Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет науки и технологий
имени академика М.Ф. Решетнева»

На правах рукописи

**Лебедев Роман Владимирович**

# МЕТОД УПРАВЛЕНИЯ РЕСУРСАМИ В КЛИЕНТ-СЕРВЕРНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ДОВЕРИЯ

Специальность 05.13.01
Системный анализ, управление и обработка информации
(космические и информационные технологии)

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель –
доктор технических наук, профессор
Мурыгин А.В.

Красноярск – 2021

ОГЛАВЛЕНИЕ

# ВВЕДЕНИЕ

**Актуальность**

Клиент-серверная архитектура является основой для большинства корпоративных информационных систем. Концепция «сервера» как центрального узла обработки информации позволяет эффективно использовать вычислительный ресурс системы за счет консолидации вычислительных мощностей и их распределения на конкурентной основе.

В реально функционирующих корпоративных информационных системах, в частности на предприятиях оборонно-промышленного комплекса (ОПК), обработка информации частично сохраняется и на стороне клиента в силу различных факторов, а с учетом их существенной географической рассредоточенности с точки зрения структуры и модели обработки информации они носят смешанный характер, принимая некоторые свойства распределенных вычислительных систем. Как следствие, такие системы имеют большие возможности горизонтального масштабирования, что выражается в преобладании прироста сегмента клиентских узлов системы перед серверным. Так ежегодный прирост числа персональных компьютеров в корпоративной локальной сети составляет около 10%, в то время как для парка серверов он не превышает 3-5%. Это обстоятельство неизбежно создает условия потенциального дефицита серверных вычислительных мощностей.

Построение эффективной системы управления вычислительными ресурсами современных клиент-серверных системах требует разработки новых методов, не зависящих от размеров системы и позволяющих автоматизировать процессы управления с учетом текущего состояния системы в целом и ее отдельных компонентов.

В современных информационных системах широко применяются методы управления на основе атрибутов или контекста. Эти подходы реализованы во многих международных стандартах, таких как IEEE 802.1p/q/v/x. Их общим недостатком является строгая детерминированность правил управления.

Изменение состояния клиентов во времени учитывается в методах управления, основанных на репутационных моделях доверия к клиенту. В таких моделях доверие формируется на основе накопленных данных о прежних состояниях клиента, но слабо учитывается его состояние в момент оценки. В этой связи актуальной является разработка методов управления вычислительными и программными ресурсами сервера на основе моделей доверия к клиентам системы, использующих данные динамических параметров клиентов в определенный момент времени.

**Степень разработанности темы исследования**

Теоретическую и методологическую основу исследования составили труды отечественных и зарубежных ученых: В.В. Подиновского, П.Н. Девянина, Р.В. Гильмутдинова, А.А. Кононова, А.А. Бешты, S.P. Mash, D.E. Denning. П.Н. Девянин внес существенный вклад в развитие моделей и методов управления доступом и информационными потоками. В.В. Подиновским проведены значительные исследования в теории измерений в части многокритериальных решений, в том числе на основе оценок качественных критериев. А.А. Бештой предложена репутационная модель доверия к наблюдаемому объекту на основе мнений клиентов системы. D.E. Denning разработал подход к оценке характеристик компьютерных систем на основе оценки их функциональных качеств, не зависящий от архитектуры и технических решений. В работе S.P. Mash формализован подход к понятию доверия и его количественной оценке.

Подходы к оценке уровня доверия также рассмотрены в работах отечественных исследователей: А.П. Дураковского, М.А. Таланова, А.С. Тимоховича, А.В. Потина, Д.С. Комина, а также иностранных: A.Arenas, B. Aziz, S. Namasudra. А.В. Потин и Д.С. Комин провели онтологический анализ предметной области понятия доверия. М.А. Таланов и А.С. Тимохович рассматривают для оценки доверия данные статистики. А.П. Дураковский описывает понятие доверия как оценку соответствия системы определенным параметрам в заданный период времени. В работах A. Arenas, B. Aziz, S. Namasudra рассматриваются методы

управления на основе реферальной репутации участников. Репутационные модели управления рассматриваются в работах D. Rosaci, G.C. Silaghi, M. Gupta, B. Yu, G. Zacharia, K. Aberer.

Исследования в области ролевых и контекстных моделей управления ведут С.В. Белим, Н.Ф. Богаченко, Е.С. Грязев, D. Zhang, Y. Zhang, W. Zeng, J. Xin, R.S. Sandhu, Z. Khan, M. Leitner, R.K. Thomas, A. Ouaddah. Проблемы управления доступом в современных клиент-серверных и распределенных системах приведены в работах В.А. Вишняков, В.И. Потапова, И.Б. Саенко, И.С. Ястребова, A. Lawall, Z.A. Zakarnain, Y. Zhang.

В современных подходах к управлению ресурсами информационных систем активно исследуются модели и методы на основе доверия, которое рассматривается в качестве меры ожидания определенных свойств и поведения от клиента системы. Подходы к доверию на основе ролевых и атрибутных моделей используются в основном в задачах строгого разграничения доступа. Существующие модели доверия на основе репутации учитывают изменения состояний системы, однако строятся, как правило, на реферальной информации о клиентах. Это накладывает дополнительные функциональные требования на компоненты системы и затрудняет их применение в существующих информационных системах предприятий, для которых проблема дефицита вычислительных и программных ресурсов стоит особенно остро.

**Цель работы**

Целью работы является повышение эффективности управления вычислительными и программными ресурсами клиент-серверных информационных систем в условиях их дефицита.

**Задачи**

В соответствии с указанной целью в работе поставлены и решены следующие задачи:

1) Аналитический обзор существующих методов и моделей управления ресурсами информационных систем различных архитектур.

2) Разработка модели доверия к клиентам информационной системы на основе контекстных данных, которая позволит получать численную оценку соответствия клиента техническим условиям выполнения целевой функции в данный момент времени.

3) Разработка метода управления ресурсами сервера в клиент-серверной информационной системе на основе доверия к клиентам, позволяющего эффективно использовать ограниченные ресурсы сервера.

4) Разработка системы управления ресурсами клиент-серверной информационной системы, позволяющей внедрять метод управления ресурсами сервера на основе оценки доверия в функционирующие клиент-серверные информационные системы без изменения их состава и режимов работы.

5) Исследование эффективности разработанного метода управления ресурсами клиент-серверной информационной системы.

**Объект исследования:** информационные системы клиент-серверной архитектуры, характеризующиеся дефицитом вычислительных или (и) программных ресурсов сервера.

**Предмет исследования:** способы управления ресурсами в клиент-серверных информационных системах, основанные на контекстной информации о клиентах.

**Методология и методы исследования**

Метод исследований строится на системном подходе и сочетании различных методов управления и обработки информации. В работе использованы методы теории множеств, теории массового обслуживания, теории измерений, теории

принятия решений, теории вероятностей, теории графов, алгебры логики. При разработке программных решений для системы управления ресурсами применялись технологии объектно-ориентированного программирования, методы логического программирования, парадигма микросервисной архитектуры, чем обеспечена возможность модификации для дальнейшего расширения функционала.

**Научная новизна**

Предмет защиты составляют следующие результаты, полученные лично автором и содержащие элементы научной новизны:

1) Предложена новая модель доверия к клиенту информационной системы на основе его сходства с эталоном, использующая в отличие от существующих подходов отношения нечеткого предпочтения для оценки важности критериев сходства, которая позволяет получить численное значение степени соответствия клиента условиям, определяемым эталоном.

2) Разработан новый метод управления вычислительными и программными ресурсами сервера в клиент-серверной информационной системе на основе оценки доверия к клиентам, который в отличие от существующих методов применяет управляющее воздействие на канал связи между клиентом и сервером и позволяет повысить эффективность использования ресурсов сервера за счет увеличения вероятности доступа к ресурсам сервера доверенных клиентов.

3) Разработана новая вероятностная модель доступа клиентов к серверу информационной системы на основе математического аппарата многоканальных систем массового обслуживания замкнутого типа с нулевой очередью и отказами, которая в отличие от известных моделей учитывает вероятность доставки запросов на обслуживание от клиентов при описании потока заявок и позволяет оценить вероятности доступа клиента к серверу с учетом изменений состояния канала связи.

**Теоретическая значимость** заключается в исследовании и развитии общего подхода к понятию доверия относительно клиентов информационных систем, который включает разработку и апробацию новой модели доверия на основе контекстной информации, позволяющей получить численное значение степени соответствия клиента заданному эталону, метода управления ресурсами клиент-серверной системы, который на основе информации о доверии к клиентам позволяет повысить эффективность использования вычислительных и программных ресурсов системы.

**Практическая значимость** заключается в разработке системы управления вычислительными и программными ресурсами клиент-серверной информационной системы, основанной на оценке доверия к клиентам, которая позволяет повысить эффективность управления ресурсами в существующих информационных системах без изменения режима их работы и технологии обработки информации. Система внедрена в ряд корпоративных информационных систем АО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва»: систему виртуализации графических вычислительных ресурсов и систему управления конкурентными лицензиями на специальное программное обеспечение. Разработанная модель доверия к клиентам используется в системе поддержки принятия решений о допуске персонала к работе со специализированным программным обеспечением.

Получено свидетельство о государственной регистрации и апробации программы «Программа анализа связей между узлами корпоративной вычислительной сети», являющейся компонентом системы управления ресурсами, которая позволяет анализировать состояние каналов связи между клиентами и сервером без имитации подключений.

Получено положительное заключение ФСТЭК России о возможности применения разработанной системы управления ресурсами в информационных системах обработки служебной информации.

**Положения, выносимые на защиту**

1) Модель доверия к клиентам в информационной системе на основе порядковой шкалы предпочтений позволяет получить численную оценку соответствия клиента заданным критериям в определенный момент времени.

– соответствует пункту 3 паспорта специальности 05.13.01: разработка критериев и моделей описания и оценки эффективности решения задач системного анализа, оптимизации, управления, принятия решений и обработки информации.

2) Метод управления ресурсами сервера в клиент-серверной информационной системе на основе оценки доверия к клиентам позволяет повысить эффективность управления дефицитными ресурсами сервера путем их распределения между клиентами, наиболее соответствующими заданным техническим условиям для выполнения целевых функций.

– соответствует пункту 4 паспорта специальности 05.13.01: разработка методов и алгоритмов решения задач системного анализа, оптимизации, управления, принятия решений и обработки информации.

3) Вероятностная модель доступа клиентов к ресурсам сервера информационной системы позволяет оценить вероятность получения доступа клиента к серверу с учетом состояний канала связи между ними.

– соответствует пункту 3 паспорта специальности 05.13.01: разработка критериев и моделей описания и оценки эффективности решения задач системного анализа, оптимизации, управления, принятия решений и обработки информации.

4) Система управления вычислительными и программными ресурсами сервера в клиент-серверной системе позволяет применять разработанный метод управления на основе оценки доверия в функционирующих клиент-серверных системах без изменения их состава и режимов работы.

– соответствует пункту 9 паспорта специальности 05.13.01: разработка проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов.

**Достоверность** результатов диссертационной работы обеспечивается корректным применением методов теории массового обслуживания, теории принятия решений, теории вероятности, строгим математическим обоснованием рассуждений, а также соответствием теоретических значений и экспериментальных данных, полученных при внедрении разработанных решений в корпоративные информационные системы. Полученные результаты согласуются с результатами исследованиях других авторов в этой области.

**Публикации**

По теме диссертационной работы опубликовано 10 работ, из которых 4 публикации в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК, 1 публикация в журнале, рецензируемом в системе Web of Science, а также получено 1 свидетельство о государственной регистрации программы для ЭВМ.

**Апробация результатов**

Результаты работы докладывались на семинарах кафедры информационно-управляющих систем и следующих конференциях:

– APITECH-II - 2020: Прикладная физика, информационные технологии и инжиниринг: II Международная конференция (25 сент.-4 окт. 2020 г., Красноярск);

– Приоритетные направления инновационной деятельности в промышленности: IX международная научная конференция (29-30 сентября 2020 г., Казань);

– Решетневские чтения: XXIV Международная научная конференция (10-13 ноября 2020 г., Красноярск);

– Актуальные вопросы проектирования автоматических космических аппаратов для фундаментальных и прикладных научных исследований: научно-техническая конференция (5-9 сентября 2017 г., Анапа);

― Решетневские чтения: XVIII Международная научная конференция, посвященная 90-летию со дня рождения генерального конструктора ракетно-космических систем академика М.Ф. Решетнева (11-14 ноября 2014 г., Красноярск);

― Решетневские чтения: XVI Международная научная конференция (7-9 ноября 2012 г., Красноярск);

― Актуальные проблемы авиации и космонавтики: VIII Всероссийская научно-практическая конференция творческой молодежи (9-14 апреля 2012 г., Красноярск);

― Решетневские чтения: XV Международная научная конференция (10-12 ноября 2011 г., Красноярск);

― Решетневские чтения: XIII Международная научная конференция (10-12 ноября 2009г., Красноярск).

**Объем и структура работы**

Диссертация состоит из введения, четырех глав, заключения, списка используемых источников (содержит 140 наименований) и 4 приложений. Общий объем диссертации составляет 146 страниц, включающих 16 таблиц (12 из которых вынесены в приложения) и 18 рисунков.

**В первой главе** рассмотрены основные типы информационных систем и их архитектур, существующие методы и модели управления ресурсами в информационных системах, наблюдаемые тенденции и актуальные проблемы, определена роль клиент-серверных систем в деятельности предприятий, также рассмотрены современные подходы к эффективному управлению ресурсами в информационных системах. Показано, что современные методы управления ресурсами в клиент-серверных системах в условиях их общего дефицита строятся на общих моделях управления доступом. Также отмечено, что традиционные подходы к управлению доступом не учитывают собственные изменения системы во времени, методы управления на основе атрибутов или контекста (ABAC, CBAC), реализованные во многих международных стандартах, таких как IEEE

802.1p/q/v/x и пр., имеют общий существенный недостаток: строгую детерминированность правил управления. На практике владелец системы чаще опирается на некоторую сводную, совокупную информацию о клиенте, принимая решение о разрешении его доступа к ресурсу сервера. Оценка доверия к клиенту используется в методах управления на основе гибких или нечетких правил, при этом применяются репутационные модели доверия, основанные на реферальной информации о клиентах. Представленные на рынке решения по управлению ресурсами в современных корпоративных информационных системах в основном производятся за рубежом, весьма дорогостоящие и сложные как на этапе внедрения, так и при их эксплуатации, что делает актуальными исследования в области создания новых методов управления на основе доверия, легко интегрируемых в существующие клиент-серверные информационные системы.

Клиент-серверная информационная система рассматривается как совокупность ограниченных ресурсов, сосредоточенных на сервере, их потребителей (клиентов), а также программно-технических средств и систем, обеспечивающих эксплуатацию этих ресурсов, управление доступом к ним и объединенных в вычислительную сеть. Под сервером понимают оконечный узел (совокупность узлов) сети, выполняющий обработку запросов на доступ к его ресурсам, доступ предоставляется на конкурентной основе. Под клиентом понимается оконечный узел, использующий ресурс сервера для выполнения своих функций, клиенты являются субъектами доступа в клиент-серверной информационной системе. В составе вычислительной сети также рассматривается сетевое оборудование, под которым понимаются программно-технические средства, обеспечивающие связь оконечных узлов сети. Технические ресурсы системы, используемые непосредственно для выполнения ее целевых функций, называют вычислительными ресурсами системы. Специальное программное обеспечение, применение которого связано с техническими или организационными (лицензионными) ограничениями называют программными ресурсами системы. Вычислительные и программные ресурсы являются ограниченными.

Показано, что основной проблемой современных корпоративных информационных систем, построенных на основе архитектуры «клиент-сервер», является сложность администрирования, мониторинга и сбора статистики, технического обслуживания удаленных узлов, аппаратная и программная гетерогенность, что осложняет (или даже исключает) возможность применения стандартных контекстных моделей управления ресурсами. Показана целесообразность подхода к управлению ресурсами на основе рейтинговых моделей доступа и целесообразность разработки методов управления ресурсами на основе оценки доверия к клиентам как меры его сходства с заданным эталоном в определенный момент времени.

**Вторая глава** посвящена построению модели доверия к клиентам и основанному на этой модели методу управления ограниченными ресурсами в клиент-серверной системе.

Под доверием к клиенту понимается численная мера его соответствия заданному эталону, который определяется владельцем информационной системы через набор проверяемых параметров – критериев доверия. Модель строится на основе нормированной порядковой шкалы оценки соответствия клиента некоторому эталону, заданному владельцем ресурса по ряду формализованных параметром – критериев доверия. Сформулированы ключевые принципы для критериев доверия, они включают: объективность (инвариантность способа интерпретации критерия относительно выбора клиента), документированность (определенность выбора формата представления и хранения проверяемых сведений), универсальность (возможность проверки критерия для любого клиента в системе).

К критериям доверия предложено относить сведения о программно-техническом составе хоста (компьютера), его функциях, данных об активности и соответствию заданным техническим политикам работы. На множестве всех критериев экспертным методом задается отношение нечеткого предпочтения по

степени их важности, каждому критерию устанавливается нормированный вес, который в дальнейшем учитывается в оценке доверия к клиенту.

Метод управления доступом на основе оценки доверия основан на управляемом воздействии на канал связи между клиентом и сервером системы. Метод предполагает выбор специального порогового значения оценки доверия, по которому клиенты с меньшим значением доверия будут отключаться от сервера на уровне канала коммуникации, что позволяет внедрять данный метод управления в существующие клиент-серверные системы без изменения из структуры и режимов работы. Пороговое значение определяется как функция от значений шкалы весов критериев доверия, что позволяет изменять перечень критериев доверия и пересматривать их весовые коэффициенты в процессе применения метода.

**В третье главе** описана система управления вычислительными и программными ресурсами сервера в клиент-серверной системе, реализующая разработанный метод управления на основе оценки доверия, обозначены необходимые технические и технологические условия для применения разработанного метода в функционирующей информационной инфраструктуре предприятия, такие как система сбора и обработки исходной информации для оценки доверия, система анализа сетевой топологии, позволяющая моделировать структуру вычислительной сети предприятия и взаимосвязи ее узлов для проверки исполнения предписаний метода.

В главе сформулированы принципы и механизмы получения информации о компьютерах корпоративной информационной инфраструктуры для последующей оценки доверия, а также логическая модель анализа топологии сети на основе конфигурационных данных коммутационных устройств, позволяющая проверять состояние канала связи между различными узлами вычислительной сети. Представлена система управления доступом в клиент-серверной системе на основе оценки доверия. Механизм управления в модели представлен как надстройка над некоторой существующей инфраструктурой клиент-серверной системы, которая влияет на текущие настройки соответствующих сетевых устройств, реализуя тем

самым механизм управления на уровне сетевом уровне стека протоколов TCP/IP без изменения состояния и режимов работы сервера и клиентов исходной системы.

**В четвертой главе** проведено исследование эффективности разработанного метода управления ресурсами в клиент-серверной системе. Показателем эффективности в работе принято считать вероятность доступа доверенного клиента к серверу в стационарном режиме работы системы.

Для исследования эффективности метода предложена вероятностная модель доступа клиентов к серверу системы с использованием математического аппарата теории массового обслуживания как система массового обслуживания замкнутого типа с нулевой очередью и отказами. Модель учитывает вероятность доставки заявок на обслуживание при описании потока заявок. Критерием эффективности выбрана оценка вероятности обработки сервером очередной заявки от доверенного клиента. Оценка эффективности метода выполняется путем сравнения значений оценки вероятности доступа клиента для системы в устоявшемся состоянии в обычном режиме работы и в режиме с ограничением доступа к серверу со стороны недоверенных клиентов. Проводится сравнение с аналогичными методами управления ресурсами на основе ролевых и атрибутных моделей доступа. Результаты оценки эффективности метода приведены в виде графиков и таблиц.

Поскольку в модели рассматриваются СМО без очереди для измерения доступного ресурса сервера используется количество каналов системы. Помимо стандартных параметров: количество клиентов, количество каналов и коэффициент загрузки – на вход модели подается значение порога доверия, а также набор критериев доверия с заданной шкалой весов. Коэффициент загрузки определяется через отношение среднего интервала между поступлением заявок на доступ клиента к серверу и среднего времени работы с сервером после получения доступа.

В силу того, что ресурс сервера и коэффициент загрузки системы в среднем являются постоянными величинами, то на оценку вероятности готовности системы влияет, главным образом, число клиентов и величина порога доверия. Рассмотрена функция зависимости оценки вероятности готовности системы от общего числа

клиентов системы и функция отношения оценок вероятностей в обычном режиме и режиме с использованием оценки доверия для разных значений порога доверия. Построены графики этих функций, которые наглядно демонстрируют изменение оценки вероятности обслуживания заявок, поступающих от доверенных клиентов.

В **заключении** приводятся основные результаты и выводы, полученные автором в ходе работы.

В **приложениях** представлены: свидетельство о регистрации программы для ЭВМ, справка о внедрении результатов диссертационной работы, исходные данные вычисления весовых коэффициентов критериев доверия в виде опросных листов экспертов, а также табличные данные расчета функции оценки доверия для выборки компьютеров предприятия.

# Глава 1. Существующие методы и модели управления ресурсами в клиент-серверных информационных системах

## 1.1 Классификация информационных систем

### 1.1.1 Понятие информационной системы

Понятие информационная система (ИС) имеет несколько значений в зависимости от контекста его применения. В [82] различают трактовку понятия ИС в широком и узком смысле. Понятие в широком смысле ИС раскрывает общие онтологические составляющие структуры понятия. ИС в этом контексте представляется как совокупность информации, информационных технологий, осуществляющих ее обработку, технических и программных средств для обеспечения потребителя (как правило, человека) ее функций.

В широком представлении о понятии ИС приведено ее определение Федеральном законе [68]: «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств». Как видно, в понятие ИС включены базы данных как отдельный функциональных компонент (об этом далее) и исключен компонент «персонал». Автор считает такое изменение закономерным и связанным с ростом степени автоматизации информационных технологий и сокращением роли человека и как основного потребителя функций, и как технологического звена в работе современных ИС.

Одно из наиболее широких определений ИС дал М.Р. Когаловский [35]: «информационной системой называется комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный персонал и обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей». Он также отмечает, что общепринятого понятия ИС не существует.

В международных и отечественных стандартах даны следующие определения понятия ИС:

– ГОСТ 33707-2016 (ISO/IEC 2382:2015) [46]: «Система, организующая обработку информации о предметной области и ее хранение»;

– ГОСТ РВ 51987 [51]: «автоматизированная система, результатом функционирования которой является представление выходной информации для последующего использования».

