ

Данная диаграмма позволяет рассмотреть процесс проведения экспертного аудита по принципу «черный ящик». Последующая декомпозиция диаграммы позволяет представить процесс в виде иерархической структуры дочерних диаграмм с все возрастающей степенью их детализации. В соответствии с методом, предложенном в диссертационной работе, контекстный функциональный блок представлен тремя подпроцессами: «Рассчитывать прогнозируемый риск нарушения ИБ», «Настраивать и обучать нейронную сеть», «Рассчитывать оперативное значение уровня риска нарушения ИБ» (рис. 3.12).

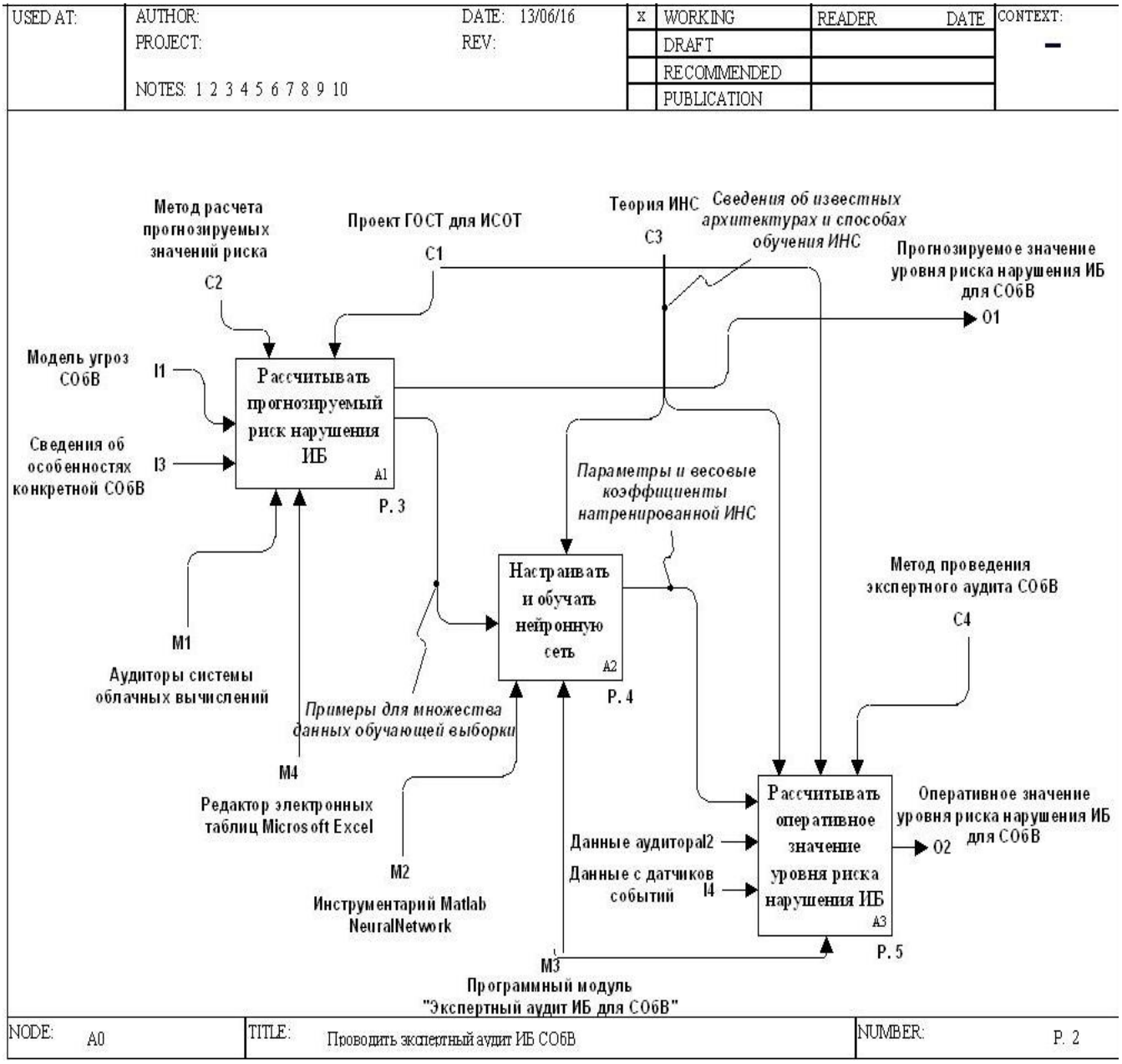


Рисунок 3.12 – Результат детализации контекстной диаграммы

Функциональный блок «Рассчитывать прогнозируемый риск нарушения ИБ» декомпозируется в соответствии с предложенным в [76] методом. На рис. 3.13 приведен результат декомпозиции функционального блока. Диаграмма, приведенная на рис. 3.14, детализирует блок «Настраивать и обучать нейронную сеть» в соответствии с методом, предложенным в диссертационной работе.

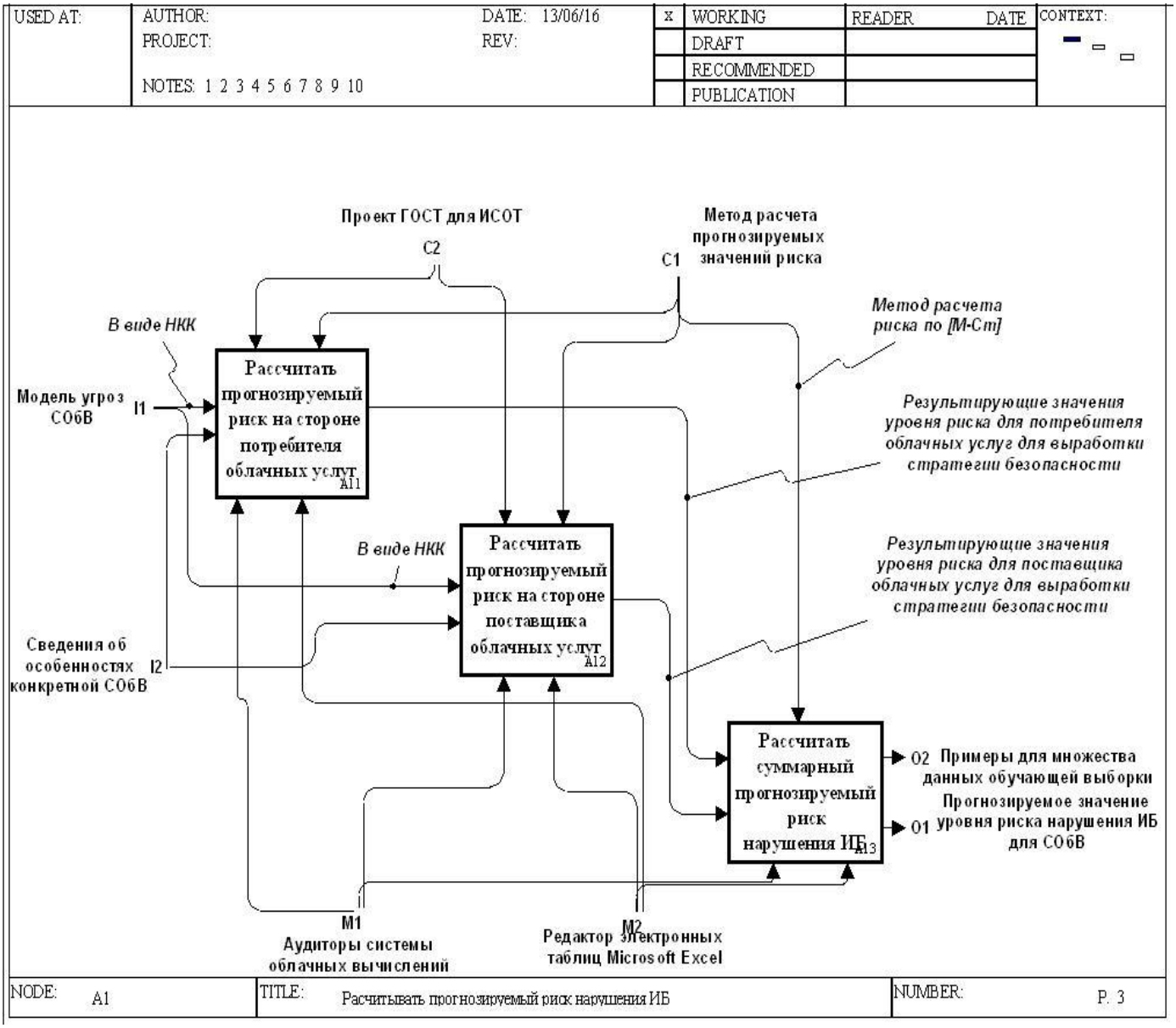


Рисунок 3.13 – Дочерняя диаграмма «Рассчитывать прогнозируемый риск нарушения ИБ»

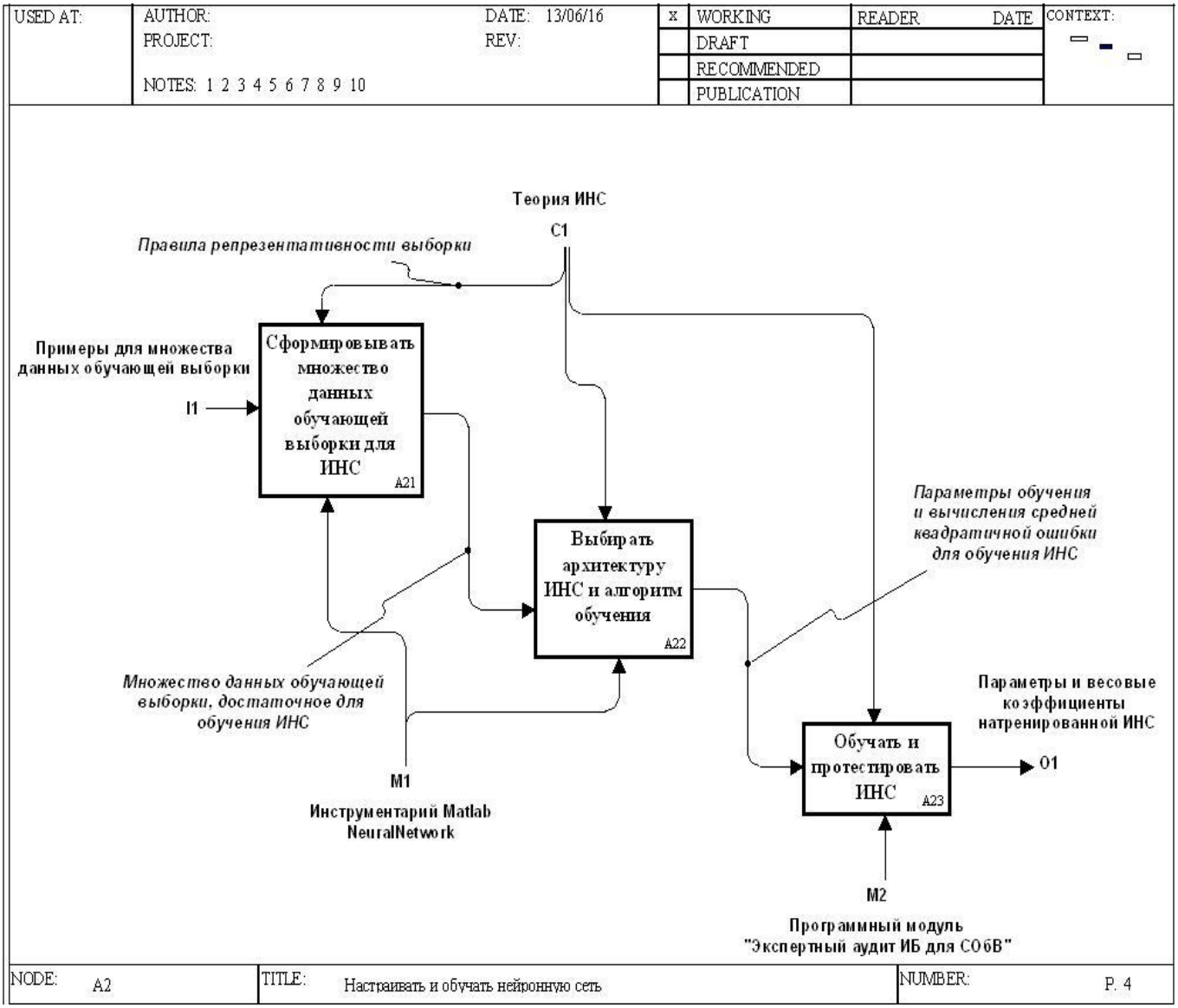


Рисунок 3.14 – Результат декомпозиции блока «Настраивать и обучать нейронную сеть»

Функциональный блок «Рассчитывать оперативное значение уровня риска нарушения ИБ» декомпозируется на два блока следующего уровня подробности (рис. 3.15). Выходами этих блоков являются значения риска нарушения ИБ для системы облачных вычислений в реальном масштабе времени.

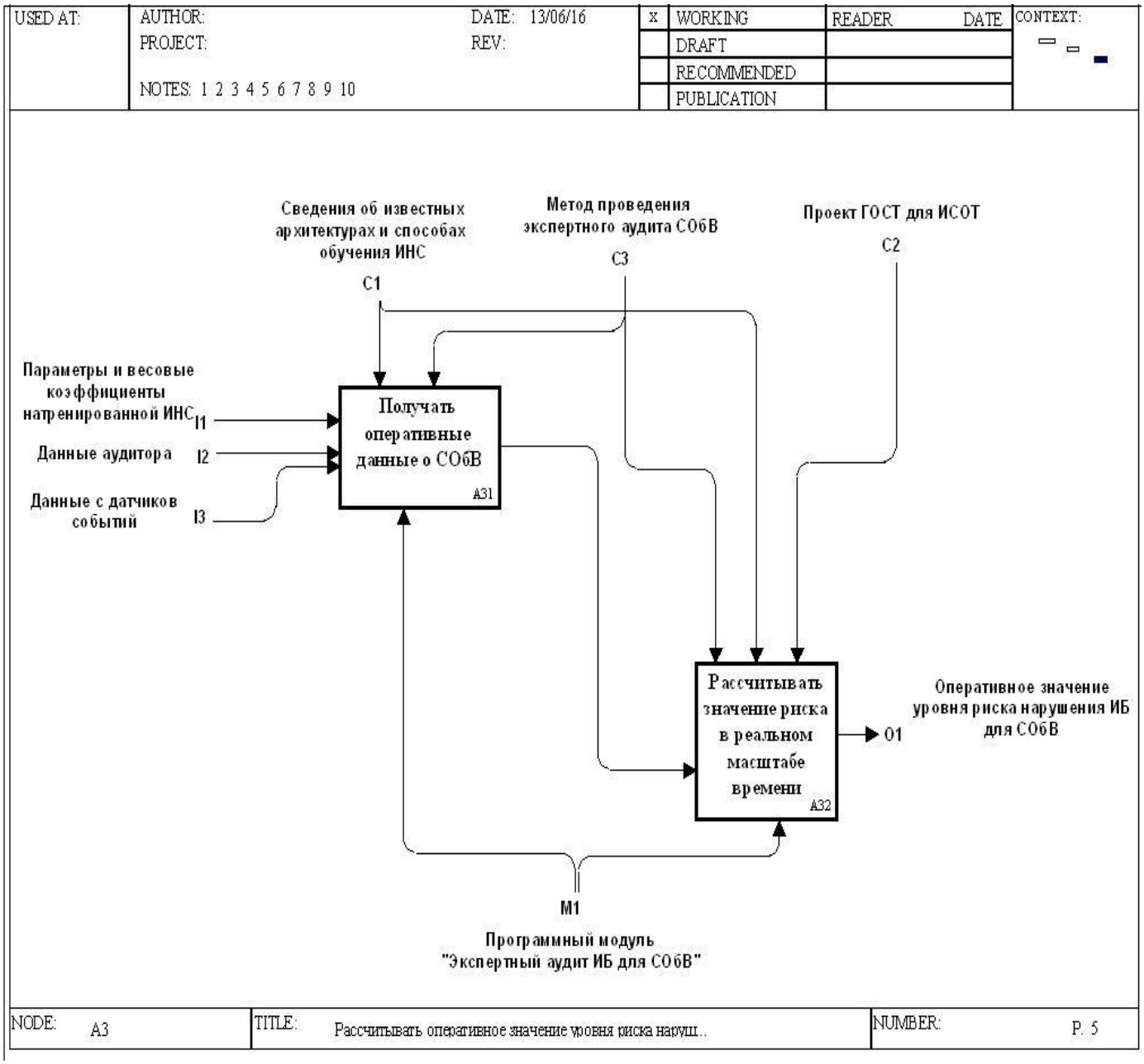


Рисунок 3.15 – Результат декомпозиции функционального блока «Рассчитывать оперативное значение уровня риска нарушения ИБ»

При анализе сложных процессов, таких как экспертный аудит ИБ информационной системы, использование моделей IDEF0 позволяет наглядно отобразить с нужной степенью детализации взаимосвязанную последовательность действий в соответствии с разработанным методом, что дает возможность эффективно его использовать на практике аудитором.

3.6 Выводы по третьей главе

1. Предложено два подхода для определения риска нарушения ИБ: расчет *прогнозируемого* значения риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз и расчет *оперативного* значения риска нарушения ИБ, когда угроза проявляется по конкретному пути распространения в реальном масштабе времени.

2. Предложен *метод* проведения *экспертного аудита* информационной безопасности, который позволяет получить численную оценку *оперативного* значения уровня риска нарушения информационной безопасности с использованием искусственной нейронной сети, при обработке ею информации с сенсоров и датчиков опасных событий, обучение которой осуществляется на множестве данных обучающей выборки, сформированной на основе расчетных значений прогнозируемого уровня риска нарушения информационной безопасности, что позволит поставщику облачных услуг *обеспечить* адекватное реагирование на возможные инциденты в реальном масштабе времени и *обосновать* свои возможности по обеспечению защищенности критичной информации потребителя.

3. Ф*ормализованы условия достаточности* множества данных обучающей выборки для обучения искусственной нейронной сети с учетом *требований репрезентативности и сформировано репрезентативное множество данных обучающей выборки н*а основе прогнозируемых значений уровня риска нарушения ИБ для обучения искусственной нейронной сети при решении задачи проведения экспертного аудита ИБ системы облачных вычислений.

4. С помощью инструментария MatLab NeuralNetwork выполнен *численный эксперимент*, в результате эксперимента выявлено, что наиболее эффективным для обучения персептрона с одним скрытым слоем и решения поставленной задачи является алгоритм обучения ИНС по методу *обратного*

распространения ошибки в силу высокой скорости работы, отсутствия переобучения сети на предложенном множестве данных обучающей выборки, а также возможности задать в качестве сигнала выхода из цикла обучения порог ошибки обучения и таким образом сократить количество итераций обучения.

5. Разработана *функциональная модель IDEF0*, наглядно отображающая процесс проведения экспертного аудита информационной безопасности системы облачных вычислений, что *позволяет* алгоритмизировать метод проведения экспертного аудита информационной безопасности для создания автоматизированного программного модуля.

ГЛАВА 4. РЕАЛИЗАЦИЯ И ВНЕДРЕНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ

В данной главе приводятся результаты проведения экспертного аудита информационной безопасности на основе получения оперативных значений уровня риска нарушения информационной безопасности в количественном выражении для системы облачных вычислений с помощью разработанного программного модуля.

Проведен численный эксперимент в целях практического исследования эффективности алгоритма обратного распространения ошибки для обучения искусственной нейронной сети в предполагаемой области применения, разработана модель автоматизированного средства, блок-схема алгоритма работы программного модуля, оценена точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле. Произведен анализ влияния величины оперативного значения уровня риска нарушения информационной безопасности от значения ценности информации и показано, что внутренние источники угроз нарушения ИБ наиболее опасны для ИС.

Результаты главы опубликованы в работах [100,101, 106, 107].

4.1 Обучение искусственной нейронной сети методом обратного распространения ошибки. Исследование эффективности выбранного алгоритма обучения ИНС

На основе исследований, проведенных в главе 3 диссертационной работы, было принято решение использовать для обучения искусственной нейронной сети метод обратного распространения ошибки.

Обучение алгоритмом обратного распространения ошибки предполагает два прохода по всем слоям сети: прямого и обратного. При прямом проходе входной вектор подается на входной слой нейронной сети, после чего распространяется по сети от слоя к слою. В результате генерируется набор выходных сигналов, это позволяет настроить сеть на данный входной образ. Во время прямого прохода все синаптические веса сети фиксированы. Во время обратного прохода все синаптические веса настраиваются в соответствии с правилом коррекции ошибок, а именно: фактический выход сети вычитается из желаемого, в результате чего формируется сигнал ошибки. Этот сигнал впоследствии распространяется по сети в направлении, обратном направлению синаптических связей. Отсюда и название – алгоритм обратного распространения ошибки. Синаптические веса настраиваются с целью максимального приближения выходного сигнала сети к желаемому.

Синапс − однонаправленная входная связь нейрона, соединенного с выходом другого нейрона, которая имеет свой вес.

Аксон − единственный отросток нейрона, по которому он передает свой выходной сигнал.

Вес − определяет, насколько соответствующий вход нейрона влияет на его состояние. Состояние нейрона можно определить по формуле 4.1 [95]:

$$S = \sum_{i=1}^{n} x_i \cdot w_i , \qquad (4.1)$$

где n – число входов нейрона;

x_i – значение i-го входа нейрона;

w_i – вес i-го синапса.

Затем определяется значение аксона нейрона по формуле 4.2:

$$Y = f(S) \qquad (4.2)$$

где f – *активационная функция* нейрона.

Наиболее часто в качестве активационной функции используется *сигмоид* искусственной нейронной сети, которая имеет следующий вид:

$$f(x) = \frac{1}{1 + e^{-ax}}, \tag{4.3}$$

Основное достоинство этой функции в том, что она дифференцируема на всей оси абсцисс и имеет очень простую производную:

$$f(x) = a \cdot f(x) \cdot (1 - f(x)), \tag{4.4}$$

Любая искусственная нейронная сеть, обучаемая по алгоритму обратного распространения ошибки, состоит из нескольких слоев нейронов, причем каждый нейрон слоя *i* связан с каждым нейроном слоя (*i+1).*

В общем случае задача обучения ИНС сводится к нахождению функциональной зависимости *Y=F(X)* где *X* – входной, а *Y* – выходной векторы. В общем случае такая задача, при ограниченном наборе входных данных, имеет бесконечное множество решений. Для ограничения пространства поиска при обучении ставится задача минимизации целевой функции ошибки НС, которая находится по методу наименьших квадратов:

$$E(w) = \frac{1}{2}\sum_{j=1}^{P}(y_j - d_j), \tag{4.5}$$

где y_j – значение j-го выхода нейронной сети;

d_j – целевое значение j-го выхода;

p – число нейронов в выходном слое.

Обучение ИНС производится с помощью градиентного спуска, т. е. на каждой итерации изменение веса производится по формуле 4.6.

$$\Delta w_{ij} = -h \cdot \frac{\delta E}{\delta w_{ij}}, \tag{4.6}$$

где h – параметр, определяющий скорость обучения.

$$\frac{\delta E}{\delta w_{ij}} = \frac{\delta E}{\delta y_j} \cdot \frac{\delta y_j}{\delta S_j} \cdot \frac{\delta S_j}{\delta w_{ij}}, \tag{4.7}$$

где y_j – значение выхода j-го нейрона;

S_j – взвешенная сумма входных сигналов.

При этом множитель находится по формуле 4.8.

$$\frac{\delta S_j}{\delta w_{ij}} = x_{ij} \tag{4.8}$$

где x_i – значение i-го входа нейрона.

Далее рассмотрим определение первого множителя формулы (13)

$$\frac{\delta E}{\delta y_j} = \sum_k \frac{\delta E}{\delta y_k} \cdot \frac{\delta y_k}{\delta S_k} \cdot \frac{\delta S_k}{\delta w_j} = \sum_k \frac{\delta E}{\delta y_k} \cdot \frac{\delta y_k}{\delta S_k} \cdot w_{jk}^{(n+1)}, \tag{4.9}$$

где k – число нейронов в слое $n+1$.

Вводим вспомогательную переменную:

$$\upsilon_j^{(n)} = \frac{\delta E}{\delta y_j} \cdot \frac{\delta y_j}{\delta S_j}. \tag{4.10}$$

По следующей формуле (4.11) определяем рекурсивную формулу для определения n-ного слоя, если нам известно следующего $(n+1)$-го слоя.

$$\upsilon_j^{(n)} = \left[\sum_k \upsilon_k^{(n+1)} \cdot w_{jk}^{(n+1)}\right] \cdot \frac{\delta y_j}{\delta S_j}. \tag{4.11}$$

Нахождение же для последнего слоя НС не представляет трудности, так как нам известен целевой вектор, т. е. вектор тех значений, которые должна выдавать ИНС при данном наборе входных значений.

$$\upsilon_j^{(n)} = (y_i^n - d_i) \cdot \frac{\delta y_j}{\delta S_j}. \quad (4.12)$$

И наконец запишем формулу в раскрытом виде:

$$\Delta w_{ij}^n = -h \cdot \upsilon_j^{(n)} \cdot x_i^n \quad (4.13)$$

Корректировка всех весов нейронной сети будет производиться по формуле 4.14:

$$\Delta w_{ij}^{(n)} = w_{ij}^{(n)}(t-1) + \Delta w_{ij}^{(n)}(t). \quad (4.14)$$

Обобщенный алгоритм для обучения нейронной сети по алгоритму обратного распространения ошибки представлен на рисунке 4.1

Рисунок 4.1 – Обобщенный алгоритм обратного распространения ошибки

В диссертационной работе был проведен численный эксперимент на сформированном массиве данных обучающей выборки в целях практического исследования эффективности выбранного алгоритма обучения искусственной нейронной сети в предполагаемой области применения. Для эксперимента использовался программный модуль Matlab. Нейронная сеть прошла 10 эпох, постепенно обучаясь и сокращая ошибку обучения. При *обучении* ошибка составила около 10^{-4} мсэ, при *тестировании* сети – от 10^{-3} до 10^{-2} мсэ. График, иллюстрирующий процесс обучения нейронной сети, представлен на рисунке 4.2.

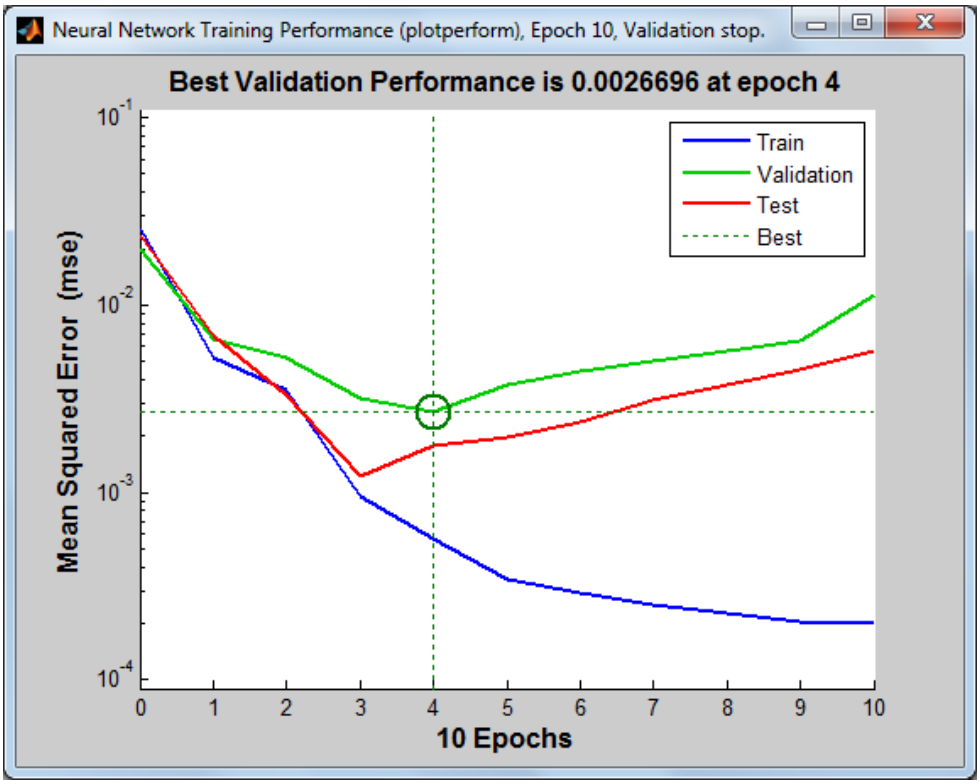


Рисунок 4.2 – График обучения ИНС в модуле nntools среды Matlab

Для проверки правильности обучения нейронной сети необходимо провести контрольный пример работы ИНС. Для этой цели в диссертационной работе предлагается применить механизм Simulink. Инструменты обучения и тестирования ИНС автоматически загружают настроенную сеть в среду Simulink. Внутренний слой с нейронами,

подстроенными по определенным коэффициентам, выглядят в виде «черного ящика» и изображается в виде прямоугольника NNET (рисунок 4.3).

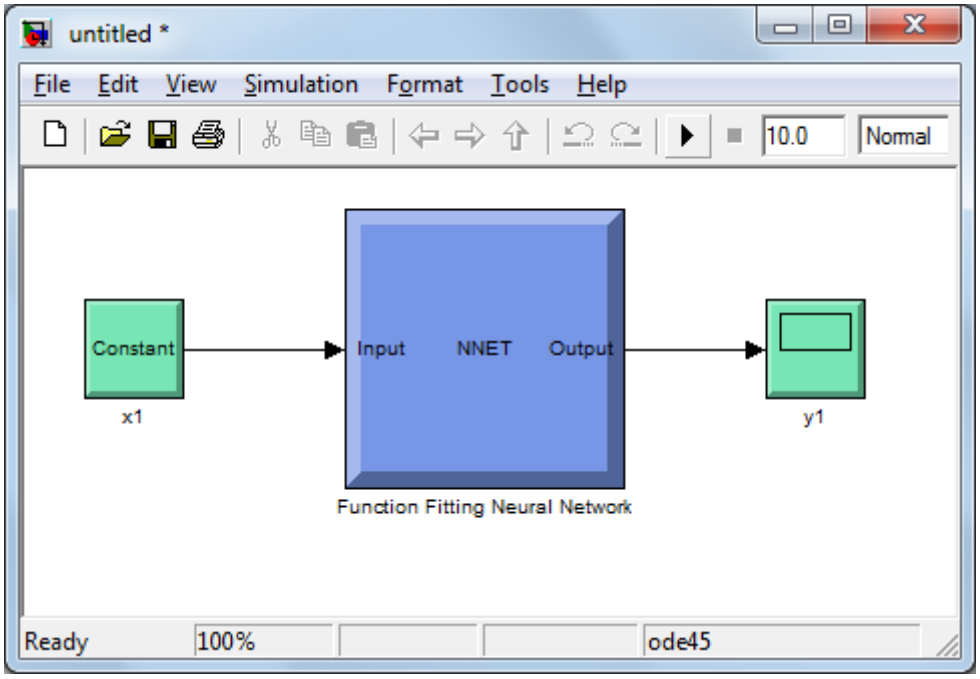


Рисунок 4.3 – Упрощенная модель нейронной сети в среде Simulink

Для проведения эксперимента необходимо задать входные переменные для проверки результатов работы ИНС (рисунок 4.4).

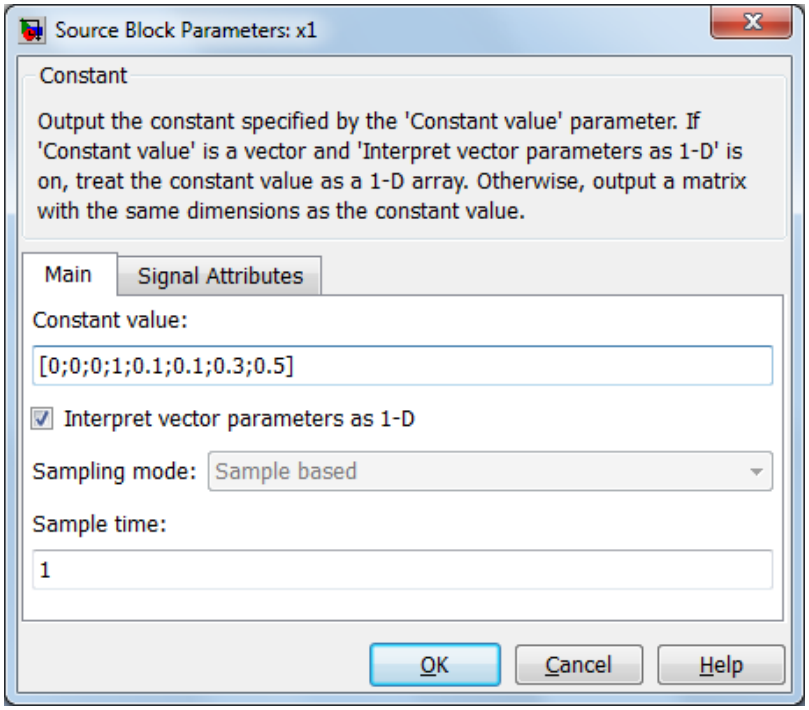


Рисунок 4.4 – Окно ввода исходных данных первого вектора для моделирования ИНС

Для проверки корректности обучения, первый вектор, на котором будет работать нейронная сеть, взят из обучающей выборки и иллюстрирует активизацию одного источника угроз из четырех. При правильной работе, нейронная сеть должна выдать точное значение выходного вектора, не сильно отличающегося по выборке. Результаты подачи входного вектора на входы персептрона отображаются в виде диаграммы Simulik (рисунок 4.5).