Информационной системой, по существу, называют определенное и конкретизированное подмножество компонентов ИС из широкого представления: базы данных, системы управления ими (СУБД), общесистемное и специальное программное обеспечение (ОПО и СПО), техническое обеспечение. ИС в узком смысле рассматривают [19] как «программно-аппаратную систему, предназначенную для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающую, в соответствии с заложенной в неё логикой обработки, возможность получения, модификации и хранения информации».

Исходя из этих соображений можно заключить, что основной задачей ИС является удовлетворение вполне конкретных информационных потребностей в рамках столь же вполне конкретной предметной области.

Современные информационные системы не представляются в отрыве от баз данных и СУБД, поэтому термин «информационная система» на практике сливается по смыслу с термином «система баз данных».

Информационные системы, функционирующие в рамках предприятия, принято называть корпоративными, их задача состоит в удовлетворении существующих информационных потребностей персонала, служб, производственных и бизнес-процессов.

### 1.1.2 Ресурсы информационных систем

Информационные системы используют различные категории ресурсов: технические средства, ОПО, СПО, информационные, лингвистические и

человеческие ресурсы, а также ресурсы физического характера (помещения, энергоснабжение, инженерная инфраструктура и т.д.).

Информационные ресурсы системы являются главным компонентом предметной области, которую поддерживает система. Выделяют два вида информационных ресурсов: данные (непосредственно используются конечными пользователями системы) и метаданные (используются компонентами системы в процессе ее работы).

Лингвистические ресурсы ИС служат для представления информационных ресурсов всех видов в определенных форматах для обеспечения интерфейса взаимодействия конечного пользователя с системой и для внутреннего транзита метаданных между компонентами системы. Следует отметить, что под конечным пользователем системы нужно понимать не только персонал системы, но и программное обеспечение, использующее информационные и лингвистические ресурсы системы для выполнения собственных задач.

Технические ресурсы, такие как аппаратные платформы (персональные компьютеры, серверы и пр.), коммуникационное (сетевое) оборудование обеспечивают обработку, хранение и передачу данных, взаимодействие компонентов ИС. Их состав, характеристики и структура определяют качественные показатели информационной системы, связанные со скоростью и объемом обрабатываемой (хранимой) информации.

В современных подходах к организации информационных систем, таких как IaaS, PaaS, SaaS, технические ресурсы могут также рассматриваться как предоставляемая услуга [105, 106]. Технические ресурсы ИС ограничены характеристиками обеспечивающих их технических средств.

Общесистемное программное обеспечение включает операционные системы (ОС) для управления и работы аппаратных средств, различные программное оболочки, служебные программы (драйверы) и т.д. В кластерных информационных системах системное программное обеспечение осуществляет также взаимосвязь технических компонентов ИС. К данной категории ресурсов относят также типовое прикладное программное обеспечение, оно, как правило, определяется под

конкретный класс задач ИС, к этой категории ресурсов относят СУБД, программное обеспечение серверных узлов и т.д. Ресурс ОС и ОПО также является ограниченным, пределы его использования определяются архитектурными особенностями аппаратного обеспечения (например, разрядность процессора), функциональными ограничениями, заложенными на этапе разработки ПО (счетчик потоков, размеры буферов памяти, типы программных переменных и пр.), или связанными с условиями использования данного ПО конкретным потребителем (лицензионные ограничения).

Технические ресурсы системы, используемые непосредственно для выполнения целевых функций (решения производственной задачи, обработки информации и пр.) называют вычислительными ресурсами системы. Специальное программное обеспечение, применение которого связано с техническими или организационными (лицензионными) ограничениями называют программными ресурсами системы. Вычислительные и программные ресурсы являются ограниченными.

### 1.1.3 Классификация информационных систем

Существуют различные подходы к классификации информационных систем [10, 18, 20, 28, 36, 48, 86].

Можно выделить следующие типы классификации ИС.

– По функциональному признаку (назначению): системы управления, вычислительные ИС (в т.ч. системы автоматизированного проектирования и разработки (САПР), поисково-справочные, системы поддержки принятия решений (СПР), информационные обучающие системы;

– По области применения: производственные, маркетинговые, финансовые, кадровые, информационные системы в экономике, в образовании, в научных исследованиях и т.д.;

– По степени автоматизации: автоматические (выполняют все операции без участия человека), автоматизированные (предполагают участие в процессе обработки информации и человека, и технических средств, причем главная роль

отводится компьютеру, являются наиболее близким типом к понятию ИС); ручные ИС (характеризуются отсутствием современных технических средств переработки информации и выполнением всех операций человеком).

— По степени физической (территориальной) разобщенности: совместные (сосредоточенные, локальные, автономные); разобщенные (распределенные, сетевые);

— По архитектуре ИС: с выделенным центром (файл-серверная, клиент-серверная, многоуровневая); без выделенного центра (распределенные системы, грид-системы, многоагентные системы).


Рисунок 1 – Общая классификация информационных систем

Общая схема классификации ИС по назначению, функциональным особенностям и характеру обрабатываемой информации представлена

на рисунке 1. Классификация ИС по типу архитектуры наглядно представлена на рисунке 2.

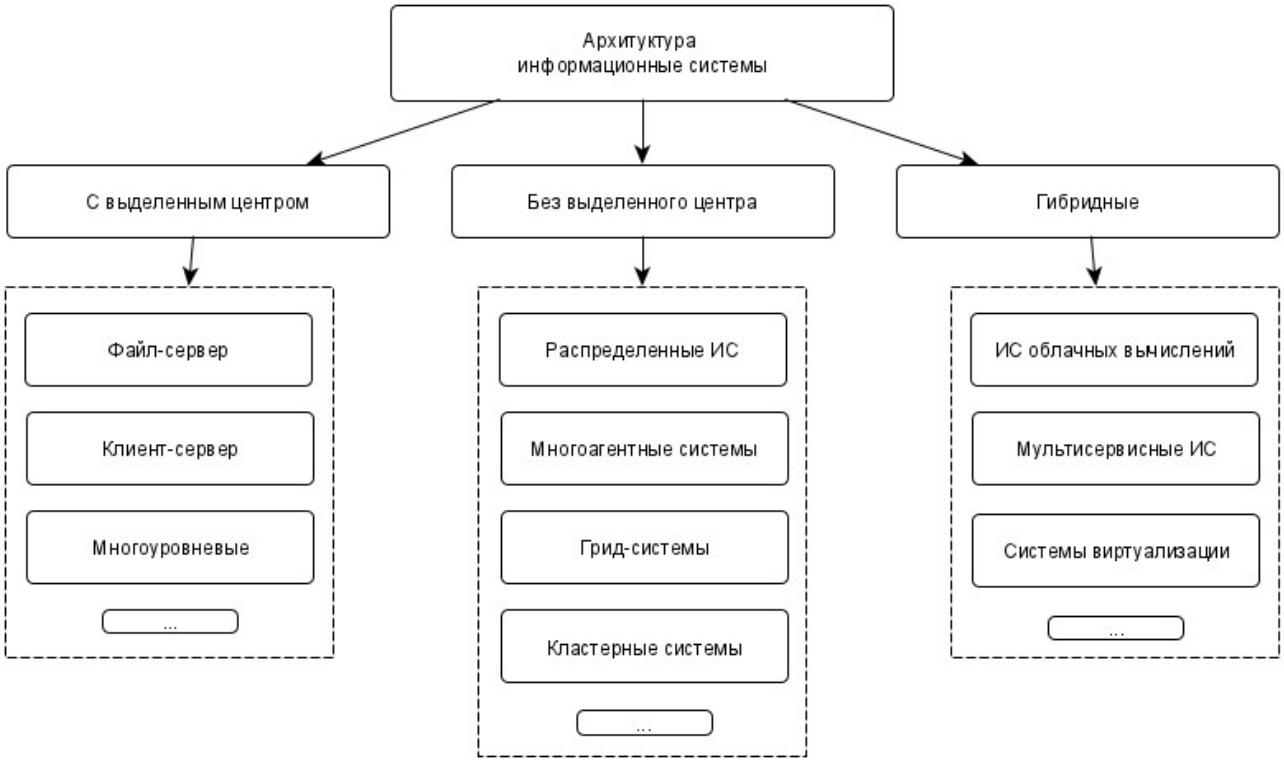



Рисунок 2 – Классификация ИС по типу архитектуры

## 1.2 Клиент-серверные информационные системы

Клиент-серверная архитектура является основой для большинства корпоративных информационных систем [30]. Концепция «сервера» как центрального узла обработки информации позволяет эффективно использовать вычислительный ресурс системы за счет консолидации вычислительных мощностей и их распределения на конкурентной основе, что обеспечивает комплексный учет условий функционирования вычислительных систем и синтез вычислительной среды [2, 80]. Клиент-серверные архитектуры являются основными для управляющих, поисково-справочных систем, САПР, СПР и иных ИС. Системы распределенных архитектур используются, в основном, в высоконагруженных вычислительных системах, а в современных информационных системах, таких как системы виртуализации, облачные сервисы и мультисервисные сети, используется смешанная архитектура.

### 1.2.1 Клиент-серверная и распределенная архитектуры

Структура типа «точка-точка» является тривиальным случаем как для архитектуры клиент-сервер, так и для архитектур ИС распределенного типа. Принципиальная разница состоит в разделении ролей между ее узлами. В исследованиях [14, 72, 73] приводятся примеры моделей распределенных систем на базе локальной вычислительной сети (ЛВС) и трех и двухуровневой клиент-серверной архитектуры с однократными параллельными запросами. Модели используются для вычисления интегральных показателей распределённой ИС. Как правило, в подобных исследованиях применяется математических аппарат теории систем массового обслуживания. В работе [112] предложено программное решение симуляции клиент-серверной архитектуры на базе распределенной программной инфраструктуры.

### 1.2.2 Проблемы современных клиент-серверных систем

В корпоративных информационных системах, в частности на предприятиях ОПК, обработка информации, как правило, частично сохраняется на стороне клиента. Это может быть обусловлено различными обстоятельствами: сложностью организации технологического процесса обработки информации, историческими или нормативными факторами. С учетом их существенной географической рассредоточенности с точки зрения структуры и модели обработки информации корпоративные системы носят смешанный характер, принимая некоторые свойства распределенных вычислительных систем [12, 49, 72, 81]. Как следствие, такие системы имеют большие возможности горизонтального масштабирования, что выражается в преобладании прироста сегмента клиентских узлов системы перед серверным. При этом подобные системы сохраняют функциональную архитектуру типа «клиент-сервер», которая является основной для большинства корпоративных и отраслевых информационных систем [67].

Так ежегодный прирост автоматизированных рабочих мест в корпоративной локальной сети составляет около 10% с учетом модернизации, в то время как

прирост парка серверов не превышает 3-5%. Это обстоятельство неизбежно создает условия потенциального дефицита серверных вычислительных мощностей, что требует разработки новых методов управления ими.

В работе [55] рассмотрена модель локальной вычислительной сети (ЛВС) геоинформационной системы, организованной как клиент-серверная система, учитывающей вклад и степень влияния на общую производительность системы используемых в ее составе компьютеров (ПЭВМ) неосновного назначения (функции обеспечения и подобные). В статье отмечается общая тенденция к росту потребности в обработке данных, увеличению объемов данных и их разнообразия. Как пример приводится статистика роста данных геодезической, геофизической, метеорологической разведки на фоне общего потока данных систем космического мониторинга; эти данные также необходимо хранить и обрабатывать, что усиливает необходимость наращивания серверных мощностей для обеспечения надежного функционирования систем. Противоречия, возникшие между ростом объема данных и возможностями владельцев ИС по их обработке, обусловливают необходимость разработки новых подходов и механизмов к управлению ограниченными ресурсами сервера.

Проблема дефицита вычислительных ресурсов также освещена в работе M. Alian [88], автор исследует параметры энергопотребления сервера при лавинном росте числа обрабатываемых запросов. В работе В.И. Потапова [123] исследованы различные характеристики надежности информационных систем типа «клиент-сервер» при высокой нагрузке на компоненты системы, описаны математические модели поведения системы на основе Марковских процессов. В работе M. Lim [117] предлагается решение оптимизации расходования вычислительных ресурсов сервера при операциях файлообмена.

Построение эффективной системы управления доступом к вычислительным ресурсам современных гетерогенных, географически распределенных клиент-серверных информационных систем требует разработки новых моделей, методов, не зависящих от размеров системы и позволяющих автоматизировать процессы

управления и учитывать текущее состояние системы в целом и ее отдельных компонентов.

## 1.3 Эффективное управление ресурсами в информационных системах

Проблема эффективного использования вычислительных и программных ресурсов активно исследуется в отношении современных информационных систем различных типов и архитектур. Как было показано в п. 1.2.2, для клиент-серверных систем характерно заметное превышение (приблизительно в 2 раза) темпов горизонтального роста клиентского сегмента в сравнении с серверным. Аналогичные показатели можно наблюдать для систем иных архитектур, в которых по функциональному или структурному признаку так же можно выделить серверный и клиентский сегменты, что очевидно связано с удешевлением производства компьютерной техники и расширением областей ее применения.

Одним из наиболее распространенных типов информационных систем, где актуальна задача эффективного управления вычислительными ресурсами, являются облачные системы на основе технологий виртуализации. Такие системы относятся к гибридному типу архитектуры, сочетая функциональные свойства сервера в клиент-серверной архитектуре уровню системы виртуализации.

В работе М.С. Кавериной [33] рассматривается задача эффективного управления виртуальными ресурсами в облачных информационных системах в условиях неопределенности количества запросов от клиентов и производительности выдаваемых ресурсов. Для оценки эффективности стратегии принятия решений применяется стохастическая событийная модель. В статьях А.И. Мышкина [44, 45] рассматривается процесс подготовки математических моделей вычислительных систем с виртуализацией, в качестве математического аппарата для расчетов используются замкнутые системы массового обслуживания. Автором предложены модели для анализа различных систем виртуализации, эффективность управления ресурсами строится на разделении выполнения задач по степени важности и классификации групп ресурсов для их выполнения. В работах отмечено, что существующие модели вычислительных систем не

позволяют определить наиболее эффективный вариант начального распределения ресурсов и провести его оптимизацию под конкретную задачу в процессе работы системы. Основную часть нужной информации для принятия решения автор предлагает формировать на основе статистики в ходе работы системы.

В работе М.М. Бутаева и А.А. Папко [11] рассмотрена проблема выбора исходных параметров моделей компьютерных систем, ориентированных на различные классы задач, адаптации теории систем массового обслуживания к исследованию и расчету этих моделей для эффективного управления ресурсами и рабочей нагрузкой виртуальных серверов. Авторы предлагают использовать для расчета моделей типизированные по классам задач профили политик управления ресурсами в виде конфигураций программного окружения объектов, файлов настроек, которыми определяются критерии оптимизации ресурсов сервера. Таким образом, в расчете модели используется информация, полученная с применением схемы принятия решений, заданной самим исследователем. Критерием эффективности управления ресурсами в работе считается вероятность простоя оборудования.

В работе N.B. Kothari [111] рассмотрена проблема дефицита вычислительных ресурсов серверов для облачных архитектур. Автор использует понятие нагрузки неопределенного типа (англ. the uncertain load appearance) для описания условий исчерпания ресурсов сервера в общей инфраструктуре при использовании стандартных методов распределения нагрузки. Такие условия возникают при большом росте числа потребителей ресурсов, любой из серверов может в любой момент столкнуться с проблемой доступности ресурсов из-за большого количества запросов. Для отслеживания появления неопределенной загрузки автор предлагает метод двухэтапной оптимизации распределения ресурсов на основе шаблонов нагрузки. Автор сравнивает алгоритмы линейной регрессии и ACO, для сравнения эффективности используется оценка среднего времени ожидания клиентов доступа к запрошенному ресурсу сервера.

В работе D. Kontoudis и P. Fouliras [110] рассмотрена проблема эффективного распределения ресурсов в клиент-серверных системах с виртуализацией, рабочие

нагрузки которых представляют собой колеблющуюся потребность в ресурсах. Отмечено, что неэффективное управление ресурсами, необходимыми для бесперебойной работы инфраструктуры, может привести к препятствиям в успешном предоставлении услуг, для оценки эффективности рассматривается коэффициент использования ресурсов. Авторы описывают метод динамического управления ресурсами серверов информационной системы на основе статистических моделей спроса. Как отмечают авторы, предлагаемый механизм обеспечивает оперативное управление ресурсом процессора и объемом памяти сервера, выделяемым под задачу посредством анализа в реальном времени наблюдаемой производительности.

P. Sharma [131] рассматривает подход к эффективному распределению вычислительных ресурсов крупных гибридных клиент-серверных систем уровня коммерческого центра обработки данных (ЦОД), за единицу ресурса предлагается брать отдельный физический узел серверной инфраструктуры. Проблема управления ресурсами в таком масштабе состоит в снижении общей производительности выданного под задачу ресурса в силу эксплуатационных издержек на техническом уровне. В качестве решения предлагается метод формирования групп (портфелей) серверов (в статье «серверный портфель», англ. «server portfolio») на основе финансовых моделей. Для оценки эффективности рассматривается коэффициент загрузки оборудования ЦОД.

К.С. Захаровым [29] рассмотрены методы управления вычислительными ресурсами ЦОД на уровне распределения виртуальных машин между гипервизорами системы виртуализации, переводя тем самым вычислительные ресурсы в категорию программных. В качестве критерия эффективности рассматривается коэффициент использования серверного оборудования. Схожий подход наблюдается в исследованиях N. Wang и B. Varghese [137], направленных на изучение возможности использования вычислительных ресурсов оборудования каналов связи.

Таким образом можно заключить, что современные исследования методов эффективного управления дефицитными программными и вычислительными

ресурсами клиент-серверных систем направлены на повышение коэффициента использования этих ресурсов. То есть изначально подразумевается, что потенциально имеющегося объема ресурсов системы хватает для удовлетворения потребностей пользователей системы, дефицит создается неоптимальным распределением, при котором может возникать их неоправданный простой или дефицит локального характера (для отдельно взятых запросов клиентов).

В данной работе рассматривается проблема абсолютного дефицита ресурсов сервера системы, при котором доступного объема ресурсов недостаточно для удовлетворения потребностей пользователя. В этой связи целесообразно рассматривать подходы к повышению эффективности управления ресурсами на основе оценки их использования клиентами системы. С этой точки зрения управление ресурсами может рассматриваться с позиции управления доступом клиента к ресурсу сервера на основе различных моделей избирательного доступа. Для оценки эффективности методов могут применяться вероятностные показатели получения клиентом запрошенного ресурса.

### 1.3.1 Управление ресурсами на основе моделей доступа

Управление доступом в информационных системах строится на формальных моделях, включает в себя процедуры идентификации субъекта доступа (клиента), подтверждение его идентичности (аутентификации) и согласование запроса на доступ со стороны владельца объекта доступа или третьей стороны [50, 51, 52]. Существенный вклад в развитие моделей и методов управления доступом и информационными потоками внес П.Н. Девянин, им сформирован подробный словарь терминов в области управления доступом, описаны формальные модели управления доступом и управления потоками информации [23, 24, 25, 26]. На его трудах, в частности, строится методологическая основа данной диссертационной работы.

Среди классических подходов к управлению доступом выделяют следующие основные модели:

– Избирательное (дискреционное) управление (англ. Discretionary Access Control, DAC) [119]: управление доступом субъектов к объектам на основе списков или матриц доступа;

– Мандатное управление (англ. Mandatory Access Control, MAC) [119, 120]: разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче разрешений на доступ для субъектов имеющих соответствующий мандат;

– Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) [97, 129]: правила доступа субъектов к объектам группируются с учётом специфики их применения, образуя роли, является развитием метода избирательного управления доступом;

– Разграничение доступа на основе атрибутов (англ. Attribute-Based Access Control, ABAC) [38, 41, 53]: метод управления доступом, основанный на анализе правил для атрибутов объектов и субъектов, возможных операций с ними и окружения, соответствующего запросу. Системы управления доступом на основе атрибутов обеспечивают мандатное и избирательное управление доступом;

– Управление доступом на основе контекста (англ. Context-based access control, CBAC): метод управления доступом, при котором решение о доступе принимается на основе контекста собранной информации о субъекте, запрошенной операции в условиях текущего окружения [138].

Указанные выше методы управления доступом считаются основными и наиболее распространенными. В некоторых работах выделяют также:

– Управление доступом на основе графов (англ. Graph-Based Access Control, GBAC) [114, 113]: это декларативный способ определения прав доступа на основе специального вида семантического графа;

– Управление доступом на основе решетчатой модели (англ. Lattice-Based Access Control, LBAC) [130]: гибридная модель доступа, сочетающая дискреционный и мандатный подходы и учитывающая все возможные комбинации взаимодействия субъектов и объектов;

– Управление доступом на основе организации (англ. Organization-Based Access Control, OrBAC) [89]: метод управления доступом, основанный на ролевой модели, адаптированный под структуру организации;

– Управление доступом на основе задач (англ. Task-Based Access Control, TBAC): ещё одно направление развития ролевого подхода [38].

Исследования в области моделей и методов управления доступом ведутся весьма активно. Целый ряд работ посвящён оптимизации иерархических структур ролевой модели [9, 93, 139]. Также ведутся разработки по совмещению нескольких классических подходов в одной политике разграничения доступа [56, 94], в частности в работах С.В. Белима [4, 5, 6] используется аппарат теории графов для совмещения ролевой и мандатной политик управления доступом.

Исследования Y. Zhang, G. Zhang [140] посвящены разработке моделей управления доступом для виртуальных и облачных сервисов, в работе отмечена как основная проблема ограниченность применения стандартных методов управления доступом на основе ролей, для ее решения применяется атрибутный подход. В статье И. Саенко [70] описана методика поэтапного разграничения доступа к информационным ресурсам в облачных инфраструктурах, в качестве основы используется ролевая модель доступа. Вопросы управления доступом в облачных ИС также рассмотрены в [13], работа посвящена изучению моделей управления доступом на основе многофакторной аутентификации (англ. Capability-Based Access Control, CpBAC – управление доступом на основе возможностей). Также задаче управления доступом в облачных сервисах посвящены работы [21, 128].

Работы Z. Khan, J.J. Lehtomaki [108] направлены на разработку моделей управления доступом в технологиях интернета вещей (IoT). Предлагаемые решения основаны на данных геолокации (Zone-Based Access Control, ZBAC). A. Ouaddah, A.A. Elkalam в [122] в рамках решения проблемы авторизации и аутентификации в IoT предлагают модель децентрализованного управления доступом на основе технологии блокчейн. Авторы отмечают, что выбранные подходы связаны главным образом с ограниченностью вычислительного ресурса клиентов в сетях интернета вещей. Схожей проблемой занимались Д. Банков и Е.

Хоров [91] в контексте доступа маломощных устройств к беспроводным сетям по протоколам LoRaWAN, в качестве решения также предлагается атрибутная модель. В работе S. Gong, L. Gao, J. Xu [99] рассматриваются подходы на основе гибридных моделей доступа к организации доступа типа точка-точка.