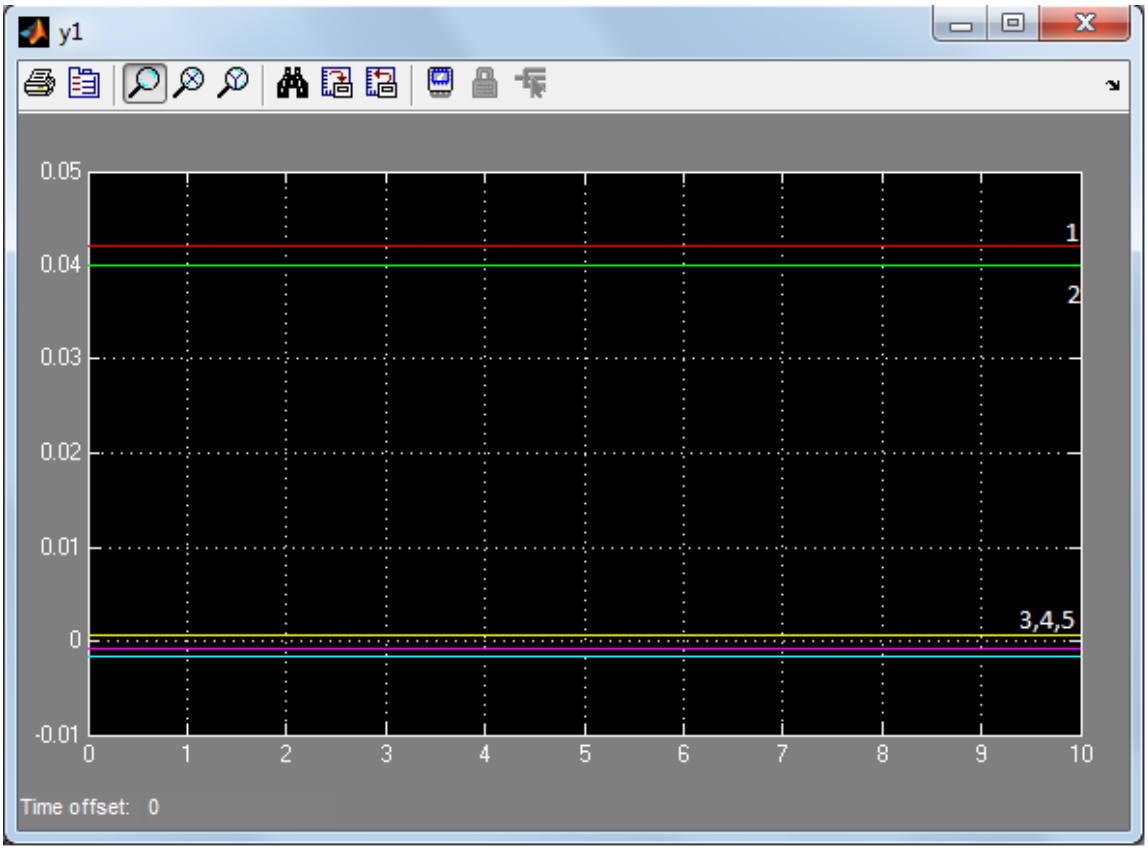


Рисунок 4.5 – Экранная форма с результатами первого контрольного примера

Таблица 4.1 − Входные данные для проверки корректности обучения (пр. 1)

Источник угрозы (вероятность активизации источника угрозы)	Объект атаки (ценность объекта атаки)
Злоумышленник (0)	Виртуальные машины и приложения потребителя (0,1)
Другой клиент поставщика облачных услуг (0)	Объекты Cloud Storage (0,1)
Сотрудник службы поставщика облачных услуг (0)	Экземпляр базы SQL (0,3)
Сотрудник потребителя облачных услуг (1)	Информационные ресурсы, обрабатываемые на стороне потребителя (0,5)

В таблице 4.1 указаны сводные значения из обучающей выборки, которые использовались для эксперимента, а в таблице 4.2 − значения выходного вектора, полученные с помощью моделирования нейронной сети. При уходе линии на диаграмме ниже нуля, графа «Отклонение» не имеет значения.

Таблица 4.2 − Выходные данные для проверки корректности обучения (пр.1)

Номер линии	Источник угроз (активный 1; неактивный 0)	Значение уровня риска в выборке	Значение уровня риска в среде Simulink	Отклонение от выборки
Первая	Суммарный (1)	0,041	0,041	0
Вторая	Сотрудник потребителя облачных услуг (1)	0,041	0,04	0,001
Третья	Злоумышленник (0)	0	0,001	0,001
Четвертая	Другой клиент поставщика облачных услуг (0)	0	- 0,001	0,001
Пятая	Сотрудник службы поставщика облачных услуг(0)	0	- 0,002	0,002

При анализе таблицы 4.2 можно сделать вывод, что нейронная сеть достаточно натренирована и показывает значение отклонения менее 0,02 от эталонного (указанного в обучающей выборке).

Для моделирования сложного сценария атак, когда активизируются более одного источника угроз, в ходе исследований проводился второй эксперимент. Входные данные, участвующие во втором эксперименте, не входят в множество данных обучающей выборки и позволяют объективно оценить степень натренированности нейронной сети и насколько хорошо она справляется с новыми данными, на которых не проводилось обучение.

В таблице 4.3 указаны сводные значения, которые использовались для проведения второго эксперимента.

Таблица 4.3 − Входные данные для проверки корректности обучения (пр. 2, активизированы три источника угроз)

Источник угрозы (вероятность активизации источника угрозы)	Объект атаки (ценность объекта атаки)
Злоумышленник (1)	Виртуальные машины и приложения потребителя (0,1)
Другой клиент поставщика облачных услуг (0)	Объекты Cloud Storage (0,1)
Сотрудник службы поставщика облачных услуг (1)	Экземпляр базы SQL (0,3)
Сотрудник потребителя облачных услуг (1)	Информационные ресурсы, обрабатываемые на стороне потребителя (0,5)

В результате задания второго входного вектора на входы персептрона формируется диаграмма Simulik, изображенная на рисунке 4.6. В таблице 4.4 представлены значения выходного вектора, полученные с помощью моделирования нейронной сети.

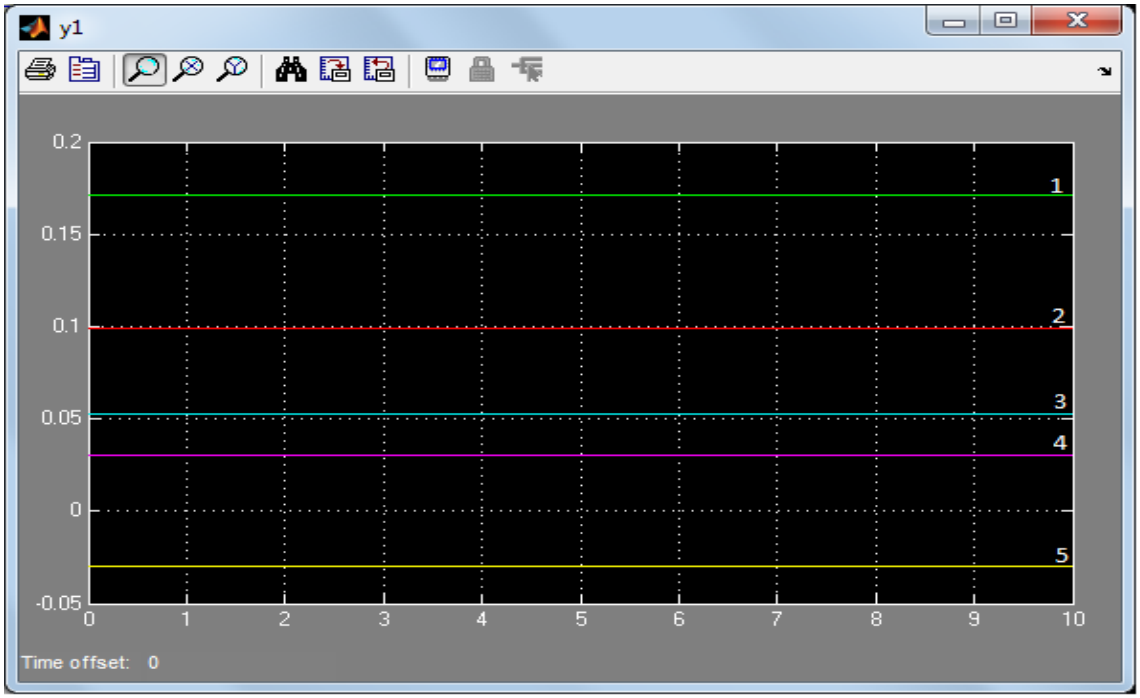


Рисунок 4.6 – Экранная форма с результатами второго контрольного примера

Таблица 4.4 −Выходные данные для проверки корректности обучения (пр. 2, активизированы три источника угроз)

Номер линии	Источник угроз (активный 0; неактивный 1)	Значение по расчету	Значение в среде Simulink	Отклонение
Первая	Суммарный (1)	0,164	0,17	0,006
Вторая	Злоумышленник (1)	0,016	0,02	0,004
Третья	Сотрудник службы поставщика облачных услуг(1)	0,1097	0,1	0,0097
Четвертая	Сотрудник потребителя облачных услуг (1)	0,042	0,05	0,008
Пятая	Другой клиент поставщика облачных услуг (0)	0	-0,025	0,025

При анализе таблицы 4.4 можно сделать вывод, что нейронная сеть достаточно натренирована и показывает значение отклонения менее 0,03 от эталонного (рассчитанного вручную по формулам).

Результаты обучения и тестирования нейронной сети показали возможность использования выбранной архитектуры и алгоритма обучения ИНС для разработки модуля численной оценки риска нарушения ИБ в программном модуле, предназначенном для автоматизации аудита ИБ СОбВ.

4.2 Разработка модели автоматизированного средства и блок-схемы алгоритма работы программного модуля, реализующего метод экспертного аудита информационной безопасности

Автоматизированное средство для аудита информационной безопасности позволит аудитору ускорить процесс принятия решений по выбору варианта реагирования на опасные инциденты. С другой стороны очевидно, что администратор безопасности быстрее и более рационально обработает опасное событие, если процедура обработки и соответствующие

технологии определены заранее, а методы реагирования зависят от того оперативного значения уровня риска нарушения ИБ, который связан с данным инцидентом.

В соответствии с предложенной в [70] методологией экспертного аудита в диссертационной работе разработан программный модуль [100], реализующий данный алгоритм [101,107]. Модель автоматизированной системы для проведения экспертного аудита представлена на рисунке 4.7.

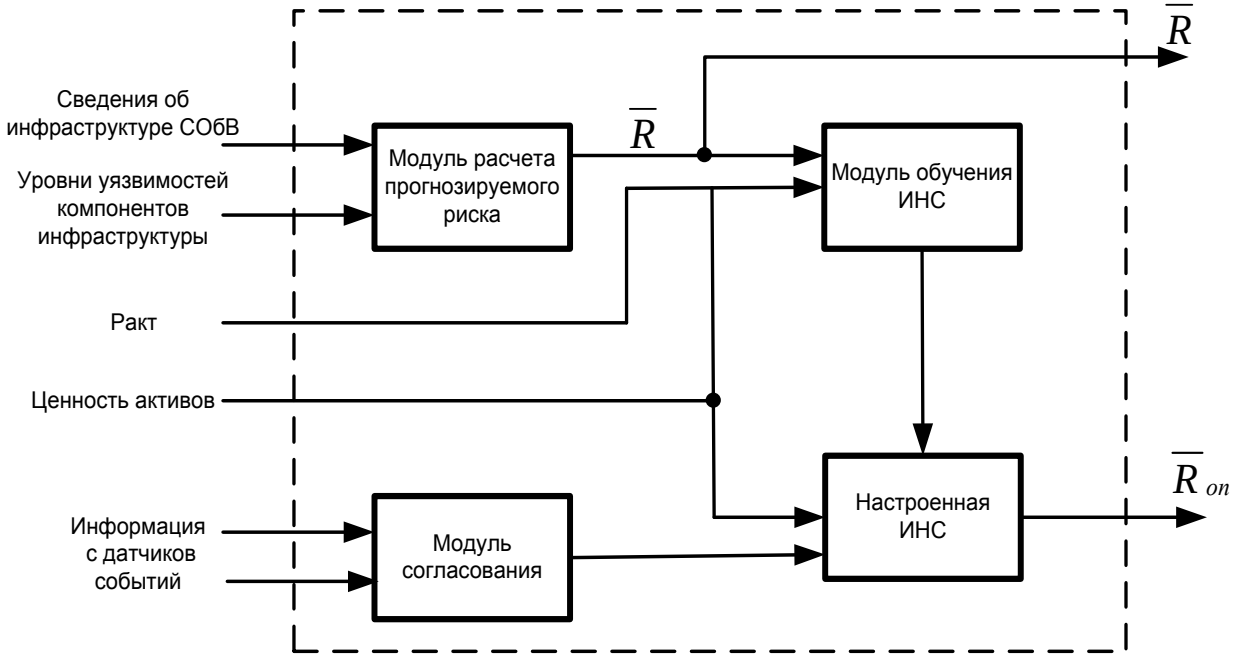


Рисунок 4.7 – Модель автоматизированной системы экспертного аудита

Модулем расчета прогнозируемого риска является XML-таблица, которая экспортирует выходные данные в txt-формат, где они преобразуются в формат класса EDIT и где формируется множество данных обучающей выборки. Формат данного класса гарантирует, что максимальный размер загружаемого в программный модуль файла с множеством данных для обучения искусственной нейронной сети не будет превышать 64 килобайт, и позволяет уменьшить время обучения нейронной сети за счет малого объема загружаемых данных, который не сказывается на количестве примеров для

обучения и не влияет на тренированность самой сети. Для расчета прогнозируемого риска аудитору необходимо ввести в модуль известные ему сведения об инфраструктуре системы облачных вычислений, а также численные значения уровней уязвимостей компонентов инфраструктуры системы. Эти значения могут быть получены в ходе поиска и нормирования соответствующих компонентов инфраструктуры в международной базе данных уязвимостей [79].

В модуле обучения искусственной нейронной сети реализован описанный выше алгоритм обратного распространения ошибки. Обучающая выборка загружается из модуля расчета прогнозируемого риска построчно, и на основе загруженных данных проводится обучение ИНС. Обучение ИНС завершается по достижению необходимого уровня среднеквадратичной ошибки обучения искусственной нейронной сети.

После успешного обучения нейронной сети и достижения необходимого уровня среднеквадратичной ошибки, специалист может приступать к проведению аудита информационной безопасности системы. Для подсчета оперативного значения уровня риска нарушения информационной безопасности аудитору необходимо подать информацию с датчиков событий системы, актуальную на данный момент времени в исследуемой системе. На основе этих данных обученная нейронная сеть рассчитает значение риска нарушения информационной безопасности для системы в реальном масштабе времени.

Затем, на основе полученных данных, аудитор может сформировать отчет в формате doc, указав используемый метод для оценки рисков и итоговое значение риска в реальном масштабе времени. В зависимости от результатов анализа аудитор указывает в отчете рекомендации по повышению уровня защищенности рассматриваемого объекта. Таким образом, помимо проведения аудита информационной безопасности системы в реальном масштабе времени, разработанный в диссертационной работе программный модуль позволит, используя рекомендации аудитора,

обоснованно планировать деятельность по обеспечению безопасности своей информационной системы и эффективно использовать ее для развития бизнеса.

Этапы расчетов в разработанном программном модуле показаны на рисунке 4.8.

Рисунок 4.8 – Этапы расчетов в разработанном программном модуле

Блок-схема алгоритма, реализующего метод оценивания оперативного значения уровня риска нарушения ИБ с помощью программного модуля «Средство аудита информационной безопасности системы облачных вычислений» представлена на рисунке 4.9.

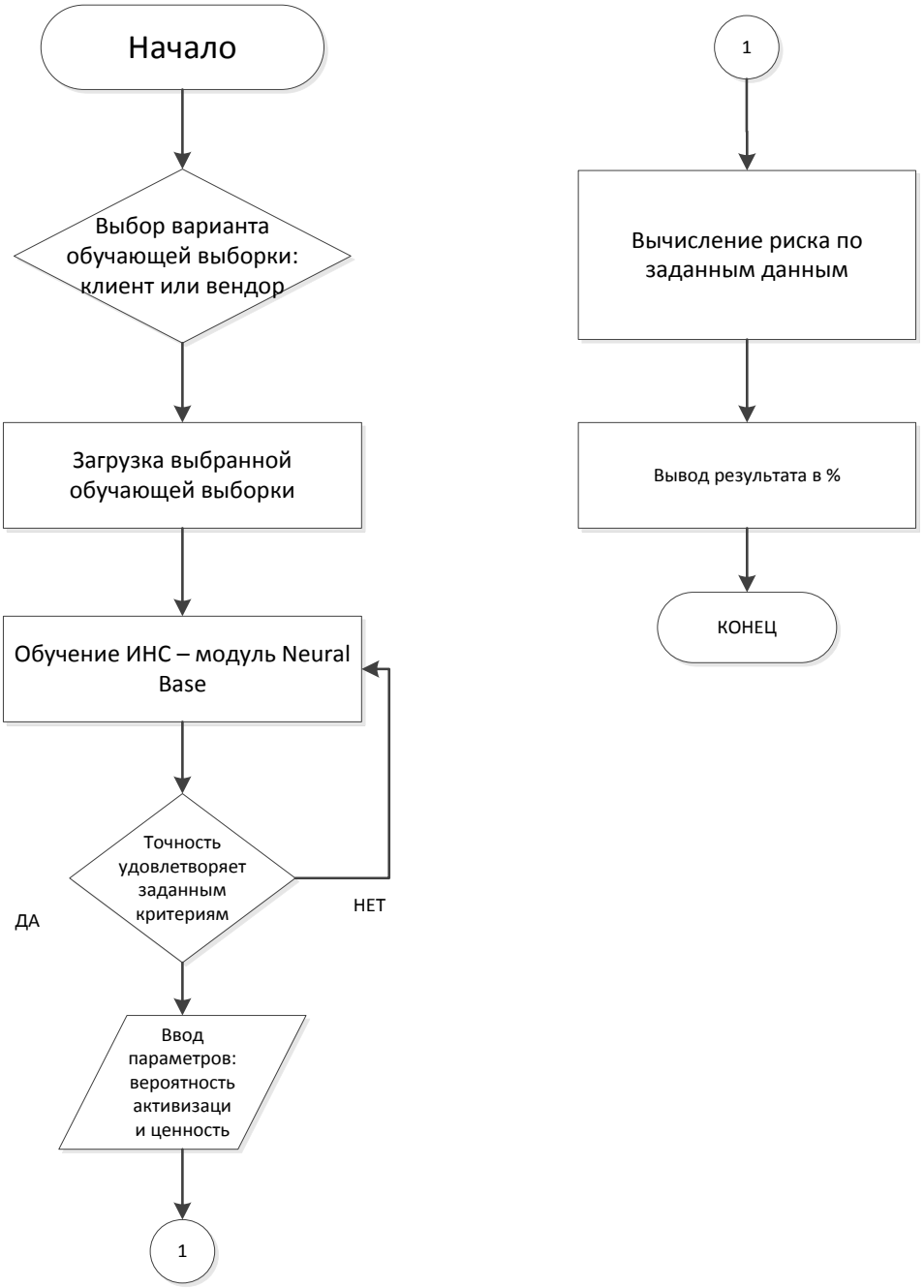


Рисунок 4.9 − Блок-схема алгоритма работы программного модуля «Средство аудита ИБ в СОбВ»

Полный алгоритм работы модуля «Обучение ИНС – модуль Neural Base», работающего по методу обратного распространения ошибки, реализованный в диссертационной работе в виде программного модуля, представлен в виде блок-схемы на рисунке 4.10.

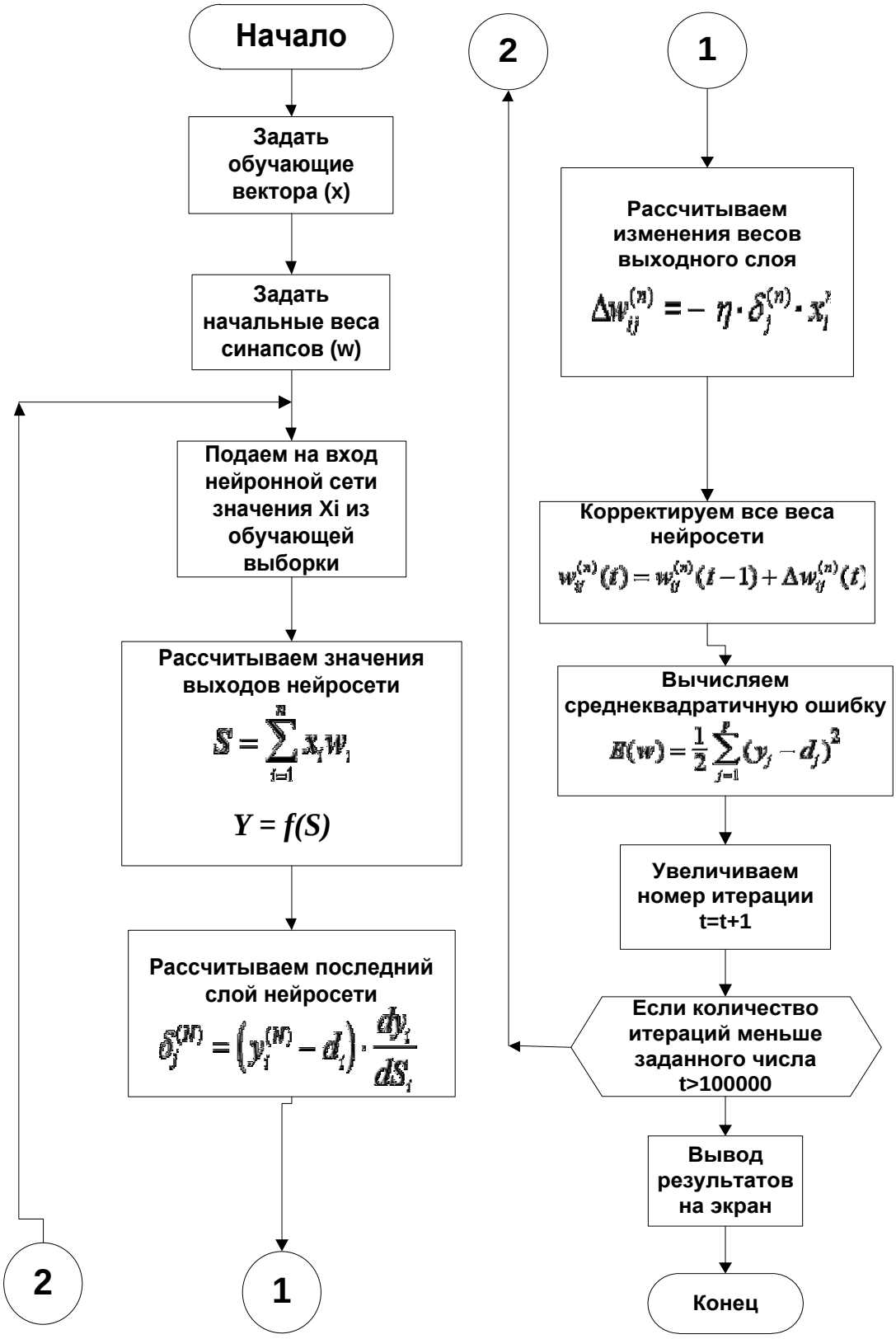


Рисунок 4.10 – Блок-схема алгоритма работы программного модуля «Обучение ИНС – модуль Neural Base»

Программный модуль реализован на языке высокого уровня Pascal ABC с использованием среды программирования Borland Delphi 7.0 и стандартной библиотеки компонентов NeuralBase.

Библиотека NeuralBase позволяет использовать искусственные нейронные сети в информационных системах с целью расширения аналитических возможностей программных модулей, реализующих данные системы. Объектно-ориентированное исполнение данной библиотеки позволяет спроектировать очень гибкую нейронную сеть, которая позволяет подстроить и обучить ИНС под конкретную задачу. Модули, включенные в библиотеку NeuralBase, представлены на рисунке 4.11 с помощью диаграммы компонентов UML.

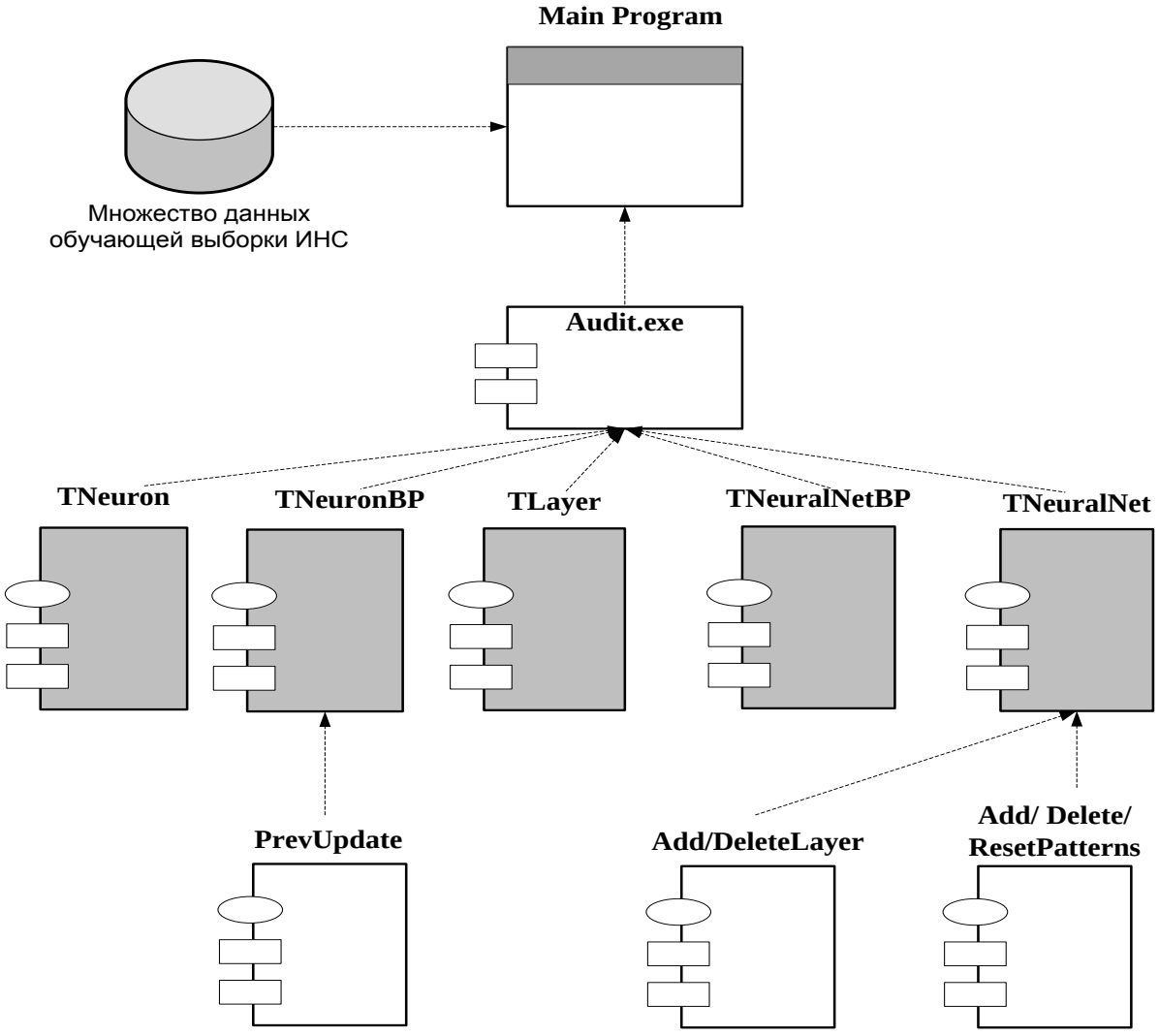


Рисунок 4.11 – UML-диаграмма программного модуля «Средство аудита ИБ в СОбВ»

Спецификация модулей библиотеки NeuralBase, подстроенной для программы «Средство аудита ИБ в СОбВ» предложена в таблице 4.5.

Таблица 4.5 – Спецификация модулей

Название	Назначение модуля
Audit	Модуль, служащий для реализации главного окна программы, − создания анимации процесса обучения нейронной сети
TNeuron	Реализуют работу с весовыми коэффициентами нейронной сети. В данном модуле проводится работа с синапсами, сумматором ИНС и выходами сети
TNeuronBP	Служит для программной реализации многослойных нейронных сетей.
PrevUpdate	Модуль для хранения величины коррекции весовых коэффициентов на предыдущем шаге обучения сети
TLayer	Модуль, позволяющий объединить все нейроны сети в слои
TNeuralNetBP	Модуль, реализующий нейронную сеть, обучаемую по алгоритму обратного распространения ошибки
TNeuralNet	Модуль, осуществляющий построение самой нейронной сети. Модуль включает в себя методы для работы со слоями сети и методы для манипуляций с исходными данными
Add/ DeleteLayer	Модуль, осуществляющий манипуляции со слоями нейронной сети
Add/ Delete/ ResetPatterns	Модуль, осуществляющий манипуляции с исходными данными обучающей выборки ИНС

Программный модуль имеет интуитивно понятный интерфейс. Визуальное отображение хода обучения нейронной сети позволяет определить время, оставшееся до успешного завершения обучения, а отображение среднеквадратичной ошибки позволяет сделать вывод о том,

насколько точно обученная нейронная сеть будет оценивать риск нарушения информационной безопасности в реальном масштабе времени.

Программный модуль выполняет процедуры контроля корректности вводимых пользователем данных и вывода соответствующих предупреждений об ошибках, в случаях если:

- суммарное значение параметра «ценность» для информационных активов, хранящихся на стороне потребителя и на стороне поставщика системы облачных вычислений не равно единице;
- задана равной нулю ценность активов на стороне потребителя системы облачных вычислений.

Преимуществом разработанного программного модуля является то, что в нем используется модель, позволяющая осуществить анализ реально выявленных угроз и выполнить оценку уровня риска нарушения информационной безопасности в реальном масштабе времени с учетом сложных сценариев атак, когда активизируются более одного источника угроз.

4.3 Описание работы с программным модулем «Средство аудита ИБ в СОбВ»

В ходе работы с программным модулем пользователь может выбрать, какую выборку требуется загрузить для обучения нейронной сети. В реализуемом в диссертационной работе примере при загрузке модуля, пользователю предлагается выбрать одну из двух сформированных выборок: либо потребителя, либо поставщика облачных услуг. В данном случае, выбор аудитора зависит от того, какая доля защищаемых информационных активов обрабатывается в исследуемый период времени в информационных системах потребителя и поставщика соответственно. До того, как пользователь

выберет обучающую выборку, кнопка «Провести обучение нейронной сети» будет неактивна.

В соответствии с тем, какая из обучающих выборок была выбрана, в модуль ввода исходных данных загружается одна из выборок для обучения искусственной нейронной сети, сформированных заранее на основе прогнозируемых значений риска нарушения ИБ в системе облачных вычислений и переведенных в формат EDIT (рисунок 4.12).

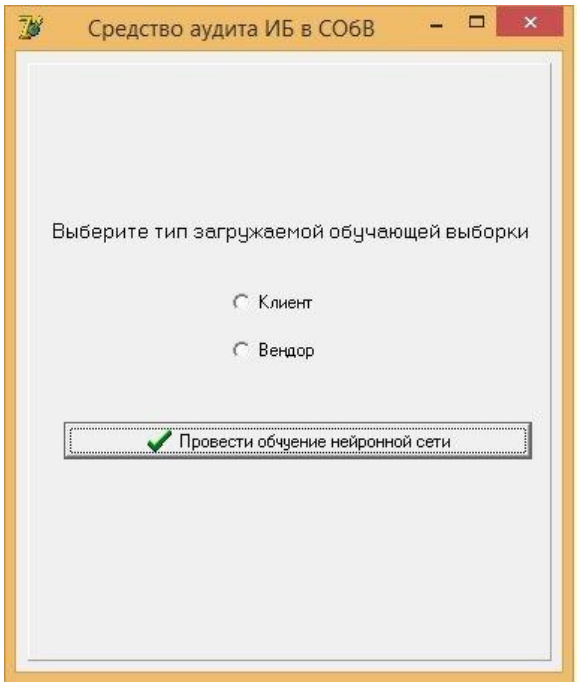


Рисунок 4.12 – Экранная форма для выбора типа загружаемой выборки

В диссертационной работе, как уже отмечалось выше, обучение искусственной нейронной сети, проводится с помощью алгоритма обратного распространения ошибки (back propagation). Этот алгоритм определяет возможность подбора весов нейронной сети с применением градиентных методов оптимизации. В процессе обучения рассчитывается целевая функция в виде квадратичной суммы разностей между фактическим и ожидаемым значениями выходных сигналов.

Следующим этапом после загрузки в модуль ввода множества данных обучающей выборки является обучение сети с помощью алгоритма обратного распространения ошибки.

После обучения нейронной сети выдается сообщение об успешном завершении обучения, выводится значение среднеквадратичной ошибки обучения нейронной сети в метрической системе mse и появляется кнопка «Приступить к работе», при нажатии которой подготовительный этап работы с ИНС завершается и аудитор может приступить к проведения аудита системы облачных вычислений (рисунок 4.13).

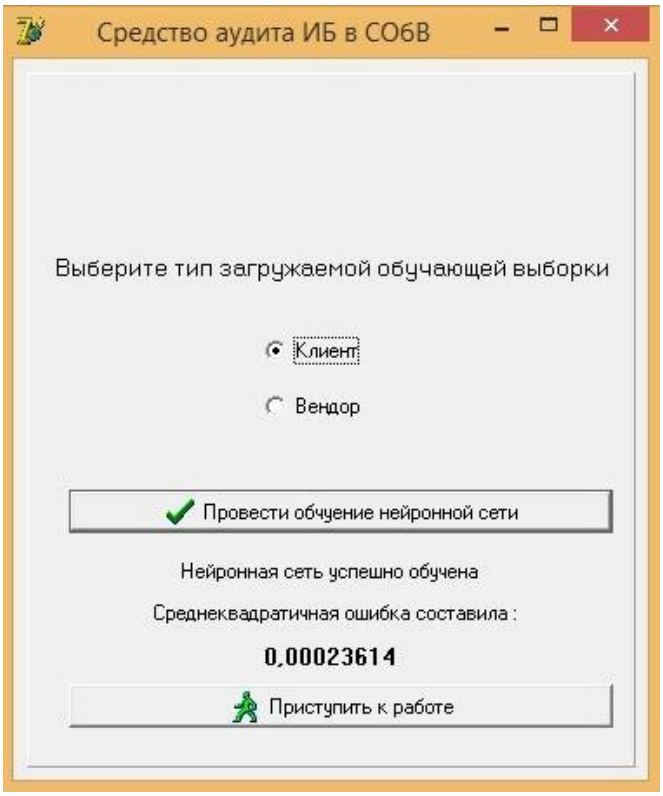


Рисунок 4.13 – Экранная форма для задания процедуры обучения ИНС с выведенным значением среднеквадратичной ошибки

Пользователю предлагается ввести числовое значение параметра «ценность» информационных активов и вероятность активизации угрозы (рисунок 4.14).