В работе С.В. Усова [78] рассмотрена иерархическая ролевая модель доступа на основе объектно-ориентированных дискреционных моделей, приведено сравнение со стандартной ролевой моделью.

Статья Е.С. Грязнова [22] посвящена вопросам управления доступом с использованием технологий виртуализации, рассмотрены системы управления доступом, основные программные модули которых работают на уровне ядра операционной системы, описан вариант принципиального усиления систем разграничения доступа за счет использования возможностей технологии виртуализации для имитации многоуровневой модели.

В современных информационных системах широко применяются методы управления на основе атрибутов или контекста (ABAC, CBAC). Эти подходы реализованы во многих международных стандартах и протоколах [101, 102, 103, 104], на рынке представлены комплексные решения от ведущих производителей (Cisco, HP и пр.) [57, 76, 124].

Общим недостатком данных подходов к управлению доступом является строгая детерминированность правил управления. На практике владелец системы чаще опирается на некоторую совокупную информацию о клиенте, принимая решение о разрешении его доступа к ресурсу сервера. В этой связи актуальной является задача разработки методов автоматизированного управления вычислительным ресурсом сервера на основе динамических характеристик клиентов. Готовые коммерческие решения, как правило, весьма дорогостоящи, сложны как на этапах внедрения, так и при эксплуатации, а также требовательны к программно-техническому оснащению исходной инфраструктуры.

В работе А. Баранова [1] рассмотрена проблема управления доступом в микросервисных архитектурах, приведен перечень архитектурных подходов для

реализации управления доступом в микросервисных приложениях, описаны возможные условия его применения, достоинства и недостатки.

А.А. Прощаева в [65] рассматривает влияние ролевой модели доступа на производительность информационной системы, в качестве критерия эффективности работы рассматривается скорость обработки запросов, в результате автор отмечает, что при сложной организации ролевой модели наблюдается существенное снижение производительности. Данное исследование показывает, что реализация сложных моделей управления доступом требует использования вычислительных ресурсов сервера системы.

### 1.3.2 Управления доступом на основе доверия

Понятие доверия имеет множество значений, А. В. Потин [113] проводит онтологический анализ предметной области доверия в контексте гарантий соответствия требованиям, дает обоснование применения понятий «требования гарантий» и «требования доверия», описывает онтологическую модель понятия «оценки гарантий». В работе S.P. Mash [33] формализован подход к понятию доверия и его количественной оценке.

Понятие доверия тесно связано с понятием репутации, во многих источниках эти понятия отождествляются. A. Arenas в [90] отмечает, что репутация, так же как и доверие, есть общее понятие, широко используемое во всех аспектах знаний. Репутация рассматривается как мера доверия или недоверия чему-либо и может основываться на опыте прошлого (прямое доверие) или на собранной реферальной информации (косвенное доверие).

Модели управления, основанные на репутации (репутационные модели), применяются в технологиях QoS [100] и различных архитектурах типа «точка-точка» [98]. Подход к управлению доступом на основе доверия в многоагентных и распределенных системах предложен D. Rosaci в [127]. В таких системах, как правило, оценка доверия проводится для всех взаимодействующих сторон. В статье P.K. Behera [92] рассматривается модель взаимного доверия пользователя и ресурса. Значение доверия к пользователю оценивается на основе параметров

поведения, а значение доверия к ресурсам – на основе оценки соответствия требованиям качества обслуживания. Эффективность модели проводится в сравнении с аналогичными решениями на основе технологий QoS.

Активно исследуются подходы к управлению доступом на основе доверия в отношении клиент-сервисных архитектур, в частности, на основе облачных технологий. В работе A. Kesarwani [107] предложена модель субъективного доверия, основанная на обработке данных о поведении пользователя в прошлом. Модель использует нечеткие значения показателей оценки доверия, атрибутами оценки доверия к ресурсу считаются рабочая нагрузка, время ответа, доступность и пр., а к пользователю, соответственно, статистика отношения неверных, поддельных и неавторизованных запросов к их общему числу. Модель доверия используется для адаптации нечетких параметров для применения в классическом атрибутном подходе к управлению доступом. На данной модели основан метод машинного обучения, прогнозирующий оценку доверия к пользователю, представленный P.M. Khilar в работе [109]. Метод использует статистику поведения пользователя и предложен как средство распознавания модулей автоматизации на стороне пользователя.

Над разработкой моделей доверия на основе реферальных данных активно работают A. Singh, K. Chatterjee [132, 133]. Проблема доверия рассматривается в рамках исследования управления доступом в открытых информационных системах клиент-серверного типа на примере информационных систем здравоохранения. Применяется подход взаимного доверия как параметра суждения при управлении доступом заинтересованных сторон, степень доверия оценивается по методике бета-распределения. Авторами разработан набор правил для управления доступом к данным, которое динамически изменяется вместе с уровнем доверия взаимодействующих сторон. Также подход к управлению доступом на основе доверия в открытых информационных системах рассмотрены в работе G.S. Tejas [136], для оценки доверия предлагается использовать показатели соответствия требованиям различных политик контроля доступа, решение о доступе принимается с использованием методов теории игр.

В работах S. Namasudra [121] и K. Riad [126] описаны схожие концепции доступа к облачным сервисам на основе рейтинга пользователей, составленного по отзывам других пользователей системы. K. Riad также приводит данные исследования эффективности применения концепции на практике на основе времени принятия решения о доступе. Аналогичный подход к оценке доверия описан в работе А.А. Бешты [7]: предложена методика оценки доверия к наблюдаемому объекту и разработана доверительная модель объекта, которая определяется на основе поданных в отношении него положительных и отрицательных голосов с учетом их важности.

Также понятие доверия применяется в контексте свойств безопасности информационных систем и их компонентов. Так в статье А. П. Дураковского [27] дается определение понятию доверия через основные свойства информации с точки зрения ее безопасности (целостности, конфиденциальности, доступности) и интегральные показатели ее защищенности, в том числе от воздействия случайных факторов; данные свойства рассматриваются в заданных временных границах. Показатель задается для всех объектов ИС и определяется путем оценки степени выполнения требований политики безопасности, при этом ведется оценка значимости отдельных требований политики. Стоит отметить, что предлагаемый индекс не дает количественного представления о степени выполнения требований, также методика не учитывает взаимосвязи между требованиями, участвующими в формировании индекса. Там же сформулирован критерий достижения доверия как показатель соответствия информационной системой требования к уровню защищенности (показатель доверия задается для всей ИС целиком).

Одной из классических считается концепция, предложенная D.E. Denning [96], по оценке защищенности компьютерных систем на основе оценки их функциональных качеств, без наложения каких-либо ограничений на выбор архитектуры и технических решений. Такой подход может быть применить для оценки доверия в отношении других свойств объектов системы, в том числе требований качества. Аналогичный подход применен в современных исследованиях, например, в статье V. Takalkar [135] для оценки доверия

пользователей социальных сетей, за основу критериев доверия принимаются наборы ролей, соответствующих пользователю.

В работе М.А. Таланова [75] в качестве основы для создания формулы доверия используется статистика, социологии и специфика бизнеса. Формула доверия рассматривается в общем виде, не позволяющем оценить уровень доверия, на который влияют количество и распределение событий на множестве групп риска и уровней критичности.

## 1.4 Выводы

В главе рассмотрены основные типы информационных систем по функциональному и архитектурному признаку. Установлено, что клиент-серверная архитектура лежит в основе большинства информационных систем предприятия (включая варианты смешанной архитектуры). Так же рассмотрены научные исследования в области развития клиент-серверных систем, показана актуальность проблемы дефицита вычислительных ресурсов, характерная для клиент-серверных и гибридных архитектур, реализующих технологии SaaS, IaaS, PaaS (доступ к программному обеспечению и вычислительным мощностям в качестве услуги).

Рассмотрены современные исследования методов эффективного управления дефицитными программными и вычислительными ресурсами клиент-серверных систем. Отмечена общая ориентированность исследований на повышение коэффициента использования этих ресурсов. При этом подразумевается, что потенциально имеющегося объема ресурсов системы хватает для удовлетворения потребностей пользователей системы, то есть дефицит создается неоптимальным распределением, при котором может возникать их неоправданный простой или дефицит локального характера (для отдельно взятых запросов клиентов). Вопросы эффективного управления ресурсами в условиях их общего дефицита не рассматриваются, что обуславливает актуальность исследований в этой области.

Также в главе рассмотрены классические и современные модели доступа в информационных системах, как один из подходов к управлению ресурсами сервера, проведен обзор исследований в данной области и анализ проблем,

связанных с применением стандартных методов, основанных на ролевой или атрибутной моделях управления доступом. Общим недостатком данных подходов является строгая детерминированность правил управления. В этой связи актуальной является задача разработки методов автоматизированного управления вычислительным ресурсом сервера на основе динамических характеристик.

Проведен обзор современных подходов к управлению ресурсами на основе контекста, в частности построенных на репутационных показателях: рейтинг популярности или коэффициент доверия. Рассмотрены подходы к пониманию понятия доверия и способам его численной оценки. Источниками сведений для оценки доверия являются, в основном, данные о соответствии объекта оценки заданным требованиям, статистика его поведения или отзывы пользователей. Иными словами, под доверием понимается степень соответствия реального объекта нашим ожиданиям.

Материалы, приведенные в настоящей главе, подтверждают актуальность проводимого в диссертационной работе исследования.

# Глава 2. Метод управления ресурсами в клиент-серверной информационной системе на основе доверия к клиентам

В данной главе описаны разработанные автором модель доверия к клиентам с использованием специальных взвешенных по степени важности критериев [58, 61] и основанный на ней метод управления вычислительным и программными ресурсам сервера в клиент-серверной информационной системе в условиях их общего дефицита.

## 2.1 Модель доверия к клиентам в информационной системе

Под доверием к клиенту понимается численная мера его соответствия заданному эталону, который определяется владельцем информационной системы через набор проверяемых параметров – критериев доверия. Доверие определяет степень лояльности владельца ресурса к клиенту при авторизации запроса на доступ.

Применяется оптимистичный подход к оценке доверия, т.е. в исходном состоянии владелец информационной системы доверяет клиенту, а в процессе формирования оценки рассматриваются показатели, снижающие степень доверия. Подход может быть мнемонически сформулирован в виде поговорки «доверяй, но проверяй».

Ключевые принципы критериев доверия:

– объективность: значение критерия должно интерпретироваться однозначно, оно не может зависеть от выбора клиента или значения других критериев;

– документированность: составляющие критерий сведения о клиенте должны быть зафиксированы в пригодном для их обработки человеком или машиной виде;

– универсальность: критерии доверия должны одинаково определяться для всех клиентов в системе.

К критериям доверия может относиться информация о программно-техническом составе хоста клиента, назначенные ему роли, атрибуты, статистика активности и инцидентов.

2.1.1 Формирование шкалы весовых коэффициентов критериев доверия

В данном пункте описан подход к формированию шкалы весов, позволяющей получить численную оценку степени соответствия объекта заданным критериям доверия с учетом их значимости. Вопросы исследования оценки сходства с заданным эталоном представлены в работе [41].

Обозначим $M = \{m_i | i = \overline{1,n},\ n \in \mathbb{N}\}$ множество критериев доверия к клиенту $X$ в системе $S$. Для каждого $m_i \in \mathrm{M}$ проведем процедуру нестрогого ранжирования по степени важности критерия или его влияния на общий уровень сходства $X$ с эталоном. Процедура проводится любым способом, например, методом сортировки: критерии перебираются по порядку и для каждого очередного $m_i$ принимается решение: $m_i \prec m_{i+1}$ – $m_{i+1}$важнее $m_i$ или $m_{i+1} \sim m_i$ – критерии равнозначны.

Таким образом, на множестве $M$ будет определено отношение частичного порядка $M_{\preccurlyeq} \in M \times M$, при котором $\forall m_i, m_j \in M : i < j \Rightarrow m_i \prec m_j \vee m_i \sim m_j$. Это отношение разделит $M$ на попарно непересекающиеся классы равнозначных критериев $(M/\sim) = \bigcup_{j \le n} [m_j]$. Будем обозначать $[m_j]$ класс эквивалентности критерия $m_j$, то есть $[m_j] = \{m \in M \mid m \sim m_j\}$. Введем на них функцию пересчета $\varphi$ по правилам (1).

$$\begin{gathered}
\varphi: (M/\sim) \to \mathbb{N}, \\
\forall m_i, m_j \in M : \ m_i \prec m_j \Rightarrow \varphi([m_i]) < \varphi([m_j]), \\
\exists i_{min} = \overline{1,n} \ \forall j \neq i_{min} : m_{i_{min}} \prec m_j \ \Rightarrow \ \varphi([m_{i_{min}}]) = 1, \\
\exists i_{max} = \overline{1,n} \ \forall j \neq i_{max} : m_j \prec m_{i_{max}} \ \Rightarrow \ \varphi([m_{i_{max}}]) = N.
\end{gathered} \tag{1}$$

Будем называть рангом критерия доверия $m$ из $M$ величину $R(m) = \varphi([m])$ и основанием шкалы величину $N^M = \sum_{i=1}^{n} R(m_i)$. Ранг критерия доверия определим как значение функции пересчета для класса эквивалентности $m$, а

основание шкалы – как сумму рангов всех критериев доверия в $M$. Введем понятие веса критерия $W(m)$, как отношение ранга критерия к основанию шкалы (2).

$$W(m) = \frac{R(m)}{N^M} = \frac{\varphi([m])}{\sum_{k=1}^{N} \varphi([m_k])}. \quad (2)$$

При этом для величины $W(m)$ справедливы свойства (3): общий вес всех критериев доверия в $M$ равен 1; критерии доверия с более высоким рангом имеют больший вес.

$$W(M) = \sum_{M} W(m) = 1,$$
$$\forall m_i \prec m_j \Rightarrow W(m_i) < W(m_j). \quad (3)$$

Подход к формированию весовых коэффициентов, описанный в данном пункте, использован также в исследованиях, связанных с управлением доступом и обеспечения надежности системах видеоконференцсвязи [43, 87].

### 2.1.2 Оценка доверия в условиях непостоянных приоритетов критериев

В классических примерах применения методов поддержки принятия решений, таких как метод анализа иерархий (МАИ), приоритеты критериев (альтернатив) часто определяются через приложение теоремы Перрона-Фробениуса как компоненты главного собственного вектора матрицы парных сравнений. При этом на саму матрицу накладываются определенные ограничения, в частности, условия ее неприводимости и неотрицательных элементов, но для ряда случаев такой подход оказывается неприменимым. Свойства и вид матрица парных сравнений, очевидно, определяются способом сравнения альтернатив и соответствующей ему измерительной шкалой. Стандартный подход в МАИ [69] к сравнению альтернатив некоторого набора $X$ предлагает использование отношения предпочтения вида $X \times X \to \{1/i\,, i \mid i = \overline{1,n}, n \in \mathbb{N}\}$, где $n$ – некоторое натуральное

число, обычно выбирается равным 9. С возрастанием степени превосходства одной альтернативы над другой возрастает значение оценки, для равнозначных альтернатив принимается оценка 1. Порядковая шкала, заданная таким образом, позволяет представить отношение предпочтения в виде неприводимой, строго положительной, примитивной матрицы $A$, собственный вектор которой можно найти, опираясь на следствие теоремы Перрона-Фробениуса, как $\lim_{k\to\infty} A^k e / \|A^k\|$, где $\|A^k\| = e^T A e$ ($e$ – единичный вектор): матрица возводится в произвольно большие степени, вычисляются суммы элементов строк , затем нормируются.

В [8, 59, 60, 61, 74] рассмотрены примеры задач принятия решений и соответствующие им шкалы оценки предпочтений, для которых не применим классический подход МАИ. В работе [39] рассматривается задача вычисления весовых коэффициентов интервальной шкалы для оценки сходства объекта с некоторым эталоном на фоне подхода к управлению вычислительными ресурсами в клиент-серверной системе на основе доверия к клиентам. Исследования вопросов выбора весовых коэффициентов различными методами рассмотрены также в работах В.М. Постникова и С.Б. Спиридонова [63, 74].

Описанный в пункте 2.1.1 подход требует важной оговорки. Частичный порядок для критериев из $M$ задается экспертным путем. Если не рассматривать тривиальный вариант, когда эксперт всего один, для применения описанного подхода на практике мнения экспертов должны быть согласованы некоторым строго определенным образом. Также, в случаях, когда задача, использующая оценки в данной шкале, является итерационной или регулярной, мнения экспертов могут меняться с накоплением опыта, эти изменения так же должны отражаться в шкале.

Множество $M_{\preccurlyeq} \in M \times M$ отношения нестрого порядка может быть представлено в виде матрицы парных сравнений $A = (a_{ij})_{n\times n} = (a_{ij})$, заполненной по правилам (4).

$$\forall i = \overline{1,n}, j = \overline{1,n} \quad a_{ij} = \begin{cases} 1, \text{если } m_i \succ m_j \text{ или } m_i \sim m_j, \\ 0 \text{ в других случаях.} \end{cases} \tag{4}$$

Будем считать, что каждый эксперт задает собственную матрицу парных сравнений $A^{\langle y \rangle}$, где $y$ – идентификатор эксперта. Не теряя общности рассуждений, можно считать, что число экспертов в системе не ограничено (т.е. $y \in \mathbb{N}$) и каждый эксперт высказывается только один раз. Тогда в качестве компромиссного мнения экспертов можно считать $\tilde{A}$ нормированную сумму представленных ими матриц парных сравнений $A^{\langle y \rangle}$. В качестве нормы матрицы $\tilde{A}$ будем принимать ее наибольший элемент. Тогда итоговая матрица парных сравнений критериев из $M$ будет найдена по формуле (5).

$$\tilde{A} = \frac{\sum_y A^{\langle y \rangle}}{\max\limits_{i,j} \left( \sum_y a_{ij}^{\langle y \rangle} \right)}. \tag{5}$$

Из формулы (5) можно заметить, что $\forall i, j = \overline{1,n}\ a_{ij} \in [0; 1]$. Это значит, что матрица $\tilde{A}$ описывает нечеткое отношение порядка на $M$ и может применяться в системах принятия решений на базе нечеткой логики. Однако в данном исследовании основным является вопрос ранжирования критериев на основе $\tilde{A}$.

В классических применениях метода анализа иерархий приоритеты критериев (альтернатив) часто определяются через приложение теоремы Перрона-Фробениуса как компоненты главного собственного вектора матрицы парных сравнений. В нашем случае такой подход неприменим, поскольку на матрицу $\tilde{A}$ не распространяется в общем случае условие неприводимости, необходимое для применения теоремы.

В задаче определения весовых коэффициентов критериев ранговой шкале важным условием является равномерность изменения значений весов. Так для частично упорядоченного множества $M$ подход (2), описанный ранее, обеспечивает приращение веса критерия в шкале на постоянную величину, равную

минимальному весу критерия $W(m_1) = {}^{1}/_{N^M} = \varepsilon$. Для нечетного отношения $\tilde{A}$ на $M$ такой подход уже неприменим, требуется найти иной подходящий метод поиска весовых коэффициентов $m_i$, основанный на обработке матрицы $\tilde{A}$. Будем обозначать как $w = (w_1, \dots, w_n)$ вектор весовых коэффициентов, где соответствующие $w_i$ определяют вес $m_i \in M$.

Рассмотрим несколько способов вычисления главного собственного вектора матрицы, не связанных с наложением на нее дополнительных ограничений. Аналогичные исследования представлены в [8, 69], а также в упомянутых ранее [63, 74]. Все способы имеют по два этапа: вычисление вектора приоритетов по матрице и, затем, его нормирование, отличают их только методы вычисления компонент вектора и его нормы. Поэтому общая формула вектора весовых коэффициентов , будет иметь вид (6), где $w^{(i)}$ – ненормированный вектор приоритетов по матрице, $\left\|w^{(i)}\right\|$ – его норма, $i$ – соответствующий индекс способа вычисления.

$$w = \frac{w^{(i)}}{\left\|w^{(i)}\right\|}. \tag{6}$$

Способ 1: вычислить $w^{(1)}$ как сумму элементов каждой строки и $\left\|w^{(1)}\right\|$ как сумму всех элементов матрицы $\tilde{A}$, затем разделить полученные значения суммы строк на сумму всех элементов (нормализовать); сумма полученных результатов будет равна единице (7).

$$w^{(1)} = \left(\sum_{j=1}^{n} a_{ij}\right)_n, \left\|w^{(1)}\right\| = \frac{1}{\sum_{k,j=1}^{n} a_{kj}}. \tag{7}$$

Способ 2: Вычислить матрицу $\tilde{A}^T$, далее найти $w^{(2)}$ как величину, обратную к значению суммы элементов каждой строки этой матрицы, и $\left\|w^{(2)}\right\|$ как сумму полученных значений $w^{(2)}$ (8).

$$w^{(2)} = \left(\frac{1}{\sum_{j=1}^{n} a_{ji}}\right)_n, \left\|w^{(2)}\right\| = \sum_{i=1}^{n} w_i . \quad (8)$$

Способ 3: нормализовать столбцы матрицы $\tilde{A}$ по общей сумме их элементов, затем вычислить $w^{(3)}$ сложением элементов каждой полученной строки, в качестве $\left\|w^{(3)}\right\|$ принять число элементов строки (9).

$$w^{(3)} = \left(\sum_{j=1}^{n} \frac{a_{ij}}{\sum_{k=1}^{n} a_{kj}}\right)_n, \left\|w^{(3)}\right\| = n. \quad (9)$$

Будем оценивать степень сходства распределения весов для критериев с методом (1), разница $\Delta$ весовых коэффициентов соседних элементов $w^{\uparrow}$упорядоченного массива компонент вектора $w$ не должна превышать вес самого маловесного критерия $\varepsilon$, т.е. $\Delta = \left|w_i^{\uparrow} - w_{i-1}^{\uparrow}\right| \in [0; \varepsilon]$ для $\forall i = \overline{2,n}$. В качестве критерия сравнения способов будем использовать максимальное значение $\Delta_{max} = \max_i \left|w_i^{\uparrow} - w_{i-1}^{\uparrow}\right|$ и $\sigma$ величину среднеквадратичного отклонения значений $\Delta$ от середины отрезка ее ожидаемых значений. Будем считать, что способ схож с методом (1), если $\Delta_{max} \leq \varepsilon$ и $\sigma \leq \frac{\varepsilon}{2}$.