Значение параметра «ценность» защищаемого информационного актива не может быть получено путем какого-либо объективного измерения. Ценность информации может быть задана собственником и определяется

степенью полезности или важности для него какого-либо актива. Возможные виды последствий и их значимость определяются собственником или владельцем информации, который может опираться в своих суждениях на рекомендации, приведенные в [69].

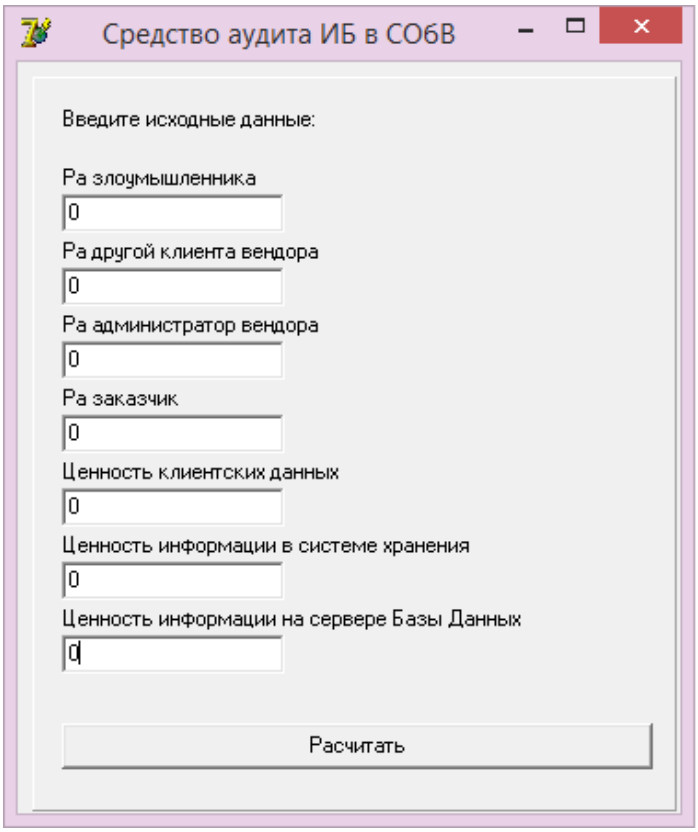


Рисунок 4.14 – Экранная форма ввода данных для аудита СОбВ

Программный модуль содержит процедуру контроля корректности вводимых данных об относительной ценности информации и о возможных значениях вероятности активизации угроз, и после того, как все значения ценностей были введены, необходимо произвести расчет (нажать кнопку «Рассчитать»), с тем, чтобы удостовериться, что относительная ценность информации, обрабатываемой во всех сегментах сети, и вероятность активизации угроз не выходят за пределы допустимых значений.

Процедура контроля корректности вводимых данных представлена на рисунке 4.15.

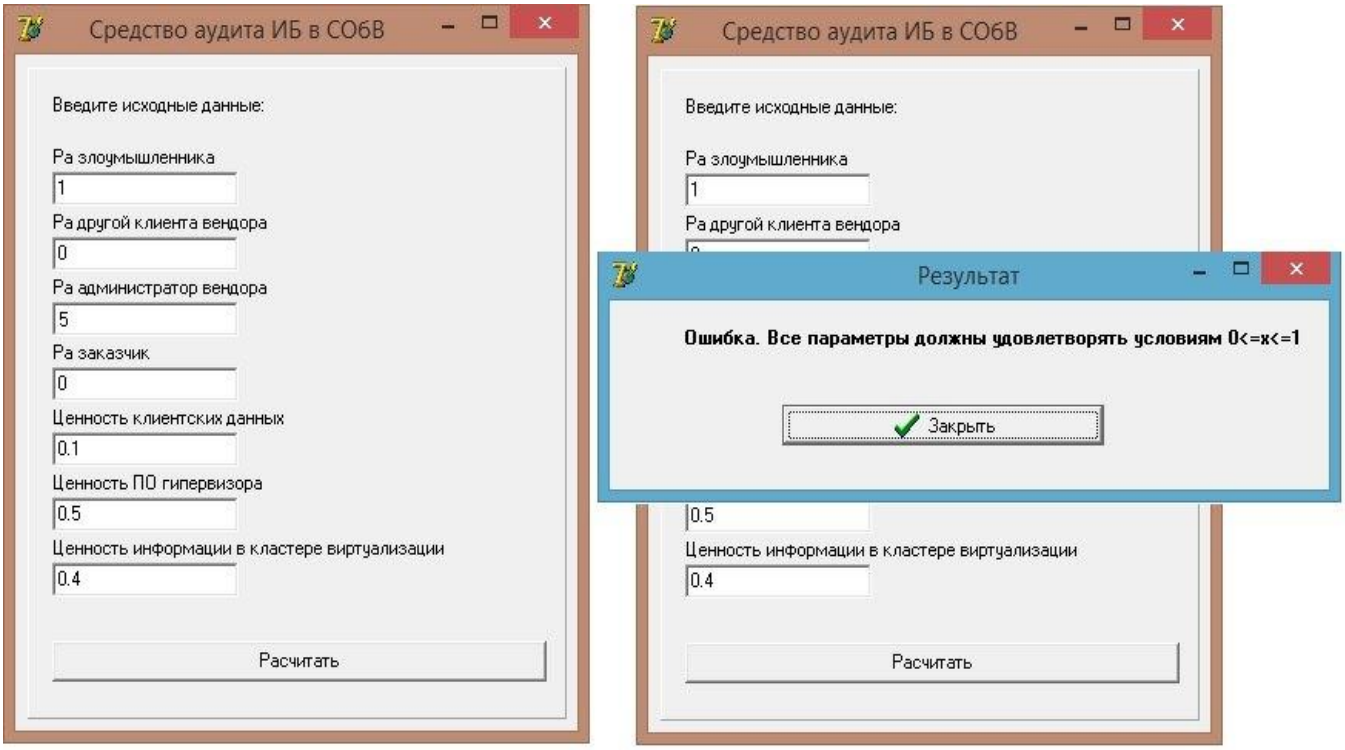


Рисунок 4.15 – Процедура контроля корректности вводимых данных и экранная форма предупреждения об ошибке

На основе полученной информации о ценности активов, обрабатываемых в системе облачных вычислений, а также о вероятности активизации угрозы, реализуемой на том или ином пути, программный модуль рассчитывает уровень оперативного значения уровня риска нарушения информационной безопасности для СОбВ. Результаты расчета риска нарушения ИБ в реальном масштабе времени с помощью разработанного в диссертационной работе модуля представлены на рисунке 4.16.

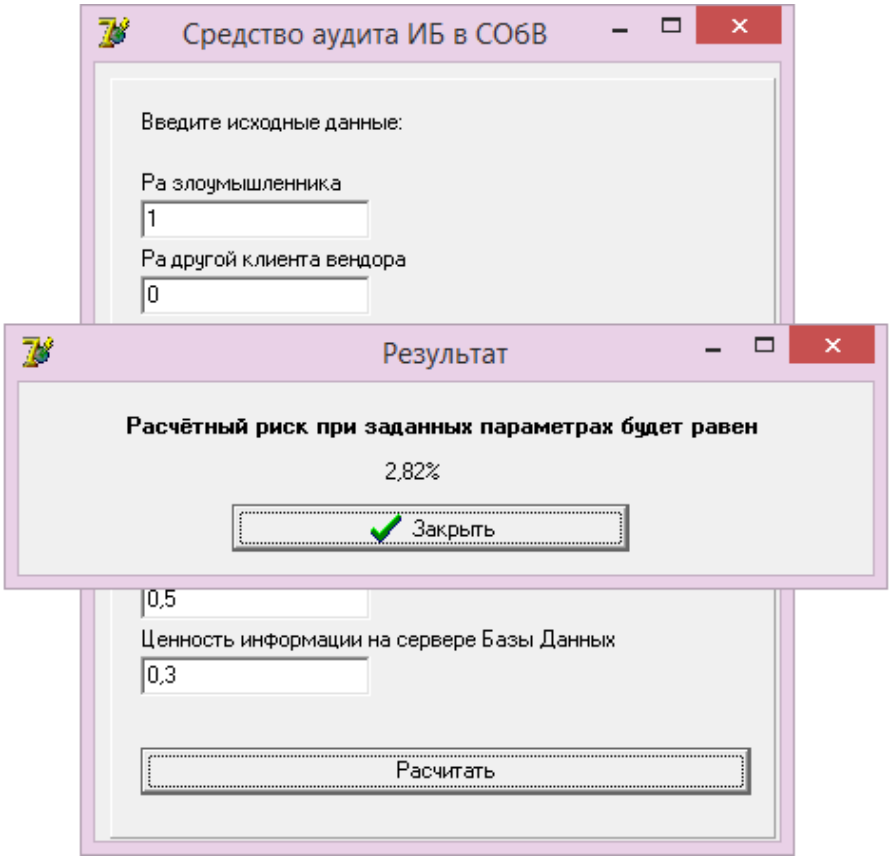


Рисунок 4.16 – Экранная форма с результатами работы программного модуля

Таким образом, показана функциональность программного модуля и доказана его применимость при проведении аудита информационной безопасности на примере системы облачных вычислений.

4.4 Описание результатов апробации разработанного программного модуля для аудита системы облачных вычислений

Метод экспертного аудита информационной безопасности и программно реализованный алгоритм решения задачи были апробированы для системы облачных вычислений, топология сети которой приведена в главе 2 диссертационной работы.

С помощью программного модуля был произведен вычислительный эксперимент, в ходе которого менялись значения вероятности активизации

угрозы и ценность информационных активов в диапазоне [0,1]. Для этого был сформирован тестовый набор, состоящий из значений входов нейронной сети, не входящих в исходную обучающую выборку для искусственной нейронной сети и помогающий определить, справится ли нейронная сеть с вычислениями, которые не были зафиксированы в обучающей выборке. В частности, на входы нейронной сети были поданы значения, когда два и более источников угроз активируются одновременно, а также значения различные значения ценностей с большой разрядностью. В обучающей выборке такие входные данные отсутствовали.

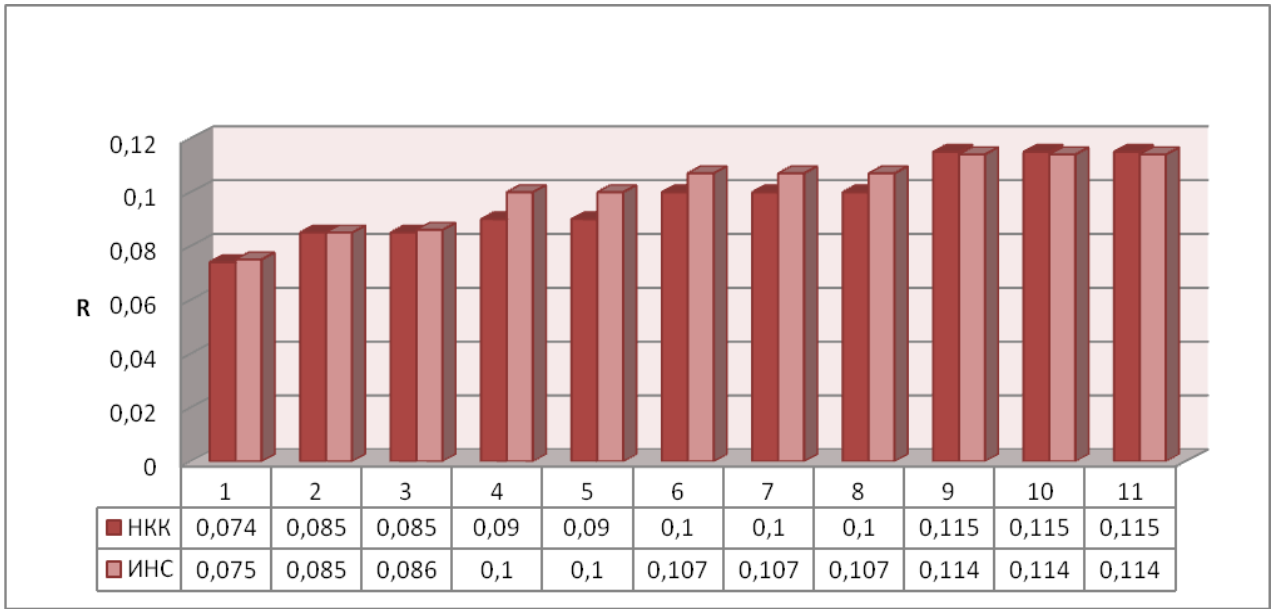
Результаты проводимого численного эксперимента сравнивались с эталонными значениями, полученными при расчете риска нарушения информационной безопасности, которые были рассчитаны вручную. В качестве иллюстрации сравнения эталонного значения уровня риска нарушения ИБ и значения, полученного опытным путем при расчете с помощью программного модуля приведена таблица 4.6.

Таблица 4.6 – Результаты тестирования программного модуля

Pu_зл	Pu_др_пт	Pu_пс	Pu_пт	C1 (Cl)	C3 (1)	C3 (2)	$R_{оп}$ (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

В таблице 4.6 значения вероятностей угроз, реализуемых: $P^{зл}$ – злоумышленником; $P^{ДР\_ПТ}$ – другим потребителем облачных услуг; $P^{ПС}$ – сотрудником поставщика облачных услуг; $P^{ПТ}$ – сотрудником потребителя облачных услуг (нарушителем политики безопасности).

Точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле, можно оценить с помощью диаграммы (рисунок 4.17).



	1	2	3	4	5	6	7	8	9	10	11
НКК	0,074	0,085	0,085	0,09	0,09	0,1	0,1	0,1	0,115	0,115	0,115
ИНС	0,075	0,085	0,086	0,1	0,1	0,107	0,107	0,107	0,114	0,114	0,114

Рисунок 4.17 – Диаграмма точности настройки ИНС

При построении диаграммы на оси абсцисс были отложены численные значения уровня риска, полученные в ходе вычисления по формулам без использования программного модуля. По оси ординат были отложены значения, полученные при тех же входных данных при обработке их с помощью программного модуля.

Таким образом, можно сделать вывод, что значения по ручному расчету и по расчету с помощью программного модуля отличаются друг от друга не более чем на тысячную долю даже в тех случаях, когда входные и выходные данные не были предварительно внесены в обучающую выборку искусственной нейронной сети. Среднее значение среднеквадратичная

ошибка обучения реализованной в программном модуле нейронной сети в общем случае составляет 10^{-3} mse.

В [102] отмечается, что угрозы нарушения информационной безопасности, связанные с деятельностью легальных пользователей ИС – внутренних источников угроз, превалируют над внешними. При этом, в статистике по инцидентам принимают участие как преднамеренные (целенаправленные), так и случайные угрозы.

С помощью программного модуля был проведен вычислительный эксперимент, в ходе которого изучалось зависимость риска нарушения информационной безопасности и ценности информационного актива системы облачных вычислений. За актив была принята информация в Cloud Storage.

На рисунке 4.18 приведены графики, отображающие зависимость величины оперативного значения риска нарушения информационной безопасности $\overline{R}$ от значения ценности информации объектов Cloud Storage.

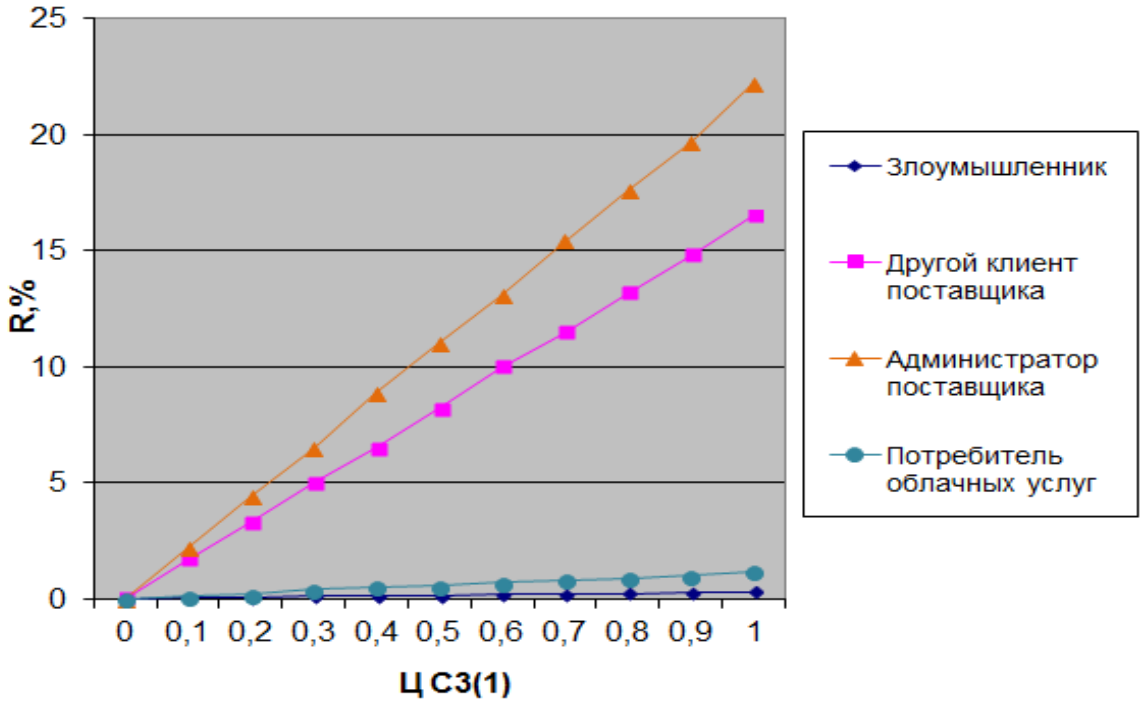


Рисунок 4.18 – График зависимости значения уровня риска и ценности информации

Таким образом, оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью внутренних источников угроз СОбВ (администратора поставщика облачных услуг и другого потребителя облачных услуг) являются с точки зрения ИБ наиболее опасными.

На основе проведенных в данной главе диссертационной работы экспериментов можно сделать выводы об эффективности и целесообразности предложенной методологии экспертного аудита информационной безопасности в системе облачных вычислений и разработанного на ее основе программного модуля «Средство аудита ИБ СОбВ».

4.5 Выводы по четвертой главе

1. Проведен численный эксперимент на сформированном массиве данных обучающей выборки в целях практического исследования эффективности алгоритма обратного распространения ошибки для обучения искусственной нейронной сети в предполагаемой области применения. Для эксперимента использовался программный модуль Matlab. Нейронная сеть прошла 10 эпох, постепенно обучаясь и сокращая ошибку обучения. При *обучении* ошибка составила около 10^{-4} мсэ, при *тестировании* сети – от 10^{-3} до 10^{-2} мсэ. Результаты обучения и тестирования нейронной сети показали возможность использования выбранной архитектуры и алгоритма обучения ИНС для разработки модуля численной оценки риска нарушения ИБ в программном модуле, предназначенном для автоматизации аудита нарушения ИБ информационной системы.

2. Разработана модель автоматизированного средства и блок-схема алгоритма работы программного модуля, реализующего метод экспертного аудита информационной безопасности. Модифицирована библиотека NeuralBase для создания программного модуля, использующего в своем составе персептрон с одним скрытым слоем, обучающийся по алгоритму

обратного распространения ошибки. Отличие от классического модуля заключается в исключении процедур работы с сетью Хопфилда и организации работы только с необходимым для проведения аудита персептроном, который обучается алгоритмом обратного распространения ошибки. Исключение процедур позволило ускорить работу библиотеки и снизить исходный размер листинга программы для ее более корректной работы. Модули использующейся библиотеки описаны с помощью UML-диаграммы.

3. Создан программный модуль, автоматизирующий процесс проведения аудита информационной безопасности, с помощью которого было оценено оперативное значения уровня риска нарушения информационной безопасности системы облачных вычислений. В примере, приведенном в диссертационной работа, суммарный риск нарушения информационной безопасности в реальном масштабе времени составил 2,82%. Оценена точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле, точность составила 0,1%.

4. Оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью внутренних источников угроз СОбВ (администратора поставщика облачных услуг и другого потребителя облачных услуг) являются с точки зрения ИБ наиболее критичными для системы облачных вычислений. Графически показано, что угрозы нарушения информационной безопасности, связанные с деятельностью внутренних источников угроз, являются наиболее опасными.

ЗАКЛЮЧЕНИЕ

1. Предложены *модель политики* информационной *безопасности* ИСОТ и *методика разработки частной политики безопасности* СОбВ, *отличающаяся назначением* нескольких максимальных ролей, которые имеют одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества СОбВ, что позволяет *исключить* из иерархии ролей роль *суперпользователя*, имеющего полномочия напрямую обращаться к результирующим потокам данных, управлять всеми конфигурационными файлами СОБВ, и *увеличить* доверие потенциальных потребителей к ИСОТ.

2. Разработана модель преднамеренных (целенаправленных) угроз нарушения информационной безопасности в системе облачных вычислений, основанная на построении нечетких когнитивных карт, в которой учитываются специфичные угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, с деятельностью такого источника угроз как другой потребитель облачных услуг, который, является клиентом облака сообщества и должен обслуживаться поставщиком изолированно от потребителя облачных услуг.

3. Предложено два подхода к аудиту ИБ СОбВ: расчет *прогнозируемого* значения риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз и расчет *оперативного* значения риска нарушения ИБ, когда угроза проявляется по конкретному пути распространения в реальном масштабе времени.

4. Предложен *метод* проведения *экспертного аудита* информационной безопасности, который позволяет получить численную оценку *оперативного* значения уровня риска нарушения информационной безопасности с использованием искусственной нейронной сети, при обработке ею информации с сенсоров и датчиков опасных событий, обучение

которой осуществляется на множестве данных обучающей выборки, сформированной на основе расчетных значений прогнозируемого уровня риска нарушения информационной безопасности, что позволит поставщику облачных услуг *обеспечить* адекватное реагирование на возможные инциденты в реальном масштабе времени и *обосновать* свои возможности по обеспечению защищенности критичной информации потребителя.

5. Создан программный модуль, автоматизирующий процесс проведения аудита информационной безопасности, с помощью которого оценено оперативное значения уровня риска нарушения информационной безопасности системы облачных вычислений. В примере, приведенном в диссертационной работа, суммарный риск нарушения информационной безопасности в реальном масштабе времени составил 2,82%. Оценена точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле, точность составила 0,1%.

6. Оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью внутренних источников угроз СОбВ (администратора поставщика облачных услуг и другого потребителя облачных услуг), являются с точки зрения ИБ наиболее критичными для системы облачных вычислений.

Перспективы дальнейшей разработки темы.

Дальнейшим развитие диссертационной работы может быть исследование возможности выбора рационального варианта оперативного реагирования на возможные инциденты, связанные с увеличением уровня риска в реальном масштабе времени.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

API − application programming interface, интерфейс программирования приложений

ИС – информационная система

СОбВ – система облачных вычислений

ЗИ – защита информации

ИБ – информационная безопасность

ИР – информационные ресурсы

ИСОТ − информационная система, построенная на основе облачных технологий

ИТ – информационные технологии

ИТТ – информационные и телекоммуникационные технологии

КИС – корпоративная информационная система

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПО – программное обеспечение

РД – руководящий документ

РС – рабочая станция

СВТ – средство вычислительной техники

СЗИ – система защиты информации

СОИБ – система обеспечения информационной безопасности

СрЗ – средство защиты

ЦОД – центр обработки данных

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. / В.Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592с.

2. ГОСТ Р XXXXX—20XX (проект, первая редакция) «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения». [Электронный ресурс] – Режим доступа : https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVlnT21yZ0k/preview

3. Сахнюк, П. А., Основы облачных технологий [Электронный ресурс] – Режим доступа : http: //www.stgau.ru/company/personal/ user/7684/files/lib/.

4. Баранова, Е.Н., «Концепция Cloud computing» [Электронный ресурс] – Режим доступа : www.itcontent.ru/archives/blog/cloud_computing

5. John Dinsdeil Synergy Research Group [Электронный ресурс] – Режим доступа : synergycro.ru/

6. Отчеты Forrester Research Кэмбридж (Массачусетс), США, [Электронный ресурс] – Режим доступа: forrester.com.

7. Риз, Дж Облачные вычисления: Пер с англ. / Дж Риз, СПб.: БВХ-Петербург, 2011 – 288 с.

8. Барский, А.Б, Желенков, Б.В. Средства оптимизации информационного взаимодействия ресурсных процессоров для минимизации времени «облачных» вычислений // Информационные технологии. – 2016. – № 1. Т. 22. – С. 14-21.

9. Андрей Авраменко «Облачные вычисления». Взгляд из IBM // Jet Info. – 2010. – № 10. С. 63-75.

10. Коваленко, О.С, Курейчик В.М. Обзор проблем и состояний облачных вычислений и сервисов // Известия Южного федерального университета. – 2012. – №7. Т. 132. – С. 146-152.

11. Клермонтский отчет об исследованиях в области баз данных . 2012. [Электронный ресурс] – Режим доступа : http://citforum.ru/database/articles/claremont_report/

12. Облачные вычисления. Блог ИТ «Альфа-банк» [Электронный ресурс] – Режим доступа : http://www.4cio.ru/pages/index/129.

13. Потехин, В.С., Синещук Ю.И., Скряга Ю.А. Информационные угрозы и уязвимости технологии облачных вычислений // Материалы VIII Санкт-Петербургской конференции «Информационная безопасность регионов России (ИБРР-2013)» / СПОИСУ. – СПб., 2013. – 293 с.

14. А.В., Долбилов, Литягин П.Е. Технология облачных вычислений. // МИР телекома. – 2013. − №1. С. 3-14.

15. IBM Spectrum Computing [Электронный ресурс] – Режим доступа: platform.com

16. Кузнецов, С.В. Обзор мартовского номера журнала Computer // IEEE Computer Society. – 2011. − № 3, Т. 44. – С 141-167.

17. Петров, Д. Встречный план [Электронный ресурс] – Режим доступа: www.kommersant.ru/doc.aspx?DocsID=1162192

18. Hugh Macleod Cloud Computing [Electronic resource]. – URL: technorati.com/posts/lv3vwaZ9hbuGSZx_jQseIqaVSlj29LQGjWyRkNoZ4b0%3D?reactions

19. Bill Thompson Storm warning for cloud computing [Electronic resource]. – URL: news.bbc.co.uk/2/hi/technology/7421099.stm

20. Tim O'Reilly «Web 2.0 and Cloud Computing» [Electronic resource]. – URL: radar.oreilly.com/2008/10/web-20-and-cloud-computing.html

21. Сенцова, А.Ю. Анализ проблемы обеспечения информационной безопасности в облачных средах // А.Ю. Сенцова, И.В. Машкина. Безопасность информационных технологий, М.: Центр экспертизы и координации информатизации. – 2014. – №1, С 72-74.

22. Ивонин, П.В. Безопасность облака в деталях // Безопасность информационных технологий, М.: Центр экспертизы и координации информатизации. – 2013. – №2, С 37-40.

23. Демурчев Н.Г., Ищенко С.О. Проблемы обеспечения информационной безопасности при переходе на облачные вычисления/ Н.Г.Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 265 с.

24. ГОСТ Р ИСО/МЭК 12207-10 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств». М.: Стандартинформ, 2010.

25. Официальный сайт Cloud Security Alliance (CSA) [Электроный ресурс]. – Режим доступа: https://cloudsecurityalliance.org/

26. Безопасность как головная боль облачных вычислений [Электрон. ресурс]. – Режим доступа: http://eopu.tu-bryansk.ru/index.php/news/46-bezopasnost-kak-golovnaya-bol-oblachnyx-vychislenij.html

27. А. Б. Данилов, Кармановский Н. С., Проблемы обеспечения безопасности облачных вычислений [Текст] // Сборник трудов молодых ученых, аспирантов и студентов научно-педагогической школы кафедры ПБКС «Информационная безопасность, проектирование и технология элементов и узлов компьютерных систем». / Под ред. Ю. А. Гатчина. –СПб: НИУ ИТМО, 2013. Выпуск 1. –С. 54 –60.

28. Андрей Федив. Сервис для хранения файлов: какой выбрать. // Копьюттера-Онлайн. Мой друг компьютер. – 2011. − №15. С. 32—22.

29. Мурзина Л., Закон для IaaS[Электронный ресурс] –Режим доступа:http://www.osp.ru/nets/2013/04/13037392/

30. Облачное хранилища данных [Электрон. ресурс]. – Режим доступа: http://forum.ru-board.com/topic.cgi?forum=5&topic=35708.

31. Официальный сайт журнала «Компьютер-Пресс» [Электронный ресурс]. – Режим доступа: http://compress.ru/article.aspx?id=21238&iid=967

32. Коржов Валерий Вход в облака: Аутентификация пользователей облачных сервисов - ключевая проблема безопасности в облаках // Журнал Computerworld. – 2013. – № 02. С 142-151.

33. Бойцов И. Н. Обзор проекта ГОСТ по защите информации в облаках [Электронный ресурс]. – Режим доступа: http://bis-expert.ru/blog/5336/43325

34. Официальный сайт Федерального агентства по техническому регулированию и метрологии (РОССТАНДАРТ) [Электронный ресурс]. – Режим доступа: http://www.gost.ru/wps/portal/pages.TechCom

35. Консультант плюс проект ФЗ 149«О внесении изменений в отдельные законодательные акты РФ в части использования облачных вычислений» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/law/hotdocs/33631.html

36. Проект ГОСТ Р XXXXX-20XX «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Основные положения»

37. Демурчев, Н.Г. Исследование существующих методов и средств защиты данных в моделях SaaS [Текст]/ Н.Г. Демурчев, .Т.К. Алимурадов. – Материалы XII Международной научно-практической конференции «ИБ-2012». Ч.1. – Таганрог: Изд-во ТТИ ЮФУ, 2012.− 346 с.

38. Орлик, С. Облачные вычисления: обзор и рекомендации [Электронный ресурс] /С. Орлик. – Режим доступа: http://cloud.sorlik.ru/synopsis-4.html.

39. Жиров, А.О. Безопасные облачные вычисления с помощью гомоморфной криптографии Безопасность информационных технологий, М.: Центр экспертизы и координации информатизации. – 2013. – №1, С 6-12.

40. Ханна, Стив Безопасность облачных вычислений: есть вопросы? [Электронный ресурс] / Стив Ханна, Есус Молина. – Режим доступа: http://cloudzone.ru/articles/analytics/11.html

41. Шпунт, Яков Как сделать облако безопасным. Рекомендации Cloud Security Alliance [Электронный ресурс] / Яков Шпунт. – Режим доступа: http://www.iemag.ru/clouds/opinions/detail.php?ID=25286

42. Машкина, И.В. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем // И.В. Машкина, А.Ю. Сенцова, РМ. Гузаиров, В. Е. Кладов Известия ЮФУ Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ. – 2012. №1. С. 25-35.

43. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — 379 p. — (Computer Communications and Networks).

44. Шумский А. А. Системный анализ в защите информации: учеб. Пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Шумский, А. А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

45. Основные международные стандарты и лучшие практики проведения аудита ИТ [Электронный ресурс]. – Режим доступа:http://habrahabr.ru/post/224895/

46. Симонов С.С. Аудит безопасности ИС // С.С. Симонов журнал Jet Info. – 2014. – №9 (76). С. 27-38.

47. Официальный сайт Softline [Электронный ресурс]. – Режим доступа: http://softline.ru/

48. National Institute of Standards and Technology [Электронный ресурс]. – Режим доступа:http://www.nist.gov/

49. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасности / С. А. Петренко, С. В. Симонов. – М. ДМК Пресс, 2004. – 392 с.

50. Официальный Интернет -ресурс ФСТЭК России. Техническая защита конфиденциальной информации. [Электронный ресурс] –Режим доступа:http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty.

51. Марков, А.С. Управление рисками – нормативный вакуум информационной безопасности Открытые системы №8, 2007 [Электронный ресурс]. – Режим доступа: http://www.osp.ru/os/2007/08/4492873

52. Белов, Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось и др. − М.: Горячая линия-Телеком, 2006. – 544 с.

53. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» введ. 01.02.2008. – М: Стандартинформ, 2008. – 31 с.

54. Программные средства проверки политики безопасности на соответствие ISO 17799 [Электронный ресурс] – Режим доступа: http://www.ixbt.com/cm/iso17799-cobra-kondor012004.shtml

55. Марков А.С. Управление рисками – нормативный вакуум информационной безопасности / А. С. Марков, В. Цирлов // Открытые системы №8, 2007.

56. Малюк А. А. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. / А. А. Малюк, С. В. Пазизин, Н. С. Погожин – 4-е издание, стереотип. – М.: Горячая линия – Телеком, 2011. – 146 с.

57. Краковский Ю. М. Информационная безопасности и защита информации: учеб. пособие / Ю. М. Краковский. – М.: ИКЦ «МарТ», 2008. – 288 с.

58. Нестеров С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsof. Методики и программные

продукты для оценки рисков. [Электрон. ресурс]. – Режим доступа: http://www.intuit.ru/department/itmngt/riskanms/4/

59. Машкина И. В. Анализ рисков объектов информатизации: учебное пособие / И. В. Машкина, Е. С. Степанова, Т. О. Вишнякова; Уфимск. гос. авиац. техн. ун-т. – Уфа: УГАТУ, 2011. – 112с.