Для сравнения данных подходов к вычислению вектора приоритетов будем использовать исходные данные для ранжирования критериев доверия из приложения В к данной работе: в опросе участвует 10 экспертов, набор критериев доверия состоит из 13 пунктов. Далее представим мнения экспертов в виде матриц парных сравнений $A^{\langle y \rangle}$ согласно правилу (4). Столбцы матриц соответствуют порядку критериев доверия в опросном листе, элемент матрицы $a_{ij}$ равен 1, если ранг критерия $m_i$ равен либо превосходит ранг $m_j$. Список матриц парных сравнений приведен так же в приложении В к диссертационной работе. Найдем

общую матрицу компромиссного мнения экспертов $\tilde{A}$, используя формулу (5), дробные значения для удобства будем записывать в виде десятичной дроби, округляя их до второго знака. Матрица приведена в (10).

$$\tilde{A} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,6 & 0 & 0 \\ 0,5 & 1 & 1 & 1 & 0,6 & 1 & 1 & 0,9 & 1 & 1 & 1 & 1 & 1 \\ 0,9 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0,8 & 1 & 1 & 1 & 1 & 1 & 0,7 \\ 0 & 1 & 1 & 0 & 0 & 0,8 & 1 & 1 & 0,8 & 1 & 1 & 1 & 0,9 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0,7 & 1 & 0,3 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0,5 & 0,3 & 1 & 1 & 1 & 1 & 1 & 0,3 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0,2 & 0,9 & 0 & 1 & 1 & 0,3 & 0,2 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0,4 & 0 & 0,4 & 1 & 0,1 & 0,1 \\ 0 & 1 & 1 & 0 & 0 & 0,3 & 0,1 & 1 & 0,7 & 0,7 & 0,9 & 1 & 0,1 \\ 0 & 1 & 1 & 0 & 0 & 0,7 & 0,9 & 1 & 0,8 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (10)$$

Будем по порядку применять к матрице $\tilde{A}$ рассматриваемые способы поиска $w$. Выделим в каждом способе два промежуточных этапа, унифицирующих эти способы и, тем самым, позволяющих вести сравнение более наглядно. В первую очередь будем искать промежуточные значения для ненормированного вектора весовых коэффициентов $w^{(i)}$, а затем, его нормы $\left\|w^{(i)}\right\|$. Формально $w^{(i)}$ представляют собой вектор-столбец, однако для удобства будем записывать их в виде строк. Сводные значения $w^{(i)}$ и $\left\|w^{(i)}\right\|$ приведены ниже:

$w^{(1)} =$ (13; 2,6; 2,6; 12; 12,9; 9,5; 9,5; 5; 8,1; 5,6; 4; 6,8; 9,4), $\left\|w^{(1)}\right\| = 101$;

$w^{(2)} =$ (0,42; 0,08; 0,08; 0,33; 0,38; 0,16; 0,16; 0,1; 0,14; 0,1; 0,08; 0,11; 0,16), $\left\|w^{(2)}\right\| = 2,3$;

$w^{(3)} =$ (2,3; 0,2; 0,2; 1,93; 2,26; 1,09; 1,09; 0,44; 0,86; 0,52; 0,34; 0,69; 1,07), $\left\|w^{(3)}\right\| = 10$.

Результаты вычислений вектора приоритетов $w$, а также величин $\Delta_{max}$ и $\sigma$ приведены в таблице 1. Из приведенных данных можно заключить, что наиболее предпочтительным с точки зрения сходства с методом (1) способ распределения весовых коэффициентов является первый из трех рассмотренных: максимальная разница $\Delta_{max}$ между двумя упорядоченными весами равна минимальному весу

критерия и среднеквадратичное отклонение не выходит за заданные границы. Для остальных двух способов наблюдается превышение $\Delta_{max} > \varepsilon$, что находит свое отражение в значении величины $\sigma$.

Таблица 1 – Значения весовых коэффициентов критериев

| Способ 1 | | | Способ 2 | | | Способ 3 | | |
|---|---|---|---|---|---|---|---|---|
| $w$ | $w^{\uparrow}$ | $\Delta$ | $w$ | $w^{\uparrow}$ | $\Delta$ | $w$ | $w^{\uparrow}$ | $\Delta$ |
| 0,13 | 0,13 | 0,00 | 0,18 | 0,18 | 0,01 | 0,23 | 0,23 | 0,00 |
| 0,03 | 0,13 | 0,01 | 0,03 | 0,17 | 0,02 | 0,02 | 0,23 | 0,03 |
| 0,03 | 0,12 | 0,02 | 0,03 | 0,14 | 0,08 | 0,02 | 0,19 | 0,08 |
| 0,12 | 0,09 | 0,00 | 0,14 | 0,07 | 0,00 | 0,19 | 0,11 | 0,00 |
| 0,13 | 0,09 | 0,00 | 0,17 | 0,07 | 0,00 | 0,23 | 0,11 | 0,00 |
| 0,09 | 0,09 | 0,01 | 0,07 | 0,07 | 0,01 | 0,11 | 0,11 | 0,02 |
| 0,09 | 0,08 | 0,01 | 0,07 | 0,06 | 0,01 | 0,11 | 0,09 | 0,02 |
| 0,05 | 0,07 | 0,01 | 0,04 | 0,05 | 0,01 | 0,04 | 0,07 | 0,02 |
| 0,08 | 0,06 | 0,01 | 0,06 | 0,04 | 0,00 | 0,09 | 0,05 | 0,01 |
| 0,06 | 0,05 | 0,01 | 0,04 | 0,04 | 0,01 | 0,05 | 0,04 | 0,01 |
| 0,04 | 0,04 | 0,01 | 0,04 | 0,04 | 0,00 | 0,03 | 0,03 | 0,01 |
| 0,07 | 0,03 | 0,00 | 0,05 | 0,03 | 0,00 | 0,07 | 0,02 | 0,00 |
| 0,09 | 0,03 | - | 0,07 | 0,03 | - | 0,11 | 0,02 | - |
| $\Delta_{max} = 0{,}02, \sigma = 0{,}01$ | | | $\Delta_{max} = 0{,}08, \sigma = 0{,}07$ | | | $\Delta_{max} = 0{,}08, \sigma = 0{,}08$ | | |

По итогу сравнения рассмотренных способов вычисления весовых коэффициентов критериев видно, что наименее адекватные результаты показали второй и третий способы. Наиболее равномерное распределение весов показал способ 1, его результаты наиболее близки к шкале, построенной в условиях определенности (полного совпадения мнений экспертов): максимальная разница между соседними весами приблизительно равна минимальному весу в шкале, среднеквадратичное отклонение минимально в сравнении с другими способами.

### 2.1.3 Формирование оценки доверия

Обозначим как $W(M) = (W_1, \dots, W_n)$ вектор весовых коэффициентов, где соответствующие $W_i$ определяют вес $m_i \in M$. Компоненты $W$ находятся в два

этапа: суммирование элементов каждой строки $\tilde{A}$ и нормализация делением каждой суммы на сумму всех элементов $\tilde{A}$ (7).

$$W = \frac{1}{\sum_{k,j=1}^{n} a_{kj}} \left( \sum_{j=1}^{n} a_{ij} \right)_n \tag{11}$$

Далее описан общий порядок оценки доверия к клиенту $X$ в системе $S$. Клиент $X$ задан кортежем бинарных значений $(x_1, \dots, x_n)$, определяющих факт соответствия клиента критериям доверия из $M$. Оценкой доверия к клиенту принято называть функцию $T(X): M \to [0; 1]$.

$$T(X) = 1 - \sum_{i=1}^{n} x_i \cdot W(m_i)\,. \tag{12}$$

Для тривиального варианта шкалы весов $W$, когда в формировании шкалы участвует только один эксперт (либо мнения экспертов совпадают) с учетом формулы (2) веса критерия формула для функции оценки доверия $T(X)$ примет более простой и определенный вид (13).

$$T(X) = 1 - \sum_{i=1}^{n} x_i \cdot W(m_i) = 1 - \frac{1}{N^M} \sum_{i=1}^{n} x_i r_i\,. \tag{13}$$

Функции оценки доверия, заданные формулами (12) и (13), являются основой разработанного метода управления ресурсами сервера в системе $S$.

## 2.2 Метод управления ресурсами на основе оценки доверия

В данном пункте проведен анализ необходимых свойств функции предложенной модели доверия, описан математический аппарат метода и приведен пошаговый порядок его применения.

### 2.2.1 Приращение функции оценки доверия

Пусть в клиент-серверной системе задано дискретное время. Для всякого клиента $X$ будем обозначать как $X^t$ состояние $X$ в момент времени $t$. Аналогично, если $x_i$ – значение $i$-го критерия доверия для клиента $X$, то ${x^t}_i$ – значение $i$-го критерия доверия для клиента $X$ в момент времени $t$. Также если $T = T(X)$ – значение оценки доверия для клиента $X$, то $T^t = T(X^t)$ – значение оценки доверия для $X$ в момент времени $t$.

Будем называть шагом приращения оценки доверия $\Delta T$ величину, на которую изменится значение функции оценки доверия $T(X)$ при изменении значения одного критерия доверия для клиента $X$. Формальная запись определения представлена в формуле (14).

$$\Delta T = \mathrm{T}(X^1) - \mathrm{T}(X^0),$$
$$\exists_1 i \in \{1, \dots, n\}: X^0 = (x_1, \dots, x_i, \dots x_n), X^1 = (x_1, \dots, \neg x_i, \dots, x_n). \qquad (14)$$

Следует заметить, что функция $T(X)$ дискретна на отрезке $[0; 1]$, возможные варианты ее значений определяются комбинациями сумм весов критериев доверия в шкале $W(M)$. Для осмысления понятия приращения функции оценки доверия обозначим как $\varepsilon = W_{min}$ величину минимального шага приращения и, соответственно, $\mathrm{E} = W_{max}$ величину максимального шага приращения функции оценки доверия $\Delta T$.

Для тривиального варианта шкалы весов $W$, когда в формировании шкалы участвует только один эксперт (либо мнения экспертов совпадают) из условия (1) и формулы (14), а также соответствующего вида функции оценки (13) следует, что значение $\Delta T$ определяется рангом $r$ изменяемого значения критерия доверия $m_i$ из

$M$. Поэтому заданные условия для ε и E будут выполняться при значениях $r = 1$ и $r = N$ соответственно и тогда $\varepsilon = \min(\Delta T) = {}^{1}/_{N^M}$, $\mathrm{E} = \max(\Delta T) = {}^{N}/_{N^M}$.

Совокупность значений выполненных ранее оценок доверия к клиенту $T^0, \dots, T^{t-1}$ удовлетворяет установленным принципам определения критерия доверия:

1) Имеет численный формат и строго определенную область значений в $Q$;

2) Существует и может применяться для всех клиентов в системе $S$;

3) Не зависит от других критериев доверия и клиентов в системе $S$, оцениваемых в момент времени $t$.

На основании этого можно заключить, что $T^0, \dots, T^{t-1}$ можно рассматривать в качестве критерия доверия к клиенту $X$ в системе $S$.

Введем в набор критериев доверия $M$ дополнительный критерий $\widehat{m}$, условно назовем его фактором положительной обратной связи. В принятой системе определения критериев доверия фактор положительной обратной связи должен быть включен в перечень критериев доверия $M = \{\widehat{m}, m_1, \dots, m_n\}$, ему должен быть присвоен определенный вес.

Введенный критерий как фактор положительной обратной связи может применяться для стимулирования клиента в повышении уровня доверия к себе при его значениях, близких к пороговому. Если уровень доверия к клиенту $X$ не поднимается выше определенного значения $\phi$ в течение времени $\hat{t}$, доверие к клиенту снижается на $W(\widehat{m})$. Пусть $X = (\hat{x}, x_1, \dots, x_n)$, где $\hat{x}$ свойство клиента, соответствующее критерию $\widehat{m}$, тогда можно определить $\hat{x}$ через условие (15).

$$\hat{x} = \begin{cases} 1, \forall i \le \hat{t}: T^{t-i}(X) \le \phi, \\ 0, \exists i \le \hat{t}: T^{t-i}(X) > \phi; \end{cases} \tag{15}$$

Целесообразно устанавливать значение $\phi$ относительно порога доверия. При приближении уровня доверия $T(X)$ к порогу доверия Z на величину, связанную с рангом фактора положительной обратной связи, в течение времени $\hat{t}$, доверие к

нему будет потеряно. В этом смысле предложено установить значение веса данного критерия равным величине минимального приращения функции оценки доверия $W(\hat{m}) = \varepsilon$ и тогда $\phi = \mathrm{Z} - \varepsilon$. Для тривиального случая такое условие эквивалентно включению фактора обратной связи в класс эквивалентности критериев с минимальным весом $\hat{m} \in [m_1]$.

### 2.2.2 Порог доверия

Порогом доверия Z будем называть минимальное значение функции оценки доверия $T(X)$ к клиенту $X$, при котором он считается доверенным в системе $S$. Формальная запись этого условия приведена в формуле (16), где $X_T$ – множество доверенных клиентов системы.

$$T(X) > \mathrm{Z} \Rightarrow X \in X_T. \tag{16}$$

Выбор порога доверия является ключевой смысловой частью разработанного метода управления ресурсами, поскольку именно значение Z определяет минимально необходимую степень доверия к клиенту для успешной авторизации его доступа к серверу системы.

Интуитивно верным является утверждение, что значение порога доверия целесообразно определять через значения функции оценки доверия $T(X)$, поскольку, как было сказано выше, функция дискретна и вполне задается комбинациями весов критериев из $W(M)$. Также справедливо, что наибольшее влияние на решение о доступе должны оказывать критерии с наибольшим весом в силу введенного подхода к формированию понятия веса по условию (1) из пункта 2.1 настоящей главы. Если порог доверия выбран таким образом, что на решение о доступе по условию (16) в момент времени $t$ повлияло изменение критерия $m_i$ такого, что $W(m_i) < \mathrm{E}$, значит, по определению отношения нестрогого порядка $M_{\preccurlyeq}: M \times M$ критерий $m_i$ более важен чем некоторый критерий $m_j = W_{max} = \mathrm{E}$, что нарушает свойство (3) для веса критериев доверия: $m_i \succ m_j \not\Rightarrow W(m_i) > W(m_j)$.

Из изложенных выше рассуждений в рамках описанного метода управления ресурсами при выборе значения порога доверия Z предложено опираться на наиболее существенные критерии доверия из $M$, то есть на критерии, вес которых сравним с E на множестве значений функции оценки доверия.

Для тривиальной шкалы весов $W(M)$, заданной четким отношением (с привлечением одного эксперта) условие сравнимости с E можно определить через класс эквивалентности критериев с наибольшим весом, т.е. $W(m) \cong \mathrm{E} \Leftrightarrow m \in [m_n]$.

Для шкалы весов $W(M)$, заданной нечетким отношением предпочтения на основе матрицы $\tilde{A}$ (основной случай с несколькими экспертами), условие сравнимости следует определять с использованием минимального значения веса критерия в шкале ε: $W(m) \cong \mathrm{E} \Leftrightarrow W(m) - \mathrm{E} < \varepsilon$.

Из этих соображений для задачи управления ресурсами системы $S$ рассмотрим два пограничных варианта определения Z.

— Лояльный: наиболее мягкий к клиенту подход, для потери доверия к себе клиент $X$ должен не соответствовать всем наиболее значимым критериям, т.е. близким по весу к E в шкале значений оценки $T$ (формула (17)).

$$\mathrm{Z}_{\text{лоял}} = 1 - \mathrm{E} \cdot |\nu|, \text{где } \nu = \{W_i \mid (\mathrm{E} - W_i) < \varepsilon\}. \quad (17)$$

— Строгий: наиболее требовательный к клиенту подход, для потери доверия к себе клиент $X$ должен не соответствовать хотя бы одному из наиболее значимых критериев (формула (18)).

$$\mathrm{Z}_{\text{строг}} = 1 - (\mathrm{E} + \varepsilon). \quad (18)$$

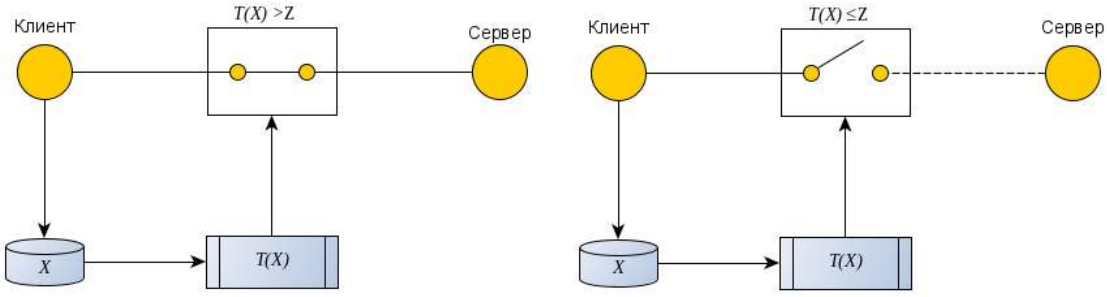
Следует заметить, что в случае строгого подхода к выбору порога для учета всех возможных весов критериев, сравнимых с E, необходимо вносить поправку в виде ε.

$$\mathrm{Z}_{\text{лоял}} = 1 - |[m_n]| \cdot \mathrm{E},$$
$$\mathrm{Z}_{\text{строг}} = 1 - \mathrm{E}. \qquad (19)$$

Для тривиального варианта шкалы весов $W(M)$ значения порога доверия Z для лояльного и строгого подходов будут задаваться формулами (19) соответственно.

### 2.2.3 Описание метода управления ресурсами на основе оценки доверия

Разработанный автором метод управления ресурсами в клиент-серверной системе предполагает управляющее воздействие на канал связи между клиентом и сервером. Для клиентов с уровнем доверия ниже установленного порога, канал связи блокируется, и сервер не получает запрос авторизации от клиента, таким образом, недоверенные клиенты не могут подключиться к системе. Схема работы метода проиллюстрирована на рисунке 3.




а) б)

Рисунок 3 – Схема метода управления ресурсами сервера на основе оценки доверия: а) для доверенного клиента; б) для недоверенного клиента

Общий порядок применения метода включает следующие этапы.

Этап 1: формирование набора критериев доверия $M$.

На данном этапе владелец системы составляет и формализует перечень характеристик и иных проверяемых сведениях о клиентах $X$, опираясь на принципы выбора критериев, описанные в пункте 2.1 данной главы. Выполнение этапа 1 зависит от наличия в распоряжении владельца системы средств сбора и обработки

информации о программно-техническом составе хостов клиентов, статистических и иных контекстных данных. Технические условия для успешного формирования перечня критериев доверия приведены в главе 3.

Этап 2. Опрос экспертов, формирование матриц парных сравнений критериев доверия $A^{\langle y \rangle}$ и матрицы компромиссного мнения $\tilde{A}$.

На этапе 2 проводится опрос экспертов, в качестве формы опроса принято использовать опросный лист из приложения В. Каждый эксперт ставит отметку в ячейке опросной таблицы для каждого критерия доверия согласно его приоритету (растет с увеличением ранга). На основе опросных листов составляются соответствующие матрицы парных сравнений $A^{\langle y \rangle}$, определяющие нестрогий порядок на множестве критериев $M$. По формуле, приведенной в пункте 2.1.2, строится матрица $\tilde{A}$ нечеткого отношения предпочтения для критериев доверия.

Этап 3. Построение порядковой шкалы весов критериев $W(M)$, выбор порога доверия Z.

Описанным в пункте 2.1.2 способом формируется вектор приоритетов критериев доверия $W(M)$, компоненты этого вектора определяют вес соответствующих критериев доверия из $M$. Далее определяются величины минимального и максимального приращений оценки доверия $\varepsilon = W_{min}$ и соответственно $\mathrm{E} = \mathrm{W}_{max}$. Исходя из их значений и выбранного подхода к управлению (строгий или лояльный) вычисляется значение порога доверия Z.

Этап 4. Вычисление оценки доверия $T(X)$ для клиента $X$.

На данном этапе клиент $X$ формально представляется в виде набора своих параметров $\{x_1, \dots, x_n\}$, соответствующих критериям доверия $\{m_1, \dots, m_n\}$ из $M$; проводится проверка параметров и вычисляется значение функции оценки доверия $T(X)$ по формуле, приведенной в пункте 2.1.3.

Этап 5. Принятие решения о клиенте $X$ к серверу системы $S$.

На завершающем этапе метода владелец системы, опираясь на полученное значение оценки доверия к клиенту и сравнивая его с порогом доверия, принимает решение о разрешении или ограничении доступа данному клиенту $X$ к серверу системы $S$. На основе принятого решения формируется управляющий сигнал на замыкание (или, в случае отказа в доступе, размыкание) канала связи между клиентом $X$ и сервером $S$. Техническая реализация данного механизма управления каналом описана в пункте 3.3.

## 2.3 Выводы

В главе представлен метод управления вычислительными и программными ресурсами в клиент-серверной системе использует актуальные контекстные данные клиентов для принятия решения о разрешении или ограничении сетевого подключения клиента к серверу системы; перечень проверяемых сведений определяется владельцем системы (сервера) исходя из его представлений о необходимой или оптимальной конфигурации характеристик клиента и статистики его поведения. Из перечня проверяемых сведений строится эталонный образ, с которым впоследствии сравниваются клиенты системы. Степень сравнения определяет оценку доверия к клиенту. Таким образом, профиль эталонного клиента должен подбираться индивидуально для каждой информационной системы предприятия и соответственно, оценка доверия к клиенту ориентирована на решаемую им задачу.

Метод предполагает воздействие на канал связи между клиентом и сервером, т.е. подразумевает вмешательство только в инфраструктурную составляющую клиент-серверной системы, не требует вмешательства в организацию работы самой системы, и не расходует вычислительные ресурсы сервера. Это делает метод весьма удобным для применения на практике и его интеграции в существующие информационные системы.

Также в главе описана модель доверия к клиентам в клиент-серверной информационной системе, на которой строится данный метод. Модель строится на

ранговой нормированной шкале взвешенных критериев доверия, по которым проводится их сравнение клиента с эталоном доверия. Шкала строится на основе экспертных оценок важности, модель использует аппарат нечеткой логики, в частности, нечетких отношений, для учета совокупного мнение экспертов. Также модель описывает способ вычисления весовых коэффициентов, обеспечивающий наиболее равномерное распределение весов в шкале.

# Глава 3. Система управления ресурсами в клиент-серверной системе, реализующая метод управления ресурсами на основе доверия

В главе описаны технические условия для реализации метода управления ресурсами в клиент-серверной системе на основе оценки доверия, приведены способы формирования исходных данных для проверки критериев и вычисления оценки доверия, механизмы управления каналом связи между хостами (оконечными узлами сетевой инфраструктуры предприятия) для непосредственной реализации метода, а также описана система управления ресурсами в клиент-серверной системе, реализующая разработанный метод на основе оценки доверия.

## 3.1 Формирование исходных данных для оценки доверия

Важным этапом при формировании набора критериев является подбор источников информации о клиентах, которые будут использоваться при оценке доверия. Владелец системы должен опираться на сведения, которые помогут ему понять, какие из клиентов будут использовать ресурс сервера наиболее эффективно. К таким сведениям может относиться информация о соответствии клиента техническим условиям обработки информации в рамках общего технологического процесса, политикам управления, сведениям о решаемых клиентом задачах, роли клиента в системе или иной контекстной информации, данные статистики, история инцидентов и т.д.

Техническими источниками сведений для сведений для проверки критериев доверия могут быть:

– учетные записи о клиенте в электронных реестрах и базах данных: службы каталогов, реестры регистрация в информационных системах;

– информация систем управления (PLM, ERP и т.д.);

– информация систем мониторинга: статистика работы с сервером, факты нарушения политик управления, компьютерные инциденты и т.д.;

– информация о технических условиях функционирования клиента: подключение к информационным системам (в том числе к информационно-

телекоммуникационным сетям (ИТКС) общего пользования), обработка специализированной информации;

– информация о программно-техническом составе клиента: состав и версии общесистемного и специального программного обеспечения, наличие важных обновлений, версии ключевых программных модулей, наличие обязательных к установке компонентов, наличие (отсутствие) технических компонентов и т.д.

Получение и подготовка информации систем управления, мониторинга и учета не представляет большой технической сложности, поскольку находится, по сути, под контролем владельца системы. Эти системы хранят данную информацию в уже пригодном для обработки формате и, как правило, снабжены инструментами для транзита в другие системы. Наибольшую сложность представляет задача получения информации о программно-техническом составе и режимах работы самого клиента, т.к. стандартные средства сбора подобной информации от клиента, как правило, отсутствуют.

Оценка доверия к клиенту относительно его программно-технических средств должна строиться на непрерывном анализе данных мониторинга. Обеспечение стабильного функционирования системы мониторинга требует отдельных технических решений на уровне клиента. Информация о фактах установки, удаления, изменения режима работы, сбоях компонентов системы мониторинга является существенной в задаче управления, потому она должна документироваться и может использоваться при оценке доверия к узлу.

Исследования автора, связанные с разработкой способов получения актуальной и адекватной информации о клиентах в корпоративной клиент-серверной системе представлены в работах [31, 42, 66].

Ниже описан подход и функциональная структура организации контроля компонентов системы мониторинга оконечных узлов. Схема и порядок взаимодействия модулей представлены на рисунке 4.

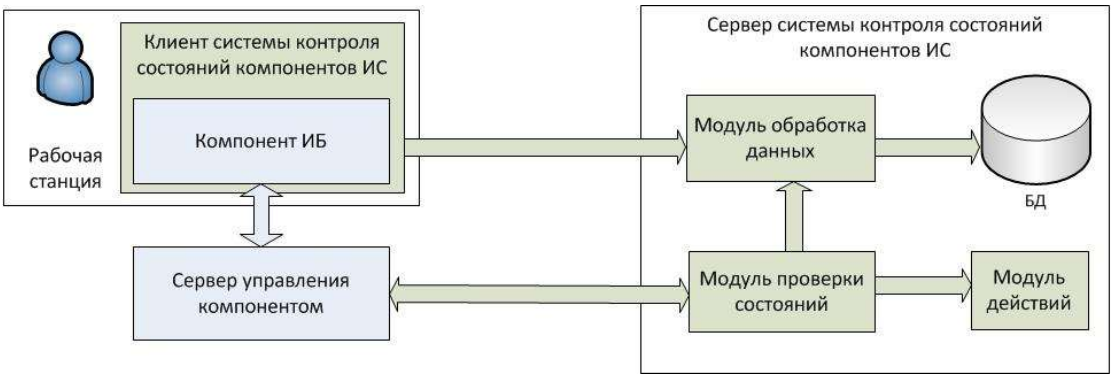



Рисунок 4 – Схема системы контроля модулей мониторинга.

Модуль «установки компонентов» выполняет анализ состояния агентов системы мониторинга на этапе установки на целевом компьютере. При этом проводится проверка совместимости программного обеспечения агента с ОПО и СПО компьютера, контроль корректности работы агента в начале штатной работы. Результаты работы модуля отправляются на сервер в виде отчета.

Модуль «приема и обработки данных» обеспечивает пополнение базы данных системы мониторинга информацией от агентов. Модуль получает на вход сообщения в заданном формате, преобразует их для хранения, дальнейшей обработки и записывает информацию в базу данных. Сообщения включают идентификационную информацию агента на целевом хосте. Реляционная БД [3] хранит данные обо всех изменениях состояний агентов систем, все записи снабжены классификаторами уровня важности.

Модуль «проверки состояний» осуществляет контроль работы агентов системы. Проверка организуется регулярным опросом состояния агентов, при котором посредством специальных сетевых пакетов рассылаются запросы состояния («Heartbeat Discovery») и далее ведется контроль получения ответных сообщений от агентов. Эти данные так же заносятся в БД системы мониторинга с определенной пометкой важности.

Модуль «действий» обеспечивает взаимосвязь автоматических компонентов мониторинга с владельцем системы через аппарат оповещения о критичных событиях в системе, также модуль инициирует запуск протоколов реагирования.

Описанный выше функционал системы мониторинга позволяет организовать автоматизированный контроль состояния программно-технических компонентов корпоративной информационной системы, обеспечить оперативное реагирование на критические события, обеспечивая при этом их документирование. Эти сведения удовлетворяют принципам выбора критериев доверия, указанным в пункте 2.1, и могут применяться в дальнейшем для использования при оценке доверия к клиентам на основе их сравнения с заданным эталоном.

### 3.2 Моделирование и анализ сетевой топологии

Решение задачи управления доступом клиентов к серверу системы посредством управляющих воздействий на канал связи требует попутного решения ряда вспомогательных задач, таких как унификация описания оконечных и сетевых объектов информационной системы и математическое моделирование связей между ними. Последнее условие имеет место в силу следующего обстоятельства. Управление доступом на уровне канала связи фактически сводится к воздействию на процедуру сетевого подключения клиента к серверу системы, что позволяет рассматривать сервер как абстрактный узел, не привязываясь к деталям его исполнения и способам авторизации доступа на уровне самого сервера. Однако решение об авторизации сетевого доступа не может приниматься владельцем системы в момент запроса на подключение от клиента в силу особенностей сетевых протоколов стека TCP/IP [125], которые не предусматривают операцию авторизации третьей стороной. Поэтому авторизация должно проходить отложено, т.е. фактически должна обеспечиваться (или ограничиваться) возможность сетевого подключения клиента к серверу. Общие вопросы проблем управления доступом в сети и сетевой авторизации рассмотрены ранее в главе 1.

Моделирование вычислительной сети (общей топологии и правил взаимосвязи между узлами) является важным этапом при решении задачи автоматического управления сетевым доступом клиентов к ресурсам сети, естественным образом включаемых в абстракцию понятия сервер. Среди существующих решений, разработанных как в рамках исследований [32, 37, 62, 95],

так и коммерческих продуктов [77], механизмы взаимосвязи элементов вычислительной сети рассматриваются лишь косвенно, при моделировании определенных свойств. В большинстве своем вопросы моделирования вычислительных сетей рассматриваются в контексте имитации сетевых устройств, часто для исследования сетевого трафика [47, 71, 116]. Для прогнозирования поведения системы при организации управления доступом описанным образом необходимо построить модель вычислительной сети, которая учитывает ее топологию и взаимодействие терминальных элементов.

В настоящем пункте описана модель вычислительной сети [40], имитирующая взаимосвязи между ее оконечными узлами на сетевом уровне взаимодействия стека протоколов TCP/IP [125]. Модель построена на основе логики предикатов первого порядка. В качестве программной платформы для реализации модели выбрана среда разработки SWI-Prolog v.6 [134] на основе языка логического программирования Prolog.

### 3.2.1 Математический аппарат для моделирования вычислительной сети

Вычислительная сеть представляется множеством объектов $node(Adr/Msk)$, характеризуемых двумя параметрами: адресом $Adr$, представляющим собой натуральное число длиной 2 байта ($Adr \in \{1, \dots, (2^{32} - 1)\}$), и маской подсети $Msk$, определяющей количество единиц в старших разрядах двухбайтового числа. Принято считать записи маски подсети в виде шестнадцатеричного числа (далее пример) 0xffffff00 (длинная запись) и десятичного 16 (короткая запись) эквивалентными. Для проверки корректности длинной записи маски подсети введен предикат $msk(A)$. Блок-схема предиката $msk(A)$ приведена на рисунке 5.

Исходя из блок-схемы можно говорить, что переменная $A$ является маской подсети в следующих случаях:

1) $A$ равна нулю;

2) $A$ четно и $A/2$ является маской подсети;

3) $A$ нечетно ($A\ mod\ 2\ =\ 1$), $A/2$ нечетно и A/2 является маской подсети.

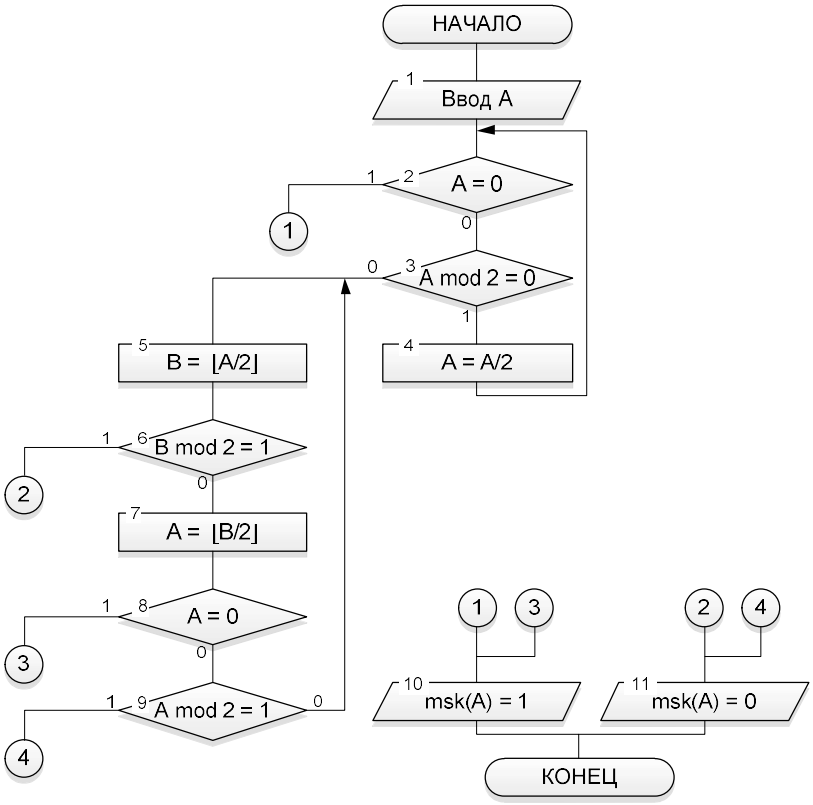



Рисунок 5 – Блок-схема предиката поверки длинной записи маски подсети

Предикат $msk(A)$ принимает значение «истина», когда его переменная удовлетворяет изложенным выше условиям. Предикат $short\_mask(S, L)$ связывает длинную запись маски подсети с соответствующей ей короткой записью: $short\_msk(S, L) := msk(L) \& (0 \leq S \leq 32) \& (L = (2^{32} - 1) << (32 - S))$.

$short\_msk(S, L)$ принимает значение «истина», когда значение его переменной $S$ (короткая запись маски) удовлетворяет определению маски подсети и равно количеству единиц в старших разрядах переменной $L$, соответствующей длинной записи маски, то есть, когда короткая запись маски подсети соответствует длинной записи.

Узел сети, таким образом, определяется через предикаты $msk$ и $short\_msk$, как продемонстрировано на рисунке 6.

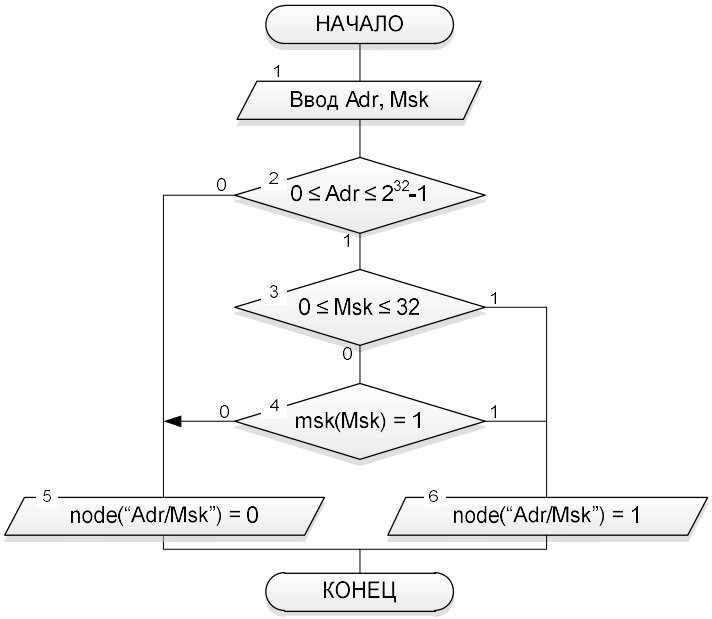



Рисунок 6 – Блок-схема предиката проверки корректности параметров узла сети

Далее подсетью $subnet$ будем называть объект сети, адрес и маска которого удовлетворяют условию $subnet(\text{“}Adr/Msk\text{”}) := Adr \wedge \neg(Msk) = 0$. Оконечным узлом (или хостом) сети будем называть остальные объекты сети, т.е. которые не является подсетями.

Понятие подсеть применяется для обозначения множества хостов, объединенных по некоторому признаку – адресу подсети. Поэтому среди хостов и подсетей введем бинарное отношение принадлежности. Хост $A$ принадлежит подсети $B$, когда $Adr_A \wedge \max(Msk_A, Msk_B) = Adr_B$. Это же условие справедливо для случая, когда $A$ является подсетью, то есть заданное отношение принадлежности устанавливается для некоторого подмножества множества всех хостов подсети $B$. Формально это отношение определено в предикате $inbound(\text{“}Adr_A/Msk_A\text{”}, \text{“}Adr_B/Msk_B\text{”})$.

Условия предиката $subnet$ в программном коде учитывают случай, когда маска подсети равна 32 ($2^{32} - 1$ в длинной записи), и подсеть фактически вырождается в хост. Условия предиката $inbound$ в программном коде так же учитывают вырожденный случай широковещательного адреса, когда часть адреса хоста, не принадлежащая маске подсети, имеет максимальное значение $Adr \wedge$

$Msk = 2^{32-S} - 1$. Широковещательный адрес подразумевает связь со всеми хостами подсети и не может отождествляться с конкретным хостом.

Поскольку вычислительная сеть по своему определению подразумевает связь между ее узлами, на множестве объектов моделируемой сети введем отношение связности, которое определим по следующим правилам:

1) Узел $A$ связан с самим собой;

2) Если узлы $A$ и $B$ принадлежат одной подсети, то они связаны (обобщение правила 1);

3) Узлы $A$ и $B$ связаны, если между ними существует маршрут, то есть они находятся в маршрутизируемых подсетях, и существуют разрешающие правила межсетевой защиты (об этих условиях далее).

На практике маршрутизируемыми называют такие подсети, для которых существуют соответствующие записи в таблицах маршрутизации – специальные на сетевых устройствах (маршрутизаторах), которые связывают различные подсети между собой. Подсети $A$ и $B$ считаются маршрутизированными в случаях когда:

1) существует запись в таблице маршрутизации, связывающая эти подсети друг с другом;

2) существует запись в таблице маршрутизации, связывающая подсеть $A$ с некоторой подсетью $C$, которая маршрутизируема с подсетью $B$.

В рамках этих допущений маршрутизацию между подсетями в модели можно считать симметричной, т.е. записи в таблицах маршрутизации работают одинаково в обе стороны. Это осознанное упрощение рассуждений, при построении модели будем считать, что внутри корпоративной вычислительной сети маршрутизация отлажена, на сетевом оборудовании присутствуют все необходимые записи, и ошибки настройки оборудования исключены. В действительности, маршрутизация как отношение на множестве подсетей несимметрична, и среди записей в таблицах на разных маршрутизаторах должны присутствовать маршруты в обе стороны.

Необходимо также отметить, что если подсети $A$ и $B$ маршрутизируемы и подсеть $C$ принадлежит подсети $A$, то $C$ маршрутизируема с $B$. Исходя из этого

замечания, понятие маршрутизации подсетей можно так же применять в отношении хостов сети без нарушения общности рассуждений.

### 3.2.2 Формирование графа вычислительной сети

В предложенной модели сети правила маршрутизации определяются через тривиальный предикат (факт – в терминах Prolog) $edge(node_1, node_2)$, $node_i$ где – есть узел сети (хост или подсеть), который описывает пару маршрутизируемых узлов. На основе правил маршрутизации топология сети в рамках модели может быть изображена в виде графа, где множество вершин составляют пары $node_i(Adr_i/Msk_i)$, а множество ребер – факты $edge_j(node_{i1}, node_{i2})$. На рисунке 7 приведен пример представления сети в форме графа.

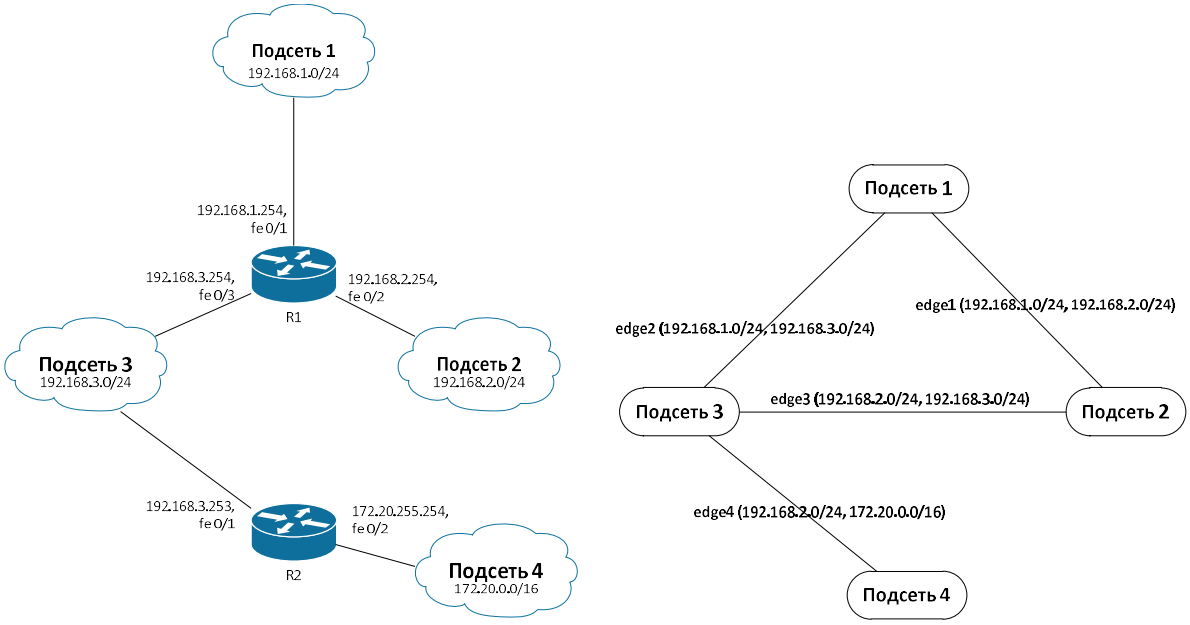



Рисунок 7 – Представление сети в виде графа.

Количество вершин $|V|$ определяется числом различных подсетей, указанных в правилах маршрутизации, а количество ребер $|E|$ можно вычислить исходя из количества записей в таблице маршрутизации на каждом маршрутизаторе по формуле (20).

$$|E| = \sum_{i=1}^{n} \frac{m_i - 1}{2} \cdot m_i \,, \tag{20}$$

где $m_i$ – количество записей на маршрутизаторе $R_i$. В тривиальном случае, то есть, когда маршрутизатор располагает записью только об одной сети ($m_i = 1$), граф сети будет состоять из единственной вершины, и ребер в нем не будет, т.е. $|E| = \frac{m_i - 1}{2} \cdot m_i = \frac{1-1}{2} \cdot 1 = 0$. Этот факт можно считать базой для применения математической индукции. Если предположить, что формула (20) справедлива для случая $m_i = k - 1$, то добавление еще одной записи на маршрутизаторе приведет к появлению в графе сети $k$-й вершины, связанной с каждой из уже существующих. То есть помимо появления новой вершины в графе появится $E' = k - 1$ новых ребер, и общее число ребер $|E|$ можно будет представить как

$$|E| = |E_{k-1}| + E' = \frac{k-1-1}{2} \cdot (k-1) + k - 1 =$$
$$= \frac{k-2}{2} \cdot k - \frac{k-2}{2} + k - 1 = \frac{k}{2} \cdot k - k - \frac{k}{2} + 1 + k - 1 =$$
$$= \frac{k}{2} \cdot k - \frac{k}{2} = \frac{(k-1)}{2} \cdot k, \tag{21}$$

где $|E_{k-1}|$ – количество ребер в графе сети с $k - 1$ вершинами.

Рассуждения, изложенные в (21) справедливы для записей на каждом маршрутизаторе в сети, общий граф сети строится из графов подсетей путем их соединения по общим вершинам (подсетям). Таким образом, количество ребер в графах подсетей – есть величины, не зависящие друг от друга, а значит, вычислить общее количество ребер в графе сети можно простым суммированием. Из вышеизложенного следует, что формула (20) справедлива.

### 3.2.3 Управление доступом хостов на уровне сетевого взаимодействия

Разделение корпоративной сети на независимые сегменты – подсети – позволяет структурировать ее и сделать сеть информационных потоков более

упорядоченной. Для организации управления взаимодействием подсетей и отдельных узлов применяются комплексы программных и аппаратных средств для фильтрации сетевых пакетов – межсетевые экраны (МЭ). Управление сетевым трафиком, проходящим через МЭ, осуществляется в соответствии с заданными правилами. Эти правила имеют общий вид $fw\_rule$(<Императив>, <Источник>:<Порт$_{И}$ >, <Назначение>:<Порт$_{Н}$ >).