60. Современные методы и средства анализа и управление рисками информационных систем компаний [Электрон. ресурс]. – Режим доступа: http://citforum.ru/products/dsec/cramm/cramm2.shtml

61. Львова А. В. Метод анализа и управления рисками безопасности защищенной информационной системы: автореф. дис. канд. техн. наук : 05.13.01, 05.13.19 / Анастасия Владимировна Львова. – М., 2009 – 20 с.

62. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Электрон. ресурс]. – Режим доступа: http://www.dsec.ru/about/articles/grif_ar_methods/

63. Гузаиров М. Б. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности / М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова // Безопасность информационных технологий. №2, 2011. С 37-49.

64. Степанова Е. С. Программная система оценки рисков нарушения информационной безопасности на основе построения нечетких когнитивных карт/ Е. С. Степанова, Р.М. Хабибуллин, И. В. Машкина // Материалы XII Международной научно-практической конференции «Информационная безопасность» Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 185-191.

65. Степанова Е. С. Программный модуль реализации алгоритма численной оценки риска нарушения информационной безопасности / Е. С. Степанова, И. В. Кансафаров // Безопасность информационных технологий. №1, 2011. С. 128-130.

66. Облачная безопасность, защищенные вычисления [Электрон. ресурс]. – Режим доступа: **trendmicro**.com.ru

67. Абрамов, Ю.А, Абстрактно-алгебраические модели дискретных систем/ Ю.А. Абрамов, Калининский университет, 1981 г. −133 с.

68. Суворов В.В. Абстрактно-алгебраический подход к построению вычислительных сред для решения задач в объектных формулировках // Вычислительные методы и программирование, 2011. – Т. 11. С. 50-61.

69. ГОСТ-50922-2006 Защита информации. Основные термины и определения– М: Стандартинформ, 2006. – 12 с.

70. Машкина, И. В. Методология экспертного аудита в системе облачных вычислений // И.В. Машкина, А.Ю. Сенцова. Безопасность информационных технологий. 2013. № 4. С. 63−70.

71. Варлатая С.К., Шахинова М.В. Анализ методов описания политики безопасности при разработке информационно-безопасных технологий. // Доклады ТУСУР, Ч. 1 «Аудит безопасности», №1 (21), , июнь 2010. С. 10-13.

72. РС БР ИББС-2.0-2007 Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0. М.: Стандартинформ, 2007. 15 с.

73. Joshi, J. A Generalized Temporal Role -Based Access Control Model / J. Joshi, E.A Bertino, U. Latif, A. Ghafoor // IEEE Trans. Knowledge and Data Engineer-ing. 2005. No. 17(1). P. 4–23.

74. National Institute of Standards and Technology. Role Based Access Con-trol (RBAC) and Role Based Security [Electronic resource]. – Режим доступа:http://csrc.nist.gov/groups/ SNS/rbac.

75. Методология организации технической поддержки [Электронный ресурс] – Режим доступа: http://msbro.ru/index.php/archives/2717

76. Гузаиров, М. Б. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности / М. Б. Гузаиров,

И. В. Машкина, Е. С. Степанова // Безопасность информационных технологий. №2, 2011. С 37-49.

77. Борисов, В.В. Нечеткие модели и сети. / В. В. Борисов, В.В. Круглов, А.С. Федулов— М. : Горячая линия - Телеком, 2007 .— 283 с.

78. Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие / В.И. Васильев. – М.: Машиностроение, 2010. – 152 с.

79. Официальный сайт международной базы данных уязвимостей [Электронный ресурс] – Режим доступа: https://nvd.nist.gov/.

80. Аудит информационной безопасности https://ru.wikipedia.org/wiki/ [Электронный ресурс] – Режим доступа: Аудит_информационной_безопасности.

81. Симонов, С.П. Аудит информационной безопасности // Информационный бюллетень Jet Info. – М.: Компания Джет Инфо Паблишер. – 1999, №9(76), 24 с.

82. Маркин, Д.Т. Аудит безопасности: какой, кому, зачем? [Электронный ресурс] – Режим доступа: http://bosfera.ru/bo/audit-informatsionnoj-bezopasnosti.

83. Официальный сайт СКБ Контур «Аудит информационной безопасности» [Электронный ресурс] – Режим доступа: https://kontur.ru/security/features/audit-ib

84. Сердюк В. А. Аудит информационной безопасности // ITResearch BYTE – 2006, №4(92). С. 165-183.

85. Седов О. Облака на горизонте // Директор информационной службы – 2010, № 07. С 43-48.

86. Перегудов, Ф.И. Введение в системный анализ: Учеб. Пособие для вузов / Ф.И. Перегудов, Ф.П. Тарасенко. – М.: Высшая школа., 1989. – 367 с.

87. Шумский, А.А. Системный анализ в защите информации: учеб. Пособие для студентов вузов, обучающихся по специальностям в обл.

информ. безопасности / А. А. Шумский, А. А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

88. Сердюк, В.А. Аудит информационной безопасности как мера для повышения уровня защиты компании // T-Comm спецвыпуск по ИБ – 2009, С. 24-26.

89. Программные средства проверки политики безопасности на соответствие ISO 17799 [Электронный ресурс] – Режим доступа: http://www.ixbt.com/cm/iso17799-cobra-kondor012004.shtml

90. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» введ. 01.12.2011. – М: Стандартинформ, 2011. – 51 с.

91. Гузаиров М. Б. Метод определения ценности информации с использованием аппарата нечеткой логики / М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова // Безопасность информационных технологий. №1, 2012. С 18-29.

92. Галушка, В.В., Фатхи В.А. Формирование обучающей выборки при использовании искусственных нейронных сетей в задачах поиска ошибок баз данных // В.В. Галушка, В.А. Фатхи. − Ростов-на-Дону: Инженерный вестник Дона, №2 (25) т. 25, 2013. – С. 237-242.

93. Representati veness of data // BaseGroup Labs — Глоссарий [Электронный ресурс] – Режим доступа: http://www.basegroup.ru/glossary/definitions/representativeness/

94. Барсегян, А.А. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP / А. А. Барсегян, М.С. Куприянов, М.С. Кузнецов, В.В. Степаненко, И.И. Холод, 2-е изд. перераб. и доп. — СПб.: БХВ-Петербург, 2007. — 384 с.

95. Осовский С. Нейронные сети для обработки информации / Пер. с польского И. Д. Рудинского. М.: Финансы и статистика, 2002. – 344 с.

96. J. Hopfield, «Neural networks and physical systems with emergent collective computational abilities», Proceedings of National Academy of Sciences, vol. 79 no. 8 pp. 2554—2558, April 1982.

97. Розенблатт, Ф. Принципы нейродинамики: Перцептроны и теория механизмов мозга / Ф. Розенблатт — М.: Мир, 1965. — 480 с.

98. Рутковский, Л. Методы и технологии искусственного интеллекта / Лешек Рутковский. – Пер. в польского И.Д. Рудинского. – М. : Горячия линия-Телеком, 2010. – 520 с.

99. Черемных С. В. Структурный анализ систем: IDEF-технологии / С. В. Черемных, И. О. Семенов, В. С. Ручкин. – М.: Финансы и статистика, 2003. – 208 с.

100. Свидетельство о государственной регистрации программы для ЭВМ № 2014616279 от 19.06.14 Средство проведения экспертного аудита информационной безопасности / Сенцова А.Ю., Машкина И.В., Чайка В.Ю.

101. Сенцова, А.Ю. Автоматизация экспертного аудита информационной безопасности на основе использования искусственной нейронной сети // А.Ю. Сенцова, И.В. Машкина. Безопасность информационных технологий. – М.: Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ, №2, 2014. С. 118-126.

102. Брэгг, Роберта Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг; пер. с англ. – М.: Издательство «Эконом», 2006. – 912 с.

103. Машкина, И.В. Разработка нечетких когнитивных карт и искусственной нейронной сети для оперативной оценки информационных рисков в системе облачных вычислений // И.В. Машкина, А.Ю. Сенцова, Е.С. Степанова Журнал «Нейрокомпьютеры разработка и применение». – М.: Изд-во «Радиотехника», 2013. С 26-30

104. Сенцова, А. Ю. Анализ информационных рисков в среде облачных вычислений на основе интеллектуальных технологий // А.Ю. Сенцова, И.В. Машкина Безопасность информационных технологий. – М.:

Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ, №1, 2013. С. 120-121.

105. Сенцова, А. Ю. Метод получения численной оценки уровня риска в системе облачных вычислений на основе данных об опасных событиях в реальном масштабе времени // А.Ю. Сенцова, И.В. Машкина. Материалы XIII Международной научно-практической конференции «Информационная безопасность-2013» Ч. 2. Материалы III Всероссийской молодежной конференции «Перспектива-2013». – Таганрог: Изд-во ЮФУ, 2013. 252с. – С. 209-215.

106. Oleg Makarevich The method of the information security risk assessment // Oleg Makarevich, Irina Mashkina, Alina Sentsova. Proceedings of the 6th International Conference on Security of Information and Networks (SIN-2013), Aksaray, Turkey. P 446-447.

107. Сенцова, А.Ю. Программное средство для оценки оперативного значения риска нарушения информационной безопасности в системе облачных вычислений // А.Ю. Сенцова, И.В. Машкина. Известия ЮФУ. Технические науки. – Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ. – 2014,№8. С. 6-16.

108. Сенцова, А.Ю. Разработка частной политики информационной безопасности системы облачных вычислений // А.Ю. Сенцова, И.В. Машкина. Вестник УГАТУ. – 2016. – Том 20, № 2 (72). – С. 134-142.

Приложение А

Сведения о практическом использовании результатов диссертационного исследования

АТЛАС ТЕЛЕКОМ

450006, г. Уфа, б-р Ибрагимова, 37, 2 этаж
Адрес для переписки: 450006, г. Уфа, а/я 132
Тел./Факс: (347) 292-98-40
E-mail: atk.ufa@mail.ru
Сайт: www.atlas02.ru

Для представления
в диссертационный совет

АКТ
внедрения результатов диссертационной работы
Сенцовой Алины Юрьевны на тему
«Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений».

ООО «Атлас-Телеком» является потребителем облачных услуг. Для проведения внутреннего экспертного аудита информационной безопасности системы облачных вычислений, в ООО «Атлас-Телеком» использованы следующие результаты диссертационной работы Сенцовой А.Ю.:

- метод проведения экспертного аудита информационной безопасности системы облачных вычислений на основе использования искусственной нейронной сети;
- программный модуль, реализующий методологию аудита информационной безопасности системы облачных вычислений.

21.07.2016г.

Директор
ООО «Атлас-Телеком»
Куликов А.Ю.

Рисунок А.1 – Акт внедрения в ООО «Атлас-Телеком»

УТВЕРЖДАЮ
Проректор по учебной работе
ФГБОУ ВО «Уфимский
государственный авиационный
технический университет»
д.ф.-м.н., профессор

_____ Н.Г. Зарипов
«__9__» _____ 20_16_ г.

АКТ

внедрения в учебный процесс результатов диссертационной работы Сенцовой Алины Юрьевны на тему «Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 –Методы и системы защиты информации, информационная безопасность.

Комиссия в составе:
заведующего кафедрой вычислительной техники и защиты информации, д.т.н., профессора Васильева В.И.,
профессора кафедры вычислительной техники и защиты информации, д.т.н., профессора Фрида А.И.,
начальника учебного управления, к.э.н., доцента Косьяненко Н.Г.
составила акт о нижеследующем.

Результаты диссертационной работы Сенцовой А.Ю. используются в учебном процессе на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет» для преподавания дисциплин «Управление информационной безопасностью» студентам, обучающимся по направлению подготовки бакалавров 10.03.01 «Информационная безопасность», по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» и по направлению подготовки магистров 09.03.01 «Информатика и вычислительная техника» и 10.04.01 «Информационная безопасность».

Внедренные результаты включают:

- метод экспертного аудита информационной безопасности в системе облачных вычислений;
- метод численной оценки оперативного значения уровня риска нарушения информационной безопасности.

В 2016 году Сенцовой А.Ю. и Машкиной И.В. подготовлено и издано учебное пособие «Численная оценка риска в системе облачных вычислений с

Рисунок А.2 – Акт внедрения в учебный процесс ФГБОУ ВО «Уфимский государственный авиационный технический университет» (часть1)

использованием пакета прикладных программ Matlab»: лабораторный практикум по дисциплинам «Управление информационной безопасностью» и «Методы анализа информационных рисков», которое стало востребованным и пользуется спросом у студентов.

Заведующий кафедрой вычислительной техники и защиты информации, д.т.н., профессор — В.И. Васильев

Профессор кафедры вычислительной техники и защиты информации, д.т.н., профессор — А.И. Фрид

Начальник учебного управления, к.э.н., доцент — Н.Г. Косьяненко

Рисунок А.2 – Акт внедрения в учебный процесс ФГБОУ ВО «Уфимский государственный авиационный технический университет» (часть2)

Приложение Б

Свидетельство о государственной регистрации программы для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2014616279

Средство проведения экспертного аудита информационной безопасности

Правообладатели: ***Сенцова Алина Юрьевна (RU), Машкина Ирина Владимировна (RU), Чайка Валентина Юрьевна (RU)***

Авторы: ***Сенцова Алина Юрьевна (RU), Машкина Ирина Владимировна (RU), Чайка Валентина Юрьевна (RU)***

Заявка № **2014613593**
Дата поступления **21 апреля 2014 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***19 июня 2014 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов


SIN '13
CONF
6TH INTERNATIONAL CONFERENCE ON
SECURITY OF INFORMATION AND NETWORKS
November 26 - 28, 2013
Aksaray, Turkey
Award for Best Poster Paper
conferred by the jury / participants upon
Oleg Makarevich., Irina. Mashkina., Alina Sentseva
for the paper titled
The Method of The Information Security Risk Assessment.....
Prof.Dr. Atilla Elçi
SIN '13 General Chair
Prof.Dr. Mustafa Acar
Rector, Aksaray University
SIN '13 Honorary Chair
AHİLER
Kalkınma Ajansı
MACQUARIE
UNIVERSITY
AKSARAY UNIVERSITY
2006
STM
IGI
World Scientific
Connecting Great Minds

Приложение В

Обучающая выборка для обучения искусственной нейронной сети

Таблица В.1 - Множество данных обучающей выборки

Ра_ЗЛ	Ра_ДР_КЛ	Ра_ПОС	Ра_ПОТ	С1	С2	С3	R
1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0
0	0	0	1	0	0,2	0,8	0,009
0	0	0	1	0,1	0,2	0,7	0,022
0	0	0	1	0,2	0,2	0,6	0,034
0	0	0	1	0,3	0,2	0,5	0,047
0	0	0	1	0,4	0,2	0,4	0,06
0	0	0	1	0,5	0,2	0,3	0,071
0	0	0	1	0,6	0,2	0,2	0,084
0	0	0	1	0,7	0,2	0,1	0,096
0	0	0	1	0,8	0,2	0	0,1
0	0	0	1	0	0	0	0
0	0	0	1	0	0,3	0,7	0,008
0	0	0	1	0,1	0,3	0,6	0,021
0	0	0	1	0,2	0,3	0,5	0,033
0	0	0	1	0,3	0,3	0,4	0,046
0	0	0	1	0,4	0,3	0,3	0,058
0	0	0	1	0,5	0,3	0,2	0,07
0	0	0	1	0,6	0,3	0,1	0,083
0	0	0	1	0,7	0,3	0	0,095
0	0	0	1	0	0	0	0
0	0	0	1	0	0,4	0,6	0,007
0	0	0	1	0,1	0,4	0,5	0,019
0	0	0	1	0,2	0,4	0,4	0,032
0	0	0	1	0,3	0,4	0,3	0,044
0	0	0	1	0,4	0,4	0,2	0,057
0	0	0	1	0,5	0,4	0,1	0,07
0	0	0	1	0,6	0,4	0	0,082
0	0	0	1	0	0	0	0
0	0	0	1	0	0,5	0,5	0,0057
0	0	0	1	0,1	0,5	0,4	0,018
0	0	0	1	0,2	0,5	0,3	0,031

Продолжение таблицы В.1

1	2	3	4	5	6	7	8
0	0	0	1	0,3	0,5	0,2	0,043
0	0	0	1	0,4	0,5	0,1	0,056
0	0	0	1	0,5	0,5	0	0,068
0	0	0	1	0	0	0	0
0	0	0	1	0	0,6	0,4	0,005
0	0	0	1	0,1	0,6	0,3	0,017
0	0	0	1	0,2	0,6	0,2	0,03
0	0	0	1	0,3	0,6	0,1	0,042
0	0	0	1	0,4	0,6	0	0,054
0	0	0	1	0	0	0	0
0	0	0	1	0	0,7	0,3	0,0034
0	0	0	1	0,1	0,7	0,2	0,016
0	0	0	1	0,2	0,7	0,1	0,028
0	0	0	1	0,3	0,7	0	0,04
0	0	1	0	0	0	0	0
0	0	1	0	0	0,2	0,8	0,176
0	0	1	0	0,1	0,2	0,7	0,154
0	0	1	0	0,2	0,2	0,6	0,13
0	0	1	0	0,3	0,2	0,5	0,1
0	0	1	0	0,4	0,2	0,4	0,088
0	0	1	0	0,5	0,2	0,3	0,065
0	0	1	0	0,6	0,2	0,2	0,044
0	0	1	0	0,7	0,2	0,1	0,0219
0	0	1	0	0,8	0,2	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0,3	0,7	0,15
0	0	1	0	0,1	0,3	0,6	0,13
0	0	1	0	0,2	0,3	0,5	0,11
0	0	1	0	0,3	0,3	0,4	0,088
0	0	1	0	0,4	0,3	0,3	0,065
0	0	1	0	0,5	0,3	0,2	0,044
0	0	1	0	0,6	0,3	0,1	0,022
0	0	1	0	0,7	0,3	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0,4	0,6	0,13
0	0	1	0	0,1	0,4	0,5	0,11
0	0	1	0	0,2	0,4	0,4	0,087
0	0	1	0	0,3	0,4	0,3	0,065
0	0	1	0	0,4	0,4	0,2	0,044