Компоненты Источник и Назначение представляют собой адреса узлов сети, определяющие начальную и конечную точки передачи пакетов данных, пакеты передаются от узла Источника к узлу Назначения. В рамках модели принято считать, что эти параметры удовлетворяют условиям предиката $node$. Императив определяет действия, выполняемые на МЭ при прохождении фильтруемого пакета, и может принимать два значения: $allow$ – пропустить пакет данных, $deny$ – заблокировать пакет. Порт является параметром протоколов TCP и UDP, позволяющим разделять пакеты данных для различных приложений на одном узле сети и так же применяется в формировании правила (вид протокола на данном этапе разработки модели сети не учитывается). Параметр Порт принимает численное значение от 1 до 65535. В структуре правила МЭ параметр Порт задается в общем случае списком значений портов TCP/UDP, который строится путем простого перечислением либо диапазоном значений. В рамках модели список портов описан с помощью предикатов

1) $port(P)$ – одиночный порт, лежащий в промежутке допустимых значений;

2) $port\_range(P)$ – есть диапазон портов: два значения одиночного порта, разделенных специальным символом и обозначающих левую и правую границы диапазона, при том левая граница всегда меньше правой;

3) $port\_any(\,)$ – обобщение диапазона портов до всего множества возможных значений (в теле правила обозначается словом «*any*»);

4) $port\_pare(P)$ – пара портов: структура, состоящая из двух частей – правая часть пары портов может являться одиночным портом либо диапазоном портов, а левая часть – одиночным портом, диапазоном либо парой портов.

Таким образом, в рамках модели параметр Порт правила МЭ может быть представлен единственным значением (в виде одиночного порта или диапазона портов), либо структурой сложенных друг в друга списков из двух элементов.

Отношение связности на множестве узлов дополнено учетом правил МЭ в соответствии со следующими принципами:

1) Правила МЭ учитываются на всем множестве узлов сети независимо от того, где именно в топологии сети установлены МЭ, поэтому для любых узлов из разных подсетей должно существовать правило межсетевого экранирования. По умолчанию, то есть, когда правило МЭ отсутствует, принято считать, что канал связи между узлами запрещен.

2) Правила МЭ имеют друг перед другом приоритет, в конфигурации устройства они задаются списком, и приоритет определяется очередностью правила в этом списке. Поскольку в рамках модели правила неупорядочены в абстракции данных, приоритетными считаются запрещающие правила.

## 3.3 Система управления ресурсами в клиент-серверной системе на основе доверия

В данном разделе будет описана модель системы управления, реализующая разработанный автором метод управления ресурсами сервера в клиент-серверной системе на основе оценки доверия к клиентам. В системе используются технические решения, обеспечивающие метод необходимой информацией для проверки критериев доверия и контроля состояния канала связи между клиентом и сервером системы, поэтому в ряде рассуждений она может также называться технической моделью. Система представляет собой надстройку над некоторой существующей инфраструктурой корпоративной информационной системы.


Рисунок 8 – Исходная структурная схема клиент-серверной системы

Рассмотрим в качестве исходной классическую схему клиент-серверной системы и уточним состав и значение ее блоков (схема приведена на рисунке 8):

– клиентом представляется некоторый оконечный узел сети (хост), на рисунке в качестве примера указана ПЭВМ;

– сервер представляет собой некоторый разделяемый клиентами ресурс, доступ к которому осуществляется посредством канала связи;

– канал является совокупностью технических средств сетевой коммуникации (коммутаторы, маршрутизаторы, линии связи), объединенных в ЛВС предприятия и устройств управления (фильтрации) сетевого трафика – межсетевых экранов.

Принято считать, что сетевая инфраструктура предприятия использует технологии на основе стека протоколов TCP/IP, средства управления межсетевым взаимодействием располагаются таким образом, что получают весь сетевой трафик. Данное условие выполняется, когда средство управления располагается в непосредственной близости (с точки зрения топологии сети) к серверу системы. В корпоративных ЛВС, где применяется разделение сети на отдельные сегменты и серверы отделены таким образом от клиентских узлов, достаточно расположить МЭ на границе сетевого сегмента сервера. В случае, когда такое расположение МЭ невозможно либо к категории клиентов относятся также другие серверы, расположенные в том же сетевом сегменте, следует выбирать МЭ соответствующего типа [79] и размещать его непосредственно на уровне узла сервера.

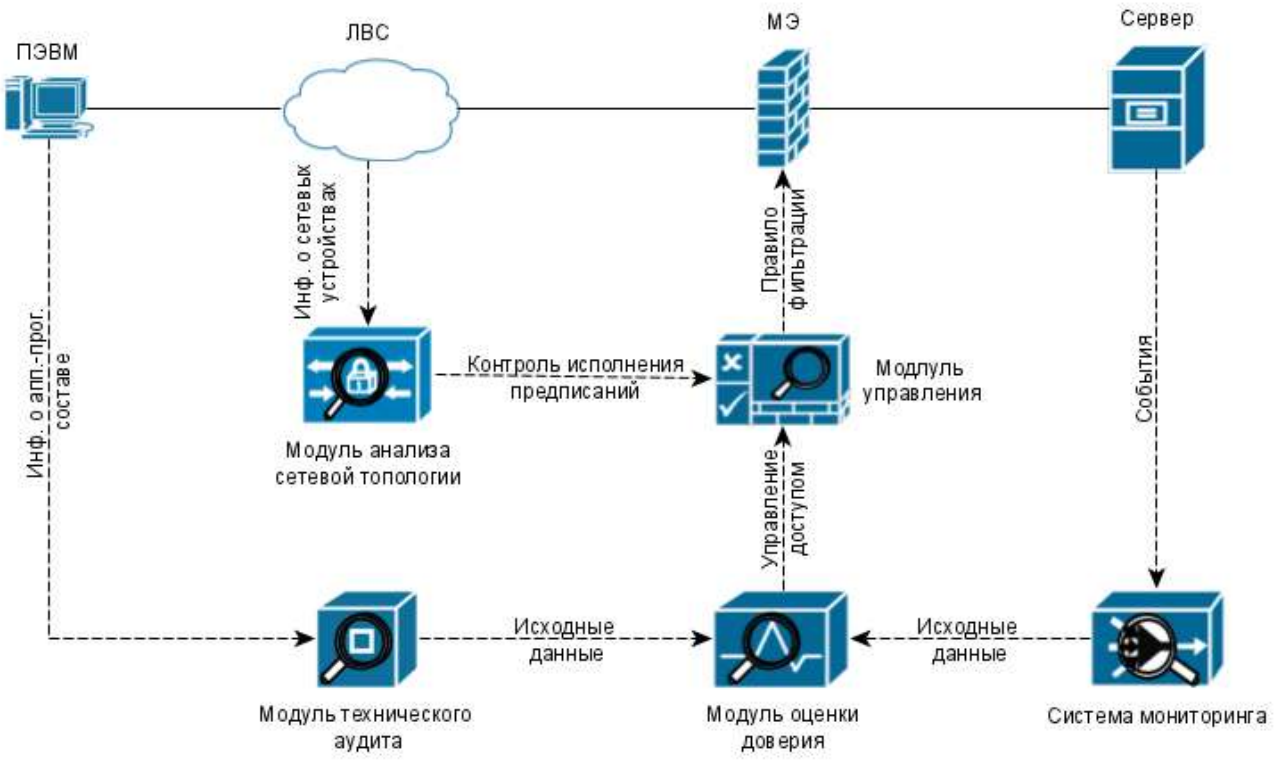



Рисунок 9 – Схема системы управления доступом на основе оценки доверия

Для реализации разработанного метода управления доступом на основе оценки доверия исходную схему клиент-серверной системы необходимо снабдить следующими функциональными блоками (рисунок 9):

— модуль оценки доверия,

— модули технического аудита и мониторинга событий,

— модуль управления устройствами сетевой фильтрации (МЭ),

— модуль анализа сетевой топологии.

Модуль оценки доверия использует информацию о программно-техническом составе хоста клиента и сигналы системы мониторинга событий в качестве исходных данных для оценки доверия к клиенту. Данный модуль реализует основной функционал метода управления доступом: формирование весовых коэффициентов критериев доверия и значения порога доверия, вычисление оценок доверия для клиентов и принятие решения о разрешении (или ограничении) доступа клиента к серверу.

Модуль управления формирует необходимые правила на соответствующем межсетевом экране. Технически модель состоит из набора программ, которые на

основе команд управления от модуля оценки доверия формируют конкретные конфигурации ACL (англ. Access Control List – список доступа) для межсетевых экранов различных производителей и моделей. Для сетевых инфраструктур, где используются комплексные решения одного производителя, данный модуль может быть частично реализован на основе готового продукта централизованного управления устройствами и политиками доступа, таких как [57, 76, 124]. В случае, когда парк устройств разнообразен, либо у владельца системы нет возможности использования коммерческого инструментария (например, в силу высокой стоимости), функционал данного модуля реализуется на базе стандартного хоста под управлением ОС общего назначения с пакетом средств автоматизации. Также модуль получает сигналы ошибок контроля исполнения предписаний от модуля анализа сетевой топологии.

Корректность настройки технических средств контролируется модулем анализа сетевой топологии. Поскольку с точки зрения сетевого взаимодействия доступ клиента к серверу системы фактически эквивалентен наличию между ними открытого канала связи (то есть, не блокируемого ACL соответствующих МЭ) решение об авторизации доступа должно приниматься до момента подключения клиента к серверу. Функционал модуля описан в пункте 3.2 настоящей главы. Технически модуль состоит из системы аккумулирования и хранения конфигураций сетевых устройств, набора трансляторов и непосредственно механизма анализа. Система сбора конфигураций формирует исходные данные для работы всего модуля, это текстовые файлы настроек конкретных МЭ и сетевых устройств, содержащие записи ACL и таблицы маршрутизации, которые затем приводятся к единой нотации механизма анализа. Также модуль получает список недоверенных данный момент времени клиентов, для которых проверяет доступность сервера системы при текущей конфигурации правил МЭ. В случае, если действующие ACL допускают подключение недоверенного клиента к серверу, формируется соответствующих сигнал для модуля управления сетевыми устройствами.

Функционал модуля технического аудита описан в пункте 3.1 настоящей Главы, его задачей является подготовка исходных данных для формирования оценок доверия к клиентам в системе. Модуль системы мониторинга имеет схожую задачу, потому описание их ролей проводится совместно. Оба модуля могут быть построены на базе соответствующих готовых решений, которые, в том числе, имеют варианты, распространяемые под свободными лицензиями (Zabbix, Nagios), т.е. могут быть внедрены без существенных финансовых затрат. Модуль технического аудита обеспечивает модуль оценки доверия сведениями о клиентах для проверки критериев доверия, связанных с программно-техническим составом хоста клиента, модуль мониторинга событий формирует исходные данные для проверки критериев доверия, связанных с активностью клиента в сети, статистическими и иными данными.

### 3.4 Применения результатов исследований на практике

Результаты работы внедрены в ряд корпоративных информационных систем АО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва» (АО «ИСС»), скан-копия справки о внедрении приведена в приложении Б:

— разработанная модель доверия используется для принятия решения о согласовании допуска персонала к работе со специализированными программными средствами;

— метод управления ресурсами на основе оценки доверия внедрен в систему управления доступом к вычислительным ресурсам системы виртуализации графических задач и систему управления конкурентными лицензиями на специальное программное обеспечение;

— также метод применяется в системе мониторинга и управления оборудованием межсетевого взаимодействия уровня ядра корпоративной вычислительной сети.

Получено свидетельство о государственной регистрации программы «Программа анализа связей между узлами корпоративной вычислительной сети», реализующей механизмы построения и анализа сетевой топологии, описанные в

данной главе, получено свидетельство на программу для ЭВМ, копия приведена в приложении А к диссертационной работе.

На основе предложенной модели системы управления доступом разработана концепция распределенной автоматизированной системы, получено положительное заключение ФСТЭК России от 18.11.2016 № 1398 о возможности ее применения для обработки служебной информации. К сожалению автора, письмо с заключением имеет ограничительную пометку и не может быть опубликовано.

В работах [83, 111] рассматривается способ применения компонентов разработанной модели системы управления ресурсами, реализующих механизмы автоматизированного сбора контекстной информации о клиентах корпоративной информационной системы и ее ресурсах в задаче формирования цифровых водяных знаков для маркирования фотодокументов при организации корпоративного электронного архива. Данный подход к управлению доступом на основе оценки доверия использован также при исследовании способов организации обработки служебной информации в корпоративной локальной сети [84].

## 3.5 Выводы

В главе описана модель структуры ЛВС, которая реализует базовые принципы сетевого взаимодействия оконечных и коммутационных узлов в вычислительных сетях TCP/IP. Модель является основой для анализа сведений о взаимосвязях реальных абонентов корпоративных ЛВС, позволяет имитировать состояние каналов связи с учетом действующих правил взаимодействия. Эта характеристика модели является ключевым достоинством в сравнении с существующими методами компьютерного моделирования вычислительных сетей, основанных на применении процедурных языков программирования и реализующих логику взаимодействия внутри сети лишь косвенно.

С учетом применяемых методов логического программирования развитие и усложнение модели будет осуществляться без вмешательства в уже существующую структуру путем добавления новых отношений на множестве ее

объектов и правил взаимодействия между ними, необходимых для реализации нужных свойств реальной корпоративной вычислительной сети. Так в структуру модели может быть добавлен функционал технологий организации взаимодействия с сетями общего пользования, такие как NAT (англ. Network Address Translation – технология трансляции сетевых адресов), а также случаи, когда конечный узел сети имеет несколько сетевых интерфейсов.

Совместно с логической моделью анализа связей узлов вычислительной сети в главе описана архитектура и состав модуля технического аудита, который обеспечивает владельца системы исходными данными для формирования оценки доверия к клиентам.

В заключительном разделе главы описана модель системы управления ресурсами в клиент-серверной системе, реализующая функционал разработанного метода управления на основе оценок доверия к клиентам. Модель представляет надстройку над существующей архитектурой клиент-серверного типа, что облегчает интеграцию в функционирующие клиент-серверные системы, поскольку не требуется прерывания их работы, изменения режима эксплуатации или структуры.

# Глава 4. Оценка эффективности метода управления ресурсами в клиент-серверной системе на основе доверия

В настоящей главе описана вероятностная модель доступа клиентов к серверу в клиент-серверной системе с ограниченными ресурсами сервера, которая позволяет оценить эффективность используемого метода управления ресурсами. Как наиболее подходящий для решения таких задач, как показано в [14, 72, 73], выбран аппарат теории систем массового обслуживания. В модели показан механизм влияния заданного метода управления доступом клиента к ресурсам сервера на характеристики эффективности системы, в частности, на вероятность обслуживания заявок от клиентов доступа в устоявшемся режиме работы системы.

Для описанной модели определен показатель эффективности и связанный с ним критерий повышения эффективности управления доступом клиентов к ресурсам сервера и проведено исследование эффективности разработанного метода управления на основе доверия по этому критерию на примере действующей информационной системы предприятия.

## 4.1 Показатель эффективности управления доступом к ресурсам

Согласно ГОСТ Р ИСО 9000-2008 [54] эффективностью называют связь между достигнутым результатом и использованными ресурсами. В контексте диссертационной работы к использованным ресурсам относятся вычислительные и программные ресурсы сервера системы, посредством которых клиенты системы выполняют производственную задачу, общий итог решения данной задачи составляет достигнутый результат. Считается, что на качество результата влияет соблюдение технологического процесса решения задачи, который в том числе включает технические условия использования ресурса сервера. Соответственно, более качественный результат решения производственной задачи будет ожидаем от клиентов, в большей степени соответствующих установленным техническим условиям.

Принимая общий случай распределения ресурсов сервера (когда клиенты получают доступ на конкурентной основе), показателем эффективности целесообразно считать вероятность доступа к ресурсу сервера для клиентов, наиболее соответствующих техническим условиям.

В контексте данной диссертационной работы степень соответствия клиента $X$ клиент-серверной системы $S$ техническим условиям определяется на основе оценки доверия $T(X)$, иными словами, показателем эффективности управления доступом в клиент-серверной системе принято считать величину $P(X_T)$ оценки вероятности доступа доверенных клиентов $X_T$ к ресурсу сервера $S$.

Соответственно, критерием повышения эффективности управления ресурсами сервера при использовании метода управления доступом к ним будем считать выполнение условия (22)

$$\tilde{P}(X_T) > P(X_T), \tag{22}$$

где $\tilde{P}(X_T)$ – показатель эффективности управления ресурсами сервера при использовании исследуемого метода управления доступом.

## 4.2 Вероятностная модель доступа клиентов к ресурсам в клиент-серверной системе

### 4.2.1 Исходные данные для построения модели

Математический аппарат вероятностной модели доступа клиента к ресурсам построен на основе многоканальных систем массового обслуживания замкнутого типа с нулевой очередью и отказами. Исследования в данной области представлены в работах Р.Ф. Гильмутдинова [16, 15, 17], также моделирование информационных систем через аппарат СМО рассмотрены в работах[36, 55, 81].

Ограниченный (дефицитный) ресурс сервера клиент-серверной системы описан через число доступных каналов СМО. Под подачей заявки от клиента подразумевается совокупность действий:

1) открытие TCP-сессии клиента с сервером;

2) авторизация доступа клиента к ресурсу сервера.

Обе составляющие заявки представляют собой неделимые процедуры и не предполагают ожидание. В этом смысле обработка заявки должна происходить в момент ее поступления, поэтому очереди в данной модели не рассматриваются.

Таким образом, клиент-серверная информационная система $S$ имеет ограниченный вычислительный ресурс для обслуживания клиентов $X$ и позволяет осуществлять одновременное подключение не более чем $N_S = \omega$ клиентам. В свою очередь $X$ состоит из ограниченного и известного числа терминальных узлов $N_X = \chi$, каждый из которых создает простейший поток заявок на доступ к S интенсивности $\lambda$ и освобождает занятый канал с интенсивностью $\mu$. Считаем, что $N_X \geq N_S$, и в случае, когда все $N_S$ каналов заняты, все поступающие заявки на доступ получают отказ и немедленно возвращаются обратно в источник, т.е. $P_{\text{ожид}} = 0$.

### 4.2.2 Описание модели в стандартном режиме работы клиент-серверной системы

Стандартными условиями работы системы (или стандартным режимом работы) будем называть работу системы без учета показателя доверия к клиенту при получении заявки от него, т.е. без применения разработанного метода управления на основе оценки доверия.

Граф состояний системы имеет весьма общий вид и приведен на рисунке 10. Индексы состояний системы $S_i$ соответствуют занятым каналам. Клиенты генерируют поток заявок самостоятельно и независимо друг от друга, общий поток заявок формируется из суммы потоков заявок от всех клиентов.

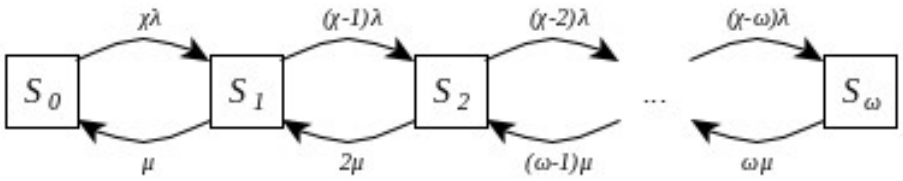



Рисунок 10 – Граф состояний модели СМО в стандартном режиме работы клиент-серверной системы

Расчет вероятностей произвольного состояния системы $P_k$ выполним через факториальный многочлен по формуле (23)

$$P_k = \frac{\chi^{[k]}}{k!}\rho^k P_0 = C_\chi^k \rho^k P_0, \tag{23}$$

где $\chi^{[k]}$ – факториальный многочлен степени $k$, $C_\chi^k$ – биномиальный коэффициент из $\chi$ по $k$. Тогда, с учетом суммарной вероятности состояний системы, можно уточнить формулу для состояния $P_k$.

$$\sum_{i=0}^{\omega} P_i = P_0 \sum_{i=0}^{\omega} C_\chi^i \rho^i = 1 \Rightarrow P_k = C_\chi^k \rho^k \left( \sum_{i=0}^{\omega} C_\chi^i \rho^i \right)^{-1}. \tag{24}$$

Из обобщенной формулу (24) вероятности состояния системы можно выразить среднее количество одновременно занятых каналов $\bar{\omega}$.

$$\bar{\omega} = \sum_{k=0}^{\omega} kP_k = \sum_{k=0}^{\omega} (\chi - \chi + k)P_k = \chi \sum_{k=0}^{\omega} P_k - \sum_{k=0}^{\omega} (\chi - k)P_k =$$

$$= \chi - (\chi - \omega)P_\omega - \sum_{k=0}^{\omega-1} (\chi - k)P_k = \chi - (\chi - \omega)P_\omega - \sum_{k=0}^{\omega-1} (\chi - k)\, C_\chi^k \rho^k P_0 =$$

$$= \chi - (\chi - \omega)P_\omega - \frac{\bar{\omega}}{\rho} \Rightarrow \frac{\bar{\omega}(1+\rho)}{\rho} = \chi - (\chi - \omega)P_\omega \;\Rightarrow$$

$$\bar{\omega} = \frac{\rho}{1+\rho}(\chi - (\chi - \omega)P_\omega). \tag{25}$$

Исходя из определения расчет абсолютной пропускной способности $A$ системы $S$ может быть выполнен по формулам (26).

$$A = \lambda(\chi - \bar{\omega})P,$$

$$A = \sum_{k=0}^{\omega-1} \lambda_k P_k = \lambda \sum_{k=0}^{\omega-1} (\chi - k)P_k = \lambda\left(\sum_{k=0}^{\omega} (\chi - k)P_k - (\chi - \omega)P_\omega\right) = \\ = \lambda(\chi - \bar{\omega} - (\chi - \omega)P_\omega). \quad (26)$$

где $P = P_{\text{готов}}$ – вероятность готовности системы S к обслуживанию заявок от $X$.

Из соотношений (26) можно записать $P$ через выражение (27).

$$P = \frac{\chi - \bar{\omega} - (\chi - \omega)P_\omega}{\chi - \bar{\omega}} = 1 - \frac{\chi - \omega}{\chi - \bar{\omega}} P_\omega. \quad (27)$$

Система уравнений (28), составленная из формул (24), (25) и (27) полностью описывает вероятность $P = P_{\text{готов}}$ системы $S$ к обслуживанию заявок от клиентов доступа $X$.

$$\begin{cases} P = 1 - \dfrac{\chi - \omega}{\chi - \bar{\omega}} P_\omega, \\ \bar{\omega} = \dfrac{\rho}{1 + \rho}(\chi - (\chi - \omega)P_\omega), \\ P_\omega = C_\chi^\omega \rho^\omega \left(\sum_{i=0}^{\omega} C_\chi^i \rho^i\right)^{-1}. \end{cases} \quad (28)$$

4.2.3 Описание модели при использовании разработанного метода

Применение разработанного метода управления ресурсами сервера системы $S$ на основе оценки уровня доверия $T(X)$ к клиентам $X$ ограничивает их возможность получения доступа к системе согласно условию (16). Учитывая, что при проверке доверия клиент определяется некоторой совокупностью своих изменяемых характеристик $X = (x_1, x_2, \dots, x_n)$, не зависимых от других клиентов и состояния системы $S$, можно считать успешный результат проверки доверия к клиенту в текущий момент времени случайным событием с вероятностью $P_T$, определяемой порогом доверия Z. При этом для клиента отказ по итогу проверки

уровня доверия равнозначен отказу в обслуживании при полной загрузке системы (в состоянии $S_\omega$). Граф состояний изображен на рисунке 11.

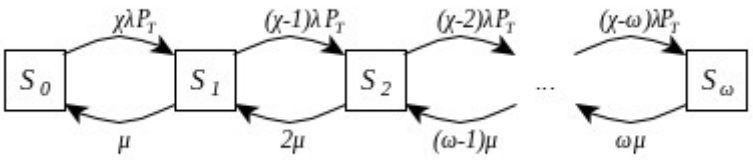



Рисунок 11 – Граф состояний модели с учетом влияния оценки доверия к клиенту на его доступ к серверу

По аналогии с формулой (23) вероятность $\tilde{P}_k$ состояния системы $S_k$ в режиме проверки доверия к клиентам может быть выведена по формуле (29).

$$\tilde{P}_k = \frac{\chi^{[k]}}{k!}\rho^k P_0 = C_\chi^k \rho^k P_T^k P_0 \tag{29}$$

При этом, учитывая формулу (23), справедливо равенство $\tilde{P}_k = P_T^k P_k$. Если считать $\tilde{\rho} = \rho P_T$, то общая формула вероятности $\tilde{P}_k$ состояния системы $S_k$ из (24) и (29) будет иметь вид

$$\tilde{P}_k = P_T^k P_k = C_\chi^k \rho^k P_T^k \left(\sum_{i=0}^{\omega} C_\chi^i \rho^i P_T^i\right)^{-1} = C_\chi^k \tilde{\rho}^k \left(\sum_{i=0}^{\omega} C_\chi^i \tilde{\rho}^i\right)^{-1}. \tag{30}$$

С учетом формулы (30) можно записать систему уравнений (28) для $\tilde{P}$ вероятности готовности системы $S$ к обработке заявок на доступ от клиентов $X$ с использованием метода управления доступом на основе проверки уровня доверия к клиенту в следующем виде.

$$\begin{cases} \tilde{P} = 1 - \dfrac{\chi - \omega}{\chi - \overline{\omega}} \tilde{P}_{\omega}, \\ \overline{\omega} = \dfrac{\tilde{\rho}}{1 + \tilde{\rho}} \left(\chi - (\chi - \omega)\tilde{P}_{\omega}\right), \\ \tilde{P}_{\omega} = C_{\chi}^{\omega} \tilde{\rho}^{\omega} \left( \sum_{i=0}^{\omega} C_{\chi}^{i} \tilde{\rho}^{i} \right)^{-1}, \\ \tilde{\rho} = \rho P_T. \end{cases} \quad (31)$$

## 4.3 Оценка эффективности применения метода управления ресурсами

### 4.3.1 Критерий эффективности метода управления ресурсами

Из системы уравнений (28) видно, что вероятность обслуживания сервером системы $S$ к заявок от клиентов $X$ (вероятность доступа клиентов к серверу) полностью определяется их количеством $N_X = \chi$, общим числом каналов $N_S = \omega$ и коэффициентом загрузки $\rho = \lambda/\mu$. Учитывая, что вычислительный ресурс системы определяется ее программно-техническим составом, можно полагать $N_S = \omega = const$. Также можно считать $\rho = const$, поскольку интенсивность запросов на доступ от клиентов и продолжительность их пребывания в системе определяется спецификой решаемых посредством нее задач. Из этих соображений можно условно считать вероятность доступа к серверу функцией от числа активных клиентов системы $P = P(\chi) : \mathbb{N} \to [0; 1]$.

В свою очередь, вероятность $P_T$ прохождения проверки уровня доверия к клиентом зависит от выбора значения порога доверия Z. Оценку вероятности $P_T$ можно непосредственно связать с Z исходя из его определения, и тогда можно полагать $P_T = P_T(\mathrm{Z}) : [0; 1] \to [0; 1]$, $\tilde{P} = \tilde{P}(\chi, \mathrm{Z}) : \mathbb{N} \times [0; 1] \to [0; 1]$.

Принято считать показателем эффективности применения метода управления ресурсами величину $\Delta P$, определяемую как отношение разности оценок вероятности доступа клиента к серверу в одном и другом режимах работы к значению оценки вероятности доступа в обычном режиме работы. Формальная запись $\Delta P$ приведена в формуле (32).

$$\Delta P = \frac{\left(\tilde{P} - P\right)}{P} \tag{32}$$

4.3.2 Расчет эффективности метода управления ресурсами

4.3.2.1 Исходные данные, описание целевой системы

На практике расчет эффективности $\Delta P$ применения разработанного метода управления ресурсами выполнен для корпоративной системы виртуализации графических вычислительных ресурсов. Система имеет клиент-серверную архитектуру, сервер представляет собой кластер высокопроизводительных серверов виртуализации (гипервизоров) с мощными аппаратными модулями обработки графических данных (видеоадаптеров), управляемым ресурсом системы является запас вычислительной мощности данных адаптеров, который весьма ограничен в силу высокой стоимости и сложности организации конкурентного использования. В силу особенностей основной деятельности рассматриваемого предприятия (разработка и проектирование в области ракетно-космической техники) графические вычисления являются важной частью производственного процесса, потому вычислительный ресурс высокоэффективных графических процессоров весьма востребован персоналом конструкторских направлений. Данные обстоятельства делают этот ресурс системы виртуализации дефицитным с точки зрения конкурентного использования пользователями (клиентами).

Доступ к ресурсу осуществляется через гостевые ОС, укомплектованные виртуальными графическими адаптерами. Клиент представляет собой совокупность следующих сущностей: работника предприятия, который выполняет производственную задачу, и ПЭВМ (хоста), подключенного к ЛВС предприятия. Клиент подключается к серверу управления системы виртуализации через ЛВС, устанавливая стандартную TCP-сессию, проходит авторизацию на подключение к графической виртуальной машине и далее, если такая машина есть на сервере, подключается к ней через программные интерфейсы программного обеспечения сервера системы. Встроенные механизмы системы виртуализации управления доступом клиента к вычислительным мощностям сервера (виртуальным машинам)

построены на классических моделях избирательного управления доступом на основе дискреционного и ролевого подходов, рассмотренных в пункте 1.3.1 диссертационной работы, которые предполагают строго детерминированные правила разграничения доступа: если клиент располагает необходимыми полномочиями (в виде соответствующей роли или прямого разрешения), сервер обязан предоставить ему доступ к ресурсу при его наличии, отказ на доступ со стороны сервера возможен в случае исчерпания ресурса (все графические виртуальные машины заняты) либо при отсутствии необходимых полномочий у клиента.

Исходные данные для расчетов приведены в таблице 2.

Таблица 2 – Исходные данные для расчета эффективности метода

| Параметр | Обозначение | Значение | Примечание |
|---|---|---|---|
| Общее количество клиентов | $\chi$ | 400 | Округленное количество потенциальных клиентов в системе; составляют генеральную совокупность для расчетов |
| Вычислительный ресурс системы | $\omega$ | 100 | Вычислительный ресурс системы обеспечивает одновременную работу 25% от общего числа потенциальных клиентов |
| интенсивность обращений клиентов | $\rho$ | 4 | Интенсивность обращений клиентов к системе превышает в 4 раза интенсивность освобождения ресурса |
| Количество критериев доверия | $\|M\|$ | 13 | Общее количество критериев доверия, используемое для оценки доверия к клиентам |
| Количество экспертов | $y$ | 4 | Количество экспертов, участвующих в формировании матрицы $\tilde{A}$ нечеткого отношения важности критериев |
| Порог доверия, вариант 1 | $\mathrm{Z}_1$ | 0,84 | Жесткий вариант порога доверия к клиенту, определен как $1-(\mathrm{E}+\varepsilon)$; значение получено на основании расчетов таблицы 3 |
| Порог доверия, вариант 2 | $\mathrm{Z}_2$ | 0,61 | Мягкий вариант порога доверия к клиенту, определен как $1-\|w\|\cdot \mathrm{E}$; значение получено на основании расчетов таблицы 3 |

Количественные данные об общем числе пользователей $\chi$ и имеющемся ресурсе сервера системы $\omega$ составлены на основе официального реестра

зарегистрированных пользователей системы и информации из технической документации на систему и потому соответствуют действительности. Данные о числе клиентов округлены в меньшую сторону, а о ресурсе сервера, напротив, в большую, поэтому результаты вычислительного эксперимента будут не хуже реальных показателей.

Коэффициент загрузки системы $\rho$ подобран на основе статистических данных о средней частоте обращений пользователей системы к серверу и средней продолжительности работы пользователя с виртуальной машиной в течение рабочего дня.

Перечень критериев доверия $M$ взят на основе реально используемого перечня с применением обезличивания по конкретным наименованиям, смысловая часть, раскрывающая суть применяемого критерия сохранена. Таким образом, перечень критериев доверия включает следующие группы критериев:

1) Атрибутные и ролевые характеристики клиента – 3 критерия;

2) Данные о программно-техническом составе хоста клиента – 5 критериев;

3) События систем мониторинга различных типов – 5 критериев.

#### 4.3.2.2 Ранжирование критериев

Ранжирование критериев проводилось с привлечением 10 экспертов, опросные листы и составленные на их основе матрицы парных сравнений критериев доверия приведены в приложении В к диссертационной работе.

По итогам ранжирования экспертами критериев доверия составлена матрица нечеткого отношения предпочтения критериев $\tilde{A}$. Матрица приведена и рассмотрена в пункте 2.1.2 диссертационной работы в рамках исследования задачи выбора способа вычисления весовых коэффициентов $W(M)$, который фактически составляет нормированную шкалу весов для критериев. Результаты расчета весовых коэффициентов приведены в таблице 3.

Таблица 3 – Ранжирование критериев доверия

| Критерий | Содержание критерия | Вес |
|---|---|---|
| $m_1$ | Способ управления учетной записью клиента | 0,137 |
| $m_2$ | Сведения о допуске клиента к работам класса 1 | 0,024 |
| $m_3$ | Сведения о допуске клиента к работам класса 2 | 0,024 |
| $m_4$ | Наличие набора 1 программного обеспечения клиента | 0,124 |
| $m_5$ | Наличие набора 2 программного обеспечения клиента | 0,134 |
| $m_6$ | Наличие набора 1 технических средств клиента | 0,093 |
| $m_7$ | Наличие набора 2 технических средств клиента | 0,092 |
| $m_8$ | Наличие набора 3 технических средств клиента | 0,049 |
| $m_9$ | Наличие событий типа 1 системы безопасности | 0,081 |
| $m_{10}$ | Наличие событий типа 2 системы безопасности | 0,054 |
| $m_{11}$ | Наличие событий типа 3 системы безопасности | 0,034 |
| $m_{12}$ | Наличие событий типа 1 системы мониторинга | 0,066 |
| $m_{13}$ | Наличие событий типа 2 системы мониторинга | 0,093 |

Выборка клиентов для расчета оценок доверия и применения метода проводилась среди зарегистрированных пользователей рассматриваемой системы, выборка полностью покрывает их общую совокупность.

4.3.2.3 Расчет оценок доверия к клиентам

Расчет оценок доверия к клиентам из выбранной совокупности проведен по общей формуле вычисления оценки доверия, указанной в пункте 2.1.3 главы 2. Результаты расчетов приведены в приложении Г данной диссертационной работы. По результатам расчетов на рисунке 12 изображена столбчатая гистограмма распределения значений оценок доверия к клиентам из заданной выборки с группировкой по значению оценки. На гистограмме столбцы, соответствующие группам клиентов, удовлетворяющих условию доверия (превышающие порог доверия Z), окрашены зеленым цветом, а столбцы с группами недоверенных клиентов окрашены оранжевым цветом. Данное разделение выполнено для значения порога доверия $Z_1 = 0{,}84$, выбранного по строгому условию.

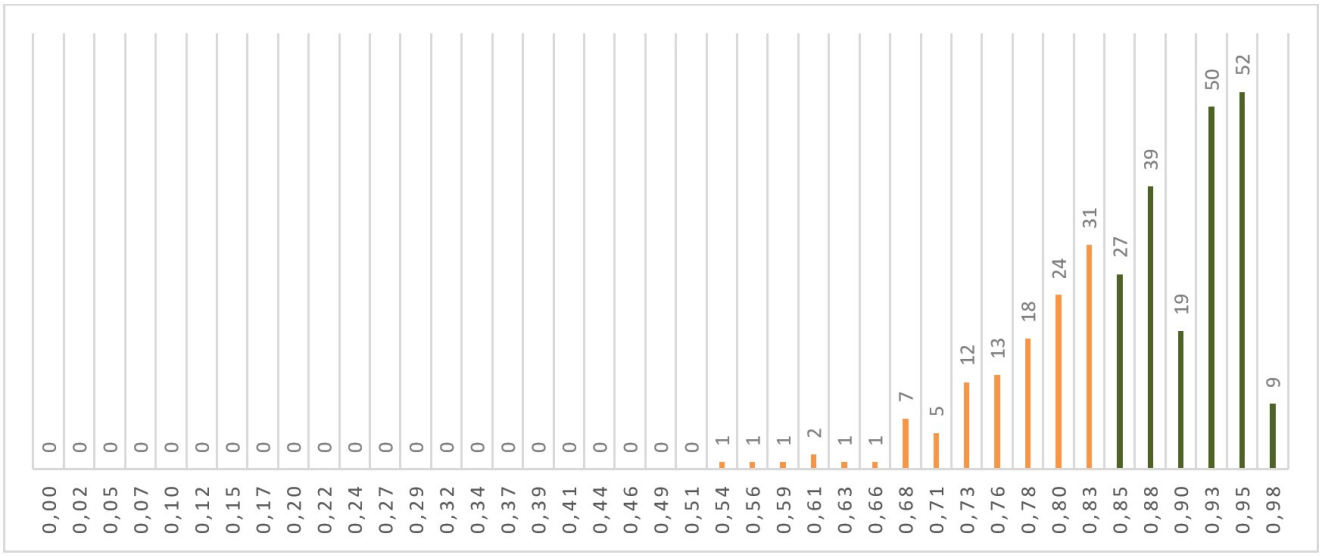



Рисунок 12 – Гистограмма распределения значений оценок доверия к клиентам рассмотренной клиент-серверной системы

Модель доверия предлагает два пограничных варианта выбора значения порога Z, строгий и лояльный, которые опираются на группу критериев доверия с наибольшими показателями веса. Согласно предложенной модели доступа вероятность получения клиентом доступа к серверу помимо состояния сервера зависит также от вероятности доставки заявки надо доступ $P_T$. Для разработанного метода управления на основе оценки доверия эта вероятность, очевидно, определяется значением вероятности получения заявки от доверенного клиента, т.е. $P_T = {\chi_T}/{\chi}$, где $\chi_T$ – количество доверенных клиентов в системе.

Далее рассмотрим все варианты значений порога доверия, покажем зависимость вероятности доверия к клиенту из заданной выборки. В виде графика зависимость показана на рисунке 13. Из рисунка видно, что при значениях порога доверия, ниже варианта по лояльному условию $\mathrm{Z}_2 = 0{,}61$ значение вероятности доверия к клиенту $P_T(\mathrm{Z})$ практически не меняется с изменением значения порога. Это свидетельствует о незначительном влиянии малых значений порога доверия на выделение группы доверенных клиентов из общей совокупности. Затем, как видно на графике, приблизительно до значения порога $\mathrm{Z} = 0{,}83$ наблюдается плавное стабильное снижение значения вероятности доверия к клиенту из выборки. Данное значение близко к расчетному значению порога $\mathrm{Z}_1 = 0{,}84$, выбранного в соответствии со строгим условием. При значениях порога, превышающих $\mathrm{Z}_1$,

изменение значения $P_T(\mathrm{Z})$ изменяются ступенчато, на кривой наблюдаются перегибы.

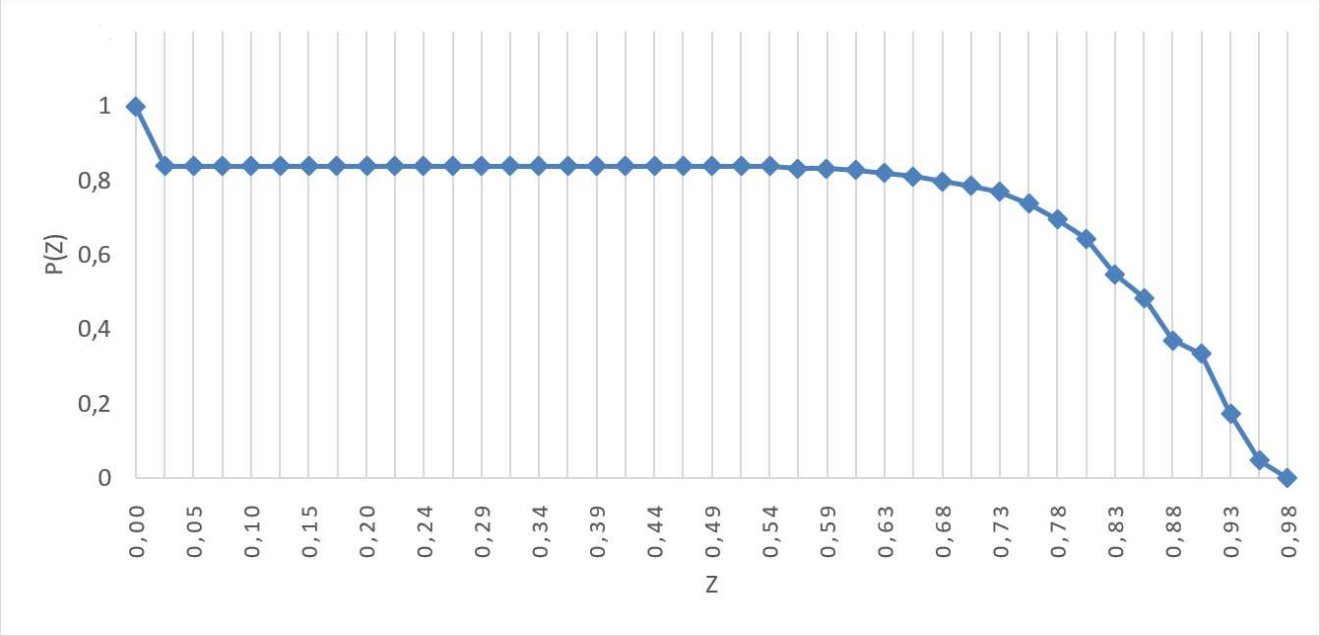



Рисунок 13 – Зависимость вероятности доверия к случайно выбранному клиенту от значения порога доверия

4.3.2.4 Расчет значений показателя эффективности

На основе данных об оценках доверия к клиентам из выборки рассмотрим зависимость значения показателя эффективности: оценки вероятности обслуживания заявок от доверенных клиентов от общего числа активных клиентов в системе. За предельное значение количества клиентов взято значение $\chi = 400$.

Рассмотрим два варианта порога доверия $\mathrm{Z}_1$ и $\mathrm{Z}_2$, выбранные выше, соответствующие строгому и лояльному условиям выбора. Сравним разработанный метод управления с аналогичными известными методами:

1) управление доступом на основе атрибутной модели доступа (ABAC);

2) приоритезация трафика от доверенных клиентов на основе технологий QoS.

Для использования данных методов в предложенной вероятностной модели доступа необходимо рассмотреть изменение вероятности $P_T$ вероятности получения сервером системы заявки от доверенного клиента.

В случае использования атрибутного управления доступом (ABAC) условие отнесения клиента системы к группе доверенных определяется на основе строгого соответствия шаблону атрибутов. Клиентам, не удовлетворяющим шаблону, доступ к серверу блокируется. В контексте принятой модели доверия без дополнительных уточнений можно считать, что такой шаблон задается критериями доверия с наибольшим весом. Обозначим как $\chi_A$ группу клиентов системы, удовлетворяющих шаблону атрибутов доступа в модели ABAC. При этом справедливо утверждение $\chi_T \geq \chi_A$, тогда обозначим как $\Delta\chi_A = \chi_T - \chi_A$ количество доверенных клиентов системы, не удовлетворяющих шаблону атрибутов, этим клиентам доступ к серверу системы будет перманентно ограничен. Тогда вероятность получения сервером запроса от доверенного клиента $P_A$ при использовании модели ABAC можно найти как $P_A = {(\chi_T - \Delta\chi_A)}\Big/{(\chi - \Delta\chi_A)}$.

При использовании технологии QoS для приоритезации запросов от доверенных клиентов имеет место следующая ситуация. Заявки поступают к серверу от всех клиентов системы, однако при поступлении на сервер в один момент времени нескольких заявок от разных клиентов, среди которых будет заявка от доверенного, приоритет будет передан заявке от доверенного клиента. Значение суммарной вероятности для таких ситуаций можно записать как $P_Q = P_T + P_T(1 - P_T) + \cdots + P_T(1 - P_T)^{\chi-1} = P_T \sum_{i=0}^{\chi-1}(1 - P_T)^i$.

Покажем на графике зависимость значения оценки вероятности $\tilde{P}(\chi)$ от числа клиентов в системе для четырех указанных способов управления доступом. Графики приведены на рисунке 14 и отражают следующие варианты:

— Оценка вероятности $P(\chi)$ для системы в стандартным режиме работы;

— Оценка вероятности $\tilde{P}_{\mathrm{Z1}}(\chi)$ при значении порога доверия $\mathrm{Z}_1 = 0{,}84$;

— Оценка вероятности $\tilde{P}_{\mathrm{Z2}}(\chi)$ при значении порога доверия $\mathrm{Z}_2 = 0{,}61$;

— Оценка вероятности $\tilde{P}_A(\chi)$ при использовании модели управления ABAC;

— Оценка вероятности $\tilde{P}_Q(\chi)$ при использовании технологии QoS.