Продолжение таблицы В.1

1	2	3	4	5	6	7	8
0	0	1	0	0,5	0,4	0,1	0,021
0	0	1	0	0,6	0,4	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0,5	0,5	0,11
0	0	1	0	0,1	0,5	0,4	0,087
0	0	1	0	0,2	0,5	0,3	0,065
0	0	1	0	0,3	0,5	0,2	0,044
0	0	1	0	0,4	0,5	0,1	0,021
0	0	1	0	0,5	0,5	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0,6	0,4	0,087
0	0	1	0	0,1	0,6	0,3	0,065
0	0	1	0	0,2	0,6	0,2	0,044
0	0	1	0	0,3	0,6	0,1	0,021
0	0	1	0	0,4	0,6	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0,7	0,3	0,065
0	0	1	0	0,1	0,7	0,2	0,044
0	0	1	0	0,2	0,7	0,1	0,021
0	0	1	0	0,3	0,7	0	0
0	1	0	0	0	0	0	0
0	1	0	0	0	0,2	0,8	0,13
0	1	0	0	0,1	0,2	0,7	0,12
0	1	0	0	0,2	0,2	0,6	0,11
0	1	0	0	0,3	0,2	0,5	0,1
0	1	0	0	0,4	0,2	0,4	0,09
0	1	0	0	0,5	0,2	0,3	0,08
0	1	0	0	0,6	0,2	0,2	0,07
0	1	0	0	0,7	0,2	0,1	0,06
0	1	0	0	0,8	0,2	0	0,05
0	1	0	0	0	0	0	0
0	1	0	0	0	0,3	0,7	0,12
0	1	0	0	0,1	0,3	0,6	0,1
0	1	0	0	0,2	0,3	0,5	0,095
0	1	0	0	0,3	0,3	0,4	0,08
0	1	0	0	0,4	0,3	0,3	0,075
0	1	0	0	0,5	0,3	0,2	0,06
0	1	0	0	0,6	0,3	0,1	0,05
0	1	0	0	0,7	0,3	0	0,04
0	1	0	0	0	0	0	0

Продолжение таблицы В.1

1	2	3	4	5	6	7	8
0	1	0	0	0	0,4	0,6	0,1
0	1	0	0	0,1	0,4	0,5	0,08
0	1	0	0	0,2	0,4	0,4	0,079
0	1	0	0	0,3	0,4	0,3	0,068
0	1	0	0	0,4	0,4	0,2	0,05
0	1	0	0	0,5	0,4	0,1	0,049
0	1	0	0	0,6	0,4	0	0,03
0	1	0	0	0	0	0	0
0	1	0	0	0	0,5	0,5	0,08
0	1	0	0	0,1	0,5	0,4	0,072
0	1	0	0	0,2	0,5	0,3	0,06
0	1	0	0	0,3	0,5	0,2	0,05
0	1	0	0	0,4	0,5	0,1	0,042
0	1	0	0	0,5	0,5	0	0,03
0	1	0	0	0	0	0	0
0	1	0	0	0	0,6	0,4	0,066
0	1	0	0	0,1	0,6	0,3	0,056
0	1	0	0	0,2	0,6	0,2	0,04
0	1	0	0	0,3	0,6	0,1	0,03
0	1	0	0	0,4	0,6	0	0,027
0	1	0	0	0	0	0	0
0	1	0	0	0	0,7	0,3	0,05
0	1	0	0	0,1	0,7	0,2	0,039
0	1	0	0	0,2	0,7	0,1	0,03
0	1	0	0	0,3	0,7	0	0,02
1	0	0	0	0	0	0	0
1	0	0	0	0	0,2	0,8	0,0067
1	0	0	0	0,1	0,2	0,7	0,013
1	0	0	0	0,2	0,2	0,6	0,019
1	0	0	0	0,3	0,2	0,5	0,025
1	0	0	0	0,4	0,2	0,4	0,031
1	0	0	0	0,5	0,2	0,3	0,038
1	0	0	0	0,6	0,2	0,2	0,044
1	0	0	0	0,7	0,2	0,1	0,049
1	0	0	0	0,8	0,2	0	0,056
1	0	0	0	0	0	0	0
1	0	0	0	0	0,3	0,7	0,009
1	0	0	0	0,1	0,3	0,6	0,015
1	0	0	0	0,2	0,3	0,5	0,021
1	0	0	0	0,3	0,3	0,4	0,03

Продолжение таблицы В.1

1	2	3	4	5	6	7	8
1	0	0	0	0,4	0,3	0,3	0,033
1	0	0	0	0,5	0,3	0,2	0,04
1	0	0	0	0,6	0,3	0,1	0,046
1	0	0	0	0,7	0,3	0	0,052
1	0	0	0	0	0	0	0
1	0	0	0	0	0,4	0,6	0,01
1	0	0	0	0,1	0,4	0,5	0,017
1	0	0	0	0,2	0,4	0,4	0,023
1	0	0	0	0,3	0,4	0,3	0,03
1	0	0	0	0,4	0,4	0,2	0,035
1	0	0	0	0,5	0,4	0,1	0,04
1	0	0	0	0,6	0,4	0	0,047
1	0	0	0	0	0	0	0
1	0	0	0	0	0,5	0,5	0,012
1	0	0	0	0,1	0,5	0,4	0,018
1	0	0	0	0,2	0,5	0,3	0,025
1	0	0	0	0,3	0,5	0,2	0,031
1	0	0	0	0,4	0,5	0,1	0,037
1	0	0	0	0,5	0,5	0	0,043
1	0	0	0	0	0	0	0
1	0	0	0	0	0,6	0,4	0,014
1	0	0	0	0,1	0,6	0,3	0,02
1	0	0	0	0,2	0,6	0,2	0,026
1	0	0	0	0,3	0,6	0,1	0,033
1	0	0	0	0,4	0,6	0	0,039
1	0	0	0	0	0	0	0
1	0	0	0	0	0,7	0,3	0,016
1	0	0	0	0,1	0,7	0,2	0,022
1	0	0	0	0,2	0,7	0,1	0,028
1	0	0	0	0,3	0,7	0	0,034
1	1	1	1	0	0	0	0
1	1	1	1	0	0,2	0,8	0,29
1	1	1	1	0,1	0,2	0,7	0,28
1	1	1	1	0,2	0,2	0,6	0,26
1	1	1	1	0,3	0,2	0,5	0,25
1	1	1	1	0,4	0,2	0,4	0,24
1	1	1	1	0,5	0,2	0,3	0,23
1	1	1	1	0,6	0,2	0,2	0,22
1	1	1	1	0,7	0,2	0,1	0,21
1	1	1	1	0,8	0,2	0	0,19

Окончание таблицы В.1

1	2	3	4	5	6	7	8
1	1	1	1	0	0	0	0
1	1	1	1	0	0,3	0,7	0,26
1	1	1	1	0,1	0,3	0,6	0,24
1	1	1	1	0,2	0,3	0,5	0,233
1	1	1	1	0,3	0,3	0,4	0,22
1	1	1	1	0,4	0,3	0,3	0,21
1	1	1	1	0,5	0,3	0,2	0,19
1	1	1	1	0,6	0,3	0,1	0,188
1	1	1	1	0,7	0,3	0	0,17
1	1	1	1	0	0	0	0
1	1	1	1	0	0,4	0,6	0,22
1	1	1	1	0,1	0,4	0,5	0,21
1	1	1	1	0,2	0,4	0,4	0,2
1	1	1	1	0,3	0,4	0,3	0,19
1	1	1	1	0,4	0,4	0,2	0,17
1	1	1	1	0,5	0,4	0,1	0,16
1	1	1	1	0,6	0,4	0	0,155
1	1	1	1	0	0	0	0
1	1	1	1	0	0,5	0,5	0,19
1	1	1	1	0,1	0,5	0,4	0,178
1	1	1	1	0,2	0,5	0,3	0,17
1	1	1	1	0,3	0,5	0,2	0,155
1	1	1	1	0,4	0,5	0,1	0,14
1	1	1	1	0,5	0,5	0	0,13
1	1	1	1	0	0	0	0
1	1	1	1	0	0,6	0,4	0,156
1	1	1	1	0,1	0,6	0,3	0,15
1	1	1	1	0,2	0,6	0,2	0,13
1	1	1	1	0,3	0,6	0,1	0,12
1	1	1	1	0,4	0,6	0	0,11
1	1	1	1	0	0	0	0
1	1	1	1	0	0,7	0,3	0,12
1	1	1	1	0,1	0,7	0,2	0,11
1	1	1	1	0,2	0,7	0,1	0,1
1	1	1	1	0,3	0,7	0	0,08

Приложение Г

Исходный текст программы «Средство аудита ИБ в СОбВ»

```
unit Unit1;
interface
// описание используемых библиотек
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms,
Dialogs,
  StdCtrls, NeuralBaseComp, NeuralBaseTypes, ComCtrls, Spin, ExtCtrls,
  Buttons;
Описание классов графических компонентов и процедур
type
  TForm1 = class(TForm)
    Panel1: TPanel;
    Label1: TLabel;
    RadioButton1: TRadioButton;
    RadioButton2: TRadioButton;
    BitBtn1: TBitBtn;
    Panel2: TPanel;
    Label2: TLabel;
    LabeledEdit1: TLabeledEdit;
    LabeledEdit2: TLabeledEdit;
    LabeledEdit3: TLabeledEdit;
    LabeledEdit4: TLabeledEdit;
    LabeledEdit5: TLabeledEdit;
    LabeledEdit6: TLabeledEdit;
    LabeledEdit7: TLabeledEdit;
    Button1: TButton;
    Label3: TLabel;
```

```
    Label4: TLabel;
    Label5: TLabel;
    BitBtn2: TBitBtn;
    Memo1: TMemo;
    NeuralNetBP1: TNeuralNetBP;
    ProgressBar1: TProgressBar;
    procedure BitBtn1Click(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure RadioButton1Click(Sender: TObject);
    procedure RadioButton2Click(Sender: TObject);
    procedure NeuralNetBP1EpochPassed(Sender: TObject);
    procedure BitBtn2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;
var
  Form1: TForm1;
implementation
uses Unit2;
{$R *.dfm}
Процедура обучения нейронной сети
procedure TForm1.BitBtn1Click(Sender: TObject);
var
  xInputVector: TVectorFloat; //входной вектор
  xOutputVector: TVectorFloat; //выходной вектор
  i,j,k:integer; //служебные переменные
  s:string;
begin
```

```
Panel1.Height := 300;
ProgressBar1.Show;
Загрузка обучающей выборки
If RadioButton1.Checked then
    memo1.Lines.LoadFromFile('client.txt')
   else
    memo1.Lines.LoadFromFile('vendor.txt');
  NeuralNetBP1.ResetPatterns;
// устанавливаем размерности входного и выходного векторов
  SetLength(xInputVector, 7);
  SetLength(xOutputVector, 1);
// разбираем текстовый массив на переменные для векторов
Процедура загрузки вектора в нейронную сеть
  For i:=0 to memo1.Lines.Count-1 do
    begin
      s := '';
      k := 0;
      For j := 1 to length(memo1.lines[i])-1 do
        begin
          If memo1.lines[i][j]<>chr(VK_tab) then
            s := s + memo1.lines[i][j]
          else
            begin
              xInputVector[k] := StrToFloat(s);
              inc(k);
              s := '';
            end;
          If j = length(memo1.lines[i])-1 then
           xOutputVector[0] := StrToFloat(s);
        end;// загружаем вектора в нейронную сеть
```

```
NeuralNetBP1.AddPattern(xInputVector, xOutputVector);
    end;// инициализируем процесс обучения
  NeuralNetBP1.TeachOffLine;
  end;
  Процедура проверки корректности входных данных
  procedure TForm1.Button1Click(Sender: TObject);
  var
    xInputVector: TVectorFloat;
    err : array [0..7] of boolean;
    i : byte;
  begin
    For i := 0 to 7 do
      err[i] := false;
    If (LabeledEdit1.Text = '0') or (LabeledEdit1.Text = '1') then
      err[0] := true
    else
      Showmessage('значение'+LabeledEdit1.EditLabel.Caption+'      должно
быть равно 1 или 0');
    If (LabeledEdit2.Text = '0') or (LabeledEdit2.Text = '1') then
      err[1] := true
    else
      Showmessage('значение'+LabeledEdit2.EditLabel.Caption+'      должно
быть равно 1 или 0');
    If (LabeledEdit3.Text = '0') or (LabeledEdit3.Text = '1') then
      err[2] := true
    else
      Showmessage('значение'+LabeledEdit3.EditLabel.Caption+'      должно
быть равно 1 или 0');
    If (LabeledEdit4.Text = '0') or (LabeledEdit4.Text = '1') then
      err[3] := true
```

```
        else
          Showmessage('значение'+LabeledEdit4.EditLabel.Caption+' должно
быть равно 1 или 0');
        If (StrToFloat(LabeledEdit5.Text)>0) and
(StrToFloat(LabeledEdit5.Text)<1) then
          err[4] := true
        else
          Showmessage('значение'+LabeledEdit5.EditLabel.Caption+' должно
быть больше 0 и меньше 1');
        If (StrToFloat(LabeledEdit6.Text)>=0.2) and
(StrToFloat(LabeledEdit6.Text)<=0.7)and(Radiobutton1.Checked) then
          err[5] := true
        else
          Showmessage('значение '+LabeledEdit6.EditLabel.Caption+' должно
быть больше 0,2 и меньше 0,7');
        If (StrToFloat(LabeledEdit7.Text)>0) and
(StrToFloat(LabeledEdit7.Text)<1) then
          err[6] := true
        else
          Showmessage('значение'+LabeledEdit7.EditLabel.Caption+' должно
быть больше 0 и меньше 1');
        If
(StrToFloat(LabeledEdit5.Text)+StrToFloat(LabeledEdit6.Text)+StrToFloat(Label
edEdit7.Text))=1 then
          err[7] := true
        else
          Showmessage('сумма параметров '+LabeledEdit5.EditLabel.Caption+'
+ '+LabeledEdit6.EditLabel.Caption+' + '+LabeledEdit7.EditLabel.Caption+'
должно быть равно 1');
```

```
If err[1] and err[2]and err[3] and err[4] and err[5] and err[6] and err[7] then
Begin// если всё корректно формируем необходимый вектор
SetLength(xInputVector, 7);
xInputVector[0] := StrToFloat(LabeledEdit1.Text);
xInputVector[1] := StrToFloat(LabeledEdit2.Text);
xInputVector[2] := StrToFloat(LabeledEdit3.Text);
xInputVector[3] := StrToFloat(LabeledEdit4.Text);
xInputVector[4] := StrToFloat(LabeledEdit5.Text);
xInputVector[5] := StrToFloat(LabeledEdit6.Text);
xInputVector[6] := StrToFloat(LabeledEdit7.Text);
NeuralNetBP1.Compute(xInputVector); //.. и прогоняем ИНС
Form2.Show;
Form2.Label2.Caption := Copy(FloatToStr(NeuralNetBP1.Output[0]*100),0,4) + '%';
Вывод результата
end;
end;
procedure TForm1.RadioButton1Click(Sender: TObject);
begin
BitBtn1.Enabled := true;
end;
procedure TForm1.RadioButton2Click(Sender: TObject);
begin
BitBtn1.Enabled := true;
end;
// функция отображения хода обучения
procedure TForm1.NeuralNetBP1EpochPassed(Sender: TObject);
begin
progressbar1.Position := progressbar1.Position +1;
```

```
      If progressbar1.Position = progressbar1.max then
        begin
          Panel1.Height := 400;
          BitBtn2.Show;
          Progressbar1.Hide;
          label3.Show;
          label4.Show;
          Label5.Caption := FloatToStr(NeuralNetBP1.TeachError);
          Label5.Show;
        end;
    end;
    procedure TForm1.BitBtn2Click(Sender: TObject);
    begin
      Panel1.Hide;
      If RadioButton1.Checked then
        begin
          LabeledEdit6.EditLabel.Caption := ' Ценность информации в системе
хранения';
          LabeledEdit7.EditLabel.Caption := 'Ценность информации на
сервере Базы Данных';
        end;
      Panel2.Show;
    end;
    end.
```