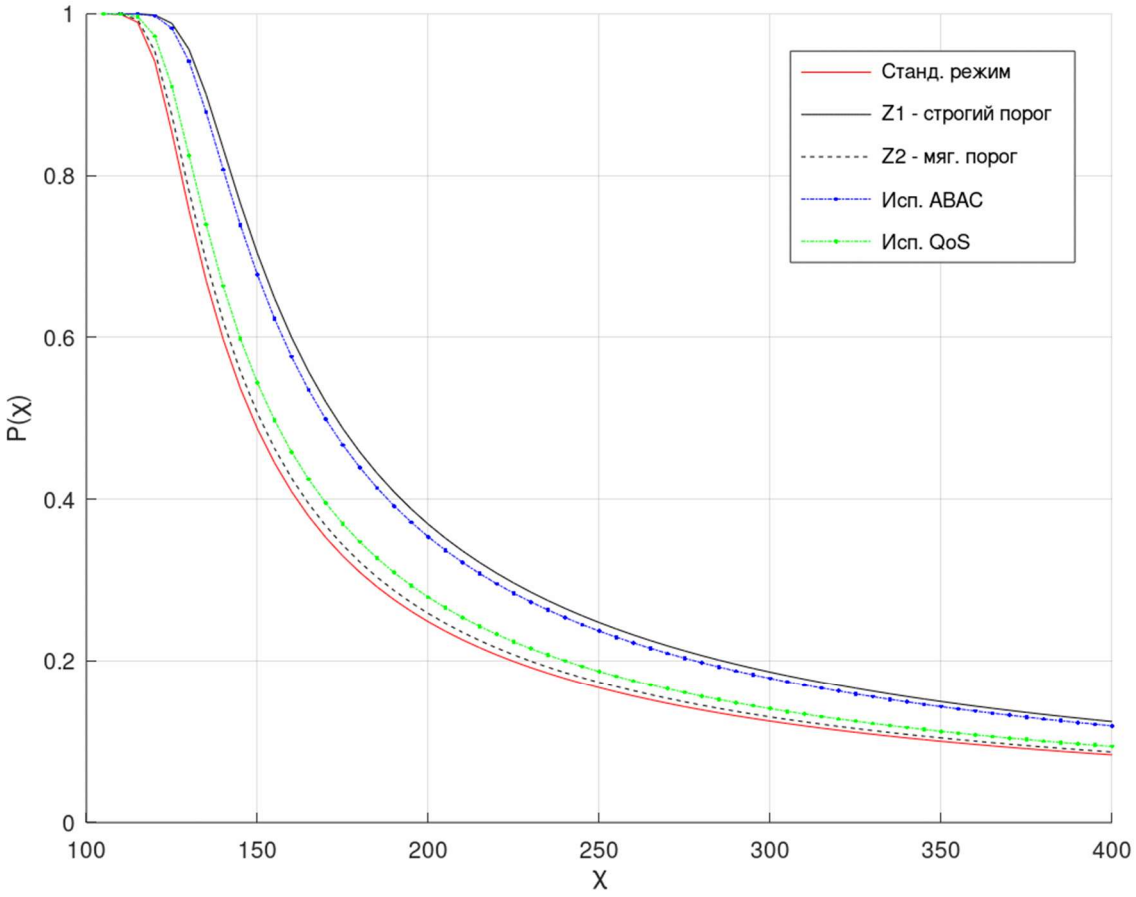



Рисунок 14 – Оценка вероятности доступа клиентов к серверу системы для рассмотренных методов управления

Из рисунка видно, как изменяется положение кривой оценки вероятности обслуживания заявок от доверенный клиентов в условиях учета оценок доверия к клиентам в зависимости от выбора метода управления доступом. Для минимального значения порога доверия $Z_2$, соответствующего наиболее лояльному подходу к оценке доверия, график оценки вероятности $\tilde{P}_{Z_2}(\chi)$ практически совпадает с графиком $P(\chi)$. Напротив, положение графика $\tilde{P}_{Z_1}(\chi)$, соответствующего оценке вероятности готовности системы при наиболее строгом значении порога доверия $Z_1$, заметно отличается от графика $P(\chi)$.

Следует отметить, что кривые, соответствующие методам ABAC и QoS расположены ниже относительно $\tilde{P}_{Z_1}(\chi)$, что говорит большей эффективности метода управления доступом на основе оценки доверия (при использовании

строгого значения порога доверия) в сравнении с аналогичными существующими методами.

Далее сравним значение показателя эффективности $\Delta P$ для выбранных пограничных значений порога доверия $Z_1$ и $Z_2$ для метода управления на основе оценки доверия и двух методов управления на основе ABAC и QoS.

Для наглядности так же построим графики зависимости $\Delta P$ от общего числа клиентов в системе $\chi$, для этого будем пользоваться формулой, приведенной в конце пункта 4.3.1 работы. Графики приведены на рисунке 15. Цвет и начертание линий выбраны по аналогии с графиком оценок вероятности доступа.

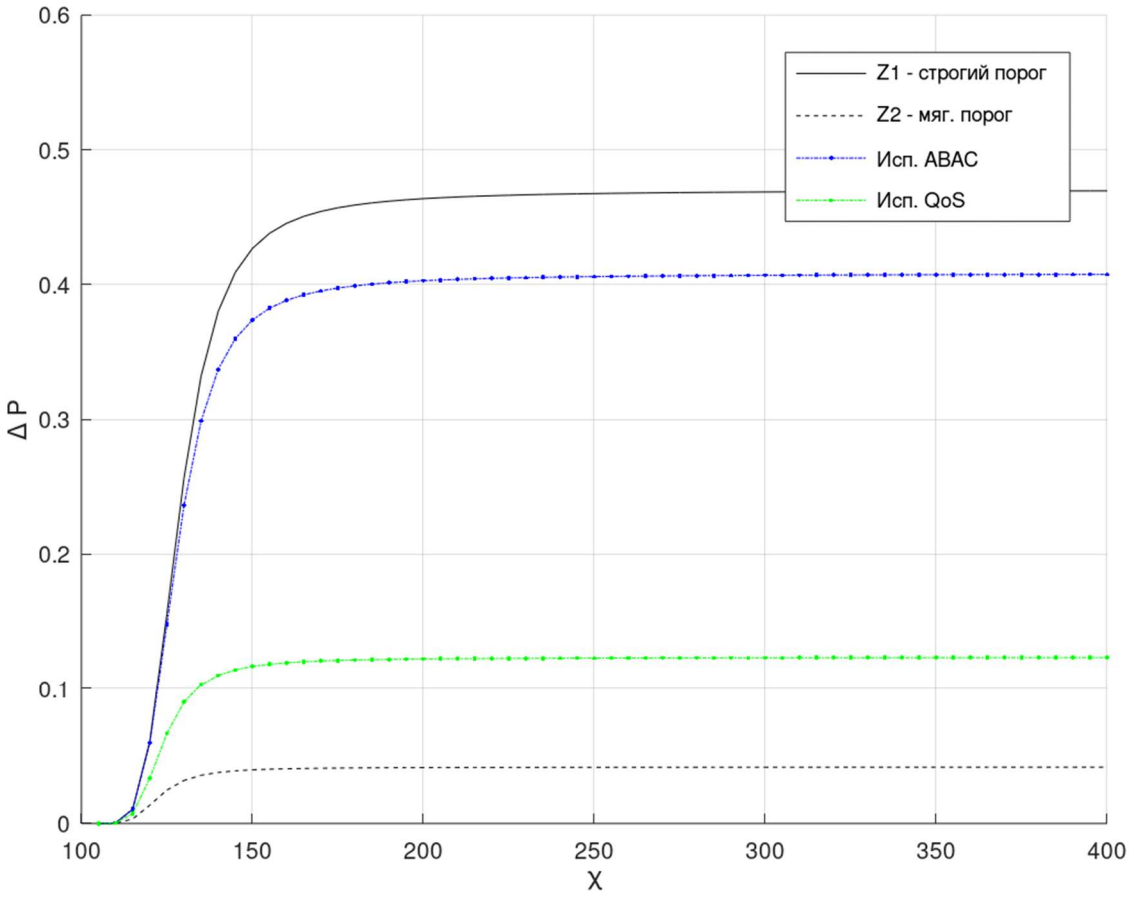



Рисунок 15 – Значения показателя эффективности $\Delta P$ для рассмотренных методов управления

Из рисунка видно, что эффект от применения разработанного метода управления на основе оценки доверия возникает, когда число активных клиентов в системе превышает объем доступного ресурса сервера, до этого момента

применение метода не имеет смысла, т.к. ресурс сервера не является дефицитным, все клиенты получают доступ к ресурсу.

В условиях дефицита ($\chi > \omega$) график показывает рост, который сглаживается и практически прекращается при значениях $\chi > 200$, приблизительное значение $\Delta P$ на этом отрезке для случая $Z_1$ составляет $\lim\limits_{\chi \to 400} \Delta P_{Z_1} = 0{,}47$, а для случая $Z_2$ $\lim\limits_{\chi \to 400} \Delta P_{Z_2} = 0{,}04$. При этом следует отметить, что значение показателя эффективности для метода управления на основе атрибутного подхода (ABAC) составляет $\lim\limits_{\chi \to 400} \Delta P_A = 0{,}41$.

Полученные значения показателя эффективности $\Delta P$ демонстрируют прирост оценки вероятности доступа доверенных клиентов при использовании разработанного метода управления доступом. По существу, можно заключить, что в заданных исходных условиях данная оценка вероятности при использовании метода для доверенных клиентов увеличивается на ~47% в случае выбора строгого значения порога доверия. Прирост обеспечивается, очевидно, ограничением доступа к ресурсу сервера для недоверенных клиентов.

При этом исследование показывает, что разработанный метод при выборе строгого порога доверия более эффективен в сравнении с аналогичными методами на основе атрибутного подхода и технологии приоритезации запросов.

### 4.3.3 Экспериментальные данные

В настоящем пункте будут приведены экспериментальные данные по применению разработанного метода управления доступом в системе виртуализации графических задач АО «ИСС» (далее по пункту – система), рассмотрены значения показателя эффективности для стандартного режима управления доступом и в условиях применения метода.

Для оценки эффективности метода по выбранному в пункте 4.1 критерию были собраны и рассмотрены данные о попытках подключения клиентов системы к кластеру серверов виртуализации (далее по пункту – сервер системы), а также данные об успешных подключениях. Среди клиентов, обращавшихся к серверу

выделена группа доверенных клиентов на каждом отрезке измерений, вычислены значения оценки вероятности доступа доверенного клиента.

Сбор данных проводился в течение 20 рабочих дней, когда происходит штатная работа системы; выходные, праздничные и предпраздничные дни в статистику не включены. За отрезок измерений приняты одни сутки. Во всех графических материалах время представлено в сутках с начала измерений без указания дат.

В первом этапе эксперимента рассматривается работа системы в стандартном режиме управления доступом, затем, на втором этапе включается механизм управления доступом на основе оценки доверия. Оценка доверия к клиентам проводится на всех этапах эксперимента. Числовые данные эксперимента приведены в таблице 4.

Таблица 4 – Экспериментальные данные

| Время, сут. | Количество уникальных подключений | Недовер. клиенты | Довер. клиенты | Кол-во успешных подключений довер. клиентов | Оценка вероятности доступа довер. клиента |
|---|---|---|---|---|---|
| 1 | 181 | 43 | 138 | 94 | 0,684 |
| 2 | 179 | 50 | 129 | 63 | 0,487 |
| 3 | 156 | 45 | 111 | 58 | 0,524 |
| 4 | 163 | 49 | 114 | 63 | 0,549 |
| 5 | 168 | 69 | 99 | 65 | 0,657 |
| 6 | 180 | 58 | 122 | 75 | 0,612 |
| 7 | 161 | 53 | 108 | 65 | 0,606 |
| 8 | 151 | 36 | 115 | 52 | 0,450 |
| 9 | 125 | 0 | 125 | 116 | 0,926 |
| 10 | 123 | 0 | 123 | 123 | 1,000 |
| 11 | 112 | 0 | 112 | 107 | 0,955 |
| 12 | 127 | 0 | 127 | 120 | 0,941 |
| 13 | 122 | 0 | 122 | 109 | 0,891 |
| 14 | 113 | 0 | 113 | 106 | 0,941 |
| 15 | 138 | 0 | 138 | 121 | 0,873 |
| 16 | 126 | 0 | 126 | 116 | 0,926 |
| 17 | 126 | 0 | 126 | 126 | 0,999 |
| 18 | 126 | 0 | 126 | 110 | 0,873 |
| 19 | 132 | 0 | 132 | 124 | 0,941 |
| 20 | 127 | 0 | 127 | 122 | 0,966 |

На рисунке 16 показаны значения общего количества запросов на доступ к ресурсам сервера системы в виде гистограммы с накоплением. Из представленных данных видно, что светлые столбцы, соответствующие запросам от недоверенных клиентов, пропадают из гистограммы, начиная с 9 суток эксперимента, это демонстрирует включение в работу метода управления на основе оценки доверия (доступ к серверу системы от недоверенных клиентов блокируется).

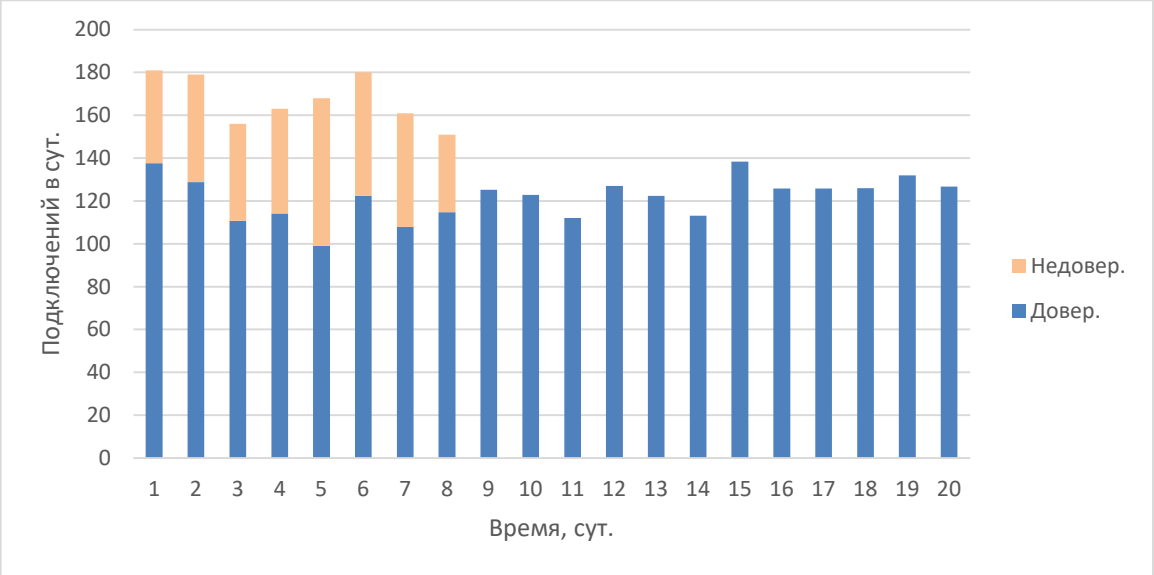



Рисунок 16 – Количество попыток подключений к серверу со стороны доверенных и недоверенных клиентов системы

На рисунке 17 приведена гистограмма успешных и неуспешных подключений доверенных клиентов к серверу системы. Клиент получает отказ в доступе, когда все ресурсы (виртуальные машины) заняты другими клиентами

Из рисунка 17 также можно заметить незначительный, но заметный прирост среднего числа запросов от доверенных клиентов: до использования метода оно составляет ~116,9 запросов в сутки, а затем возрастает до ~124,8. По мнению автора данное изменение связано с приведением части ранее недоверенных клиентов в соответствие заданным техническим условиям и, как следствие, повышением оценки доверия к себе.

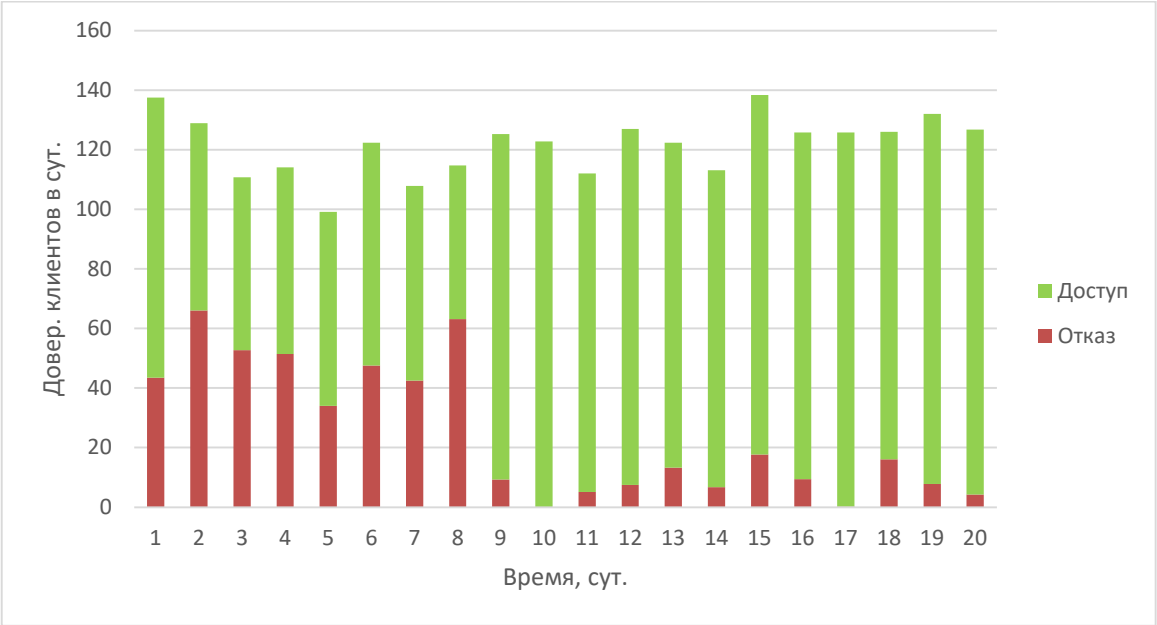



Рисунок 17 – Гистограмма подключений доверенных клиентов к серверу системы

На рисунке 18 приведены значения вероятности доступа доверенного клиента к серверу системы. Точками показаны значения оценки вероятности для соответствующего отрезка измерений (дня), а пунктиром изображена линия тренда ее изменений в ходе эксперимента.

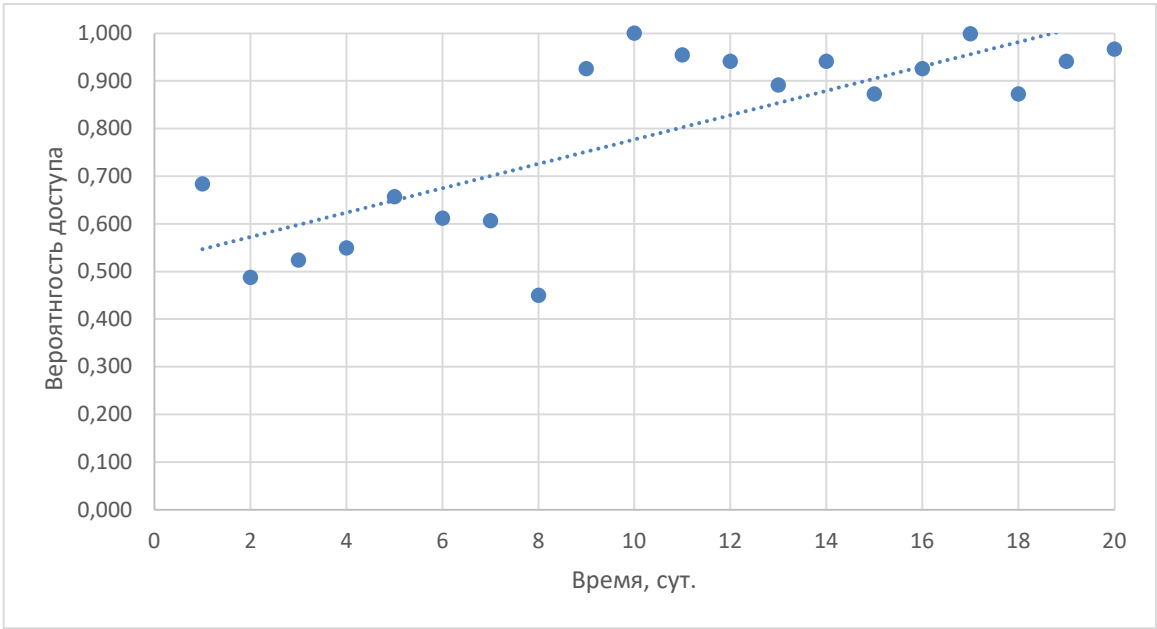



Рисунок 18 – Оценка вероятности доступа доверенного клиента к серверу системы

Из рисунка видно, что значения вероятности доступа в стандартном режиме управления доступом к серверу имеют более выраженный разброс по сравнению с

ними в период использования метода. Это связано с общим количеством обращений к серверу, которое в стандартном режиме очевидно выше, т.к. в поток заявок включаются все активные клиенты системы. Кучность оценок вероятности доступа при использовании разработанного метода особенно наблюдается в начале его работы, а затем, с ростом общего числа доверенных клиентов снижается. Данное обстоятельство по мнению автора не свидетельствует о снижении эффективности метода, т.к. ресурсы сервера используются доверенными клиентами. Снижение вероятности доступа клиента к ресурсу в этом случае обуславливается общим дефицитом ресурса сервера и не влияет на принятый показатель эффективности.

Значение линии тренда в серединах интервалов, соответствующих этапам эксперимента, соответственно равны ~0,63 и ~0,9. Принимая эти значения как средние для оценок вероятности доступа к серверу в стандартном режиме работы $P$ и при использовании метода $\tilde{P}$, можно рассчитать значение критерия эффективности: $\Delta P = \left(\tilde{P} - P\right)/P \approx 0{,}43$. Полученное значение соответствует ожидаемому значению $\Delta P$ согласно расчетам на разработанной вероятностной модели доступа.

## 4.4 Выводы

В данной главе проведено исследование эффективности разработанного метода управления ресурсами в клиент-серверной системе на основе оценки доверия к клиентам, сформулированы показатель эффективности и соответствующий ему критерий. Показателем эффективности принята вероятность доступа доверенного клиента к серверу в стационарном режиме работы системы.

Для исследования эффективности метода разработана новая вероятностная модель доступа на основе многоканальных СМО замкнутого типа с нулевой очередью, которая учитывает вероятность доставки заявки от клиента к серверу в общем потоке. Модель позволяет узнать, как состояние канала связи между клиентом и сервером влияет на характеристики системы в стационарном

состоянии. В этой связи поток заявок от клиентов рассматривается как простой Пуассоновский.

Оценка эффективности метода проведена для реальной информационной системы предприятия – системы виртуализации графических вычислительных ресурсов. С использованием модели проведено сравнение эффективности разработанного метода управления доступом на основе доверия с аналогичными методами управления на основе атрибутной модели и приоритезации запросов. Показано, что разработанный метод показывает большую эффективность в сравнении с аналогами.

Проведен производственный эксперимент по применению разработанного метода управления доступом в информационной системе предприятия. Полученные в ходе эксперимента данные подтверждают эффективность метода. Ожидаемые значения показателя эффективности, рассчитанные на модели, соответствуют экспериментальным.

# ЗАКЛЮЧЕНИЕ

1) В работе проведен аналитический обзор существующих моделей и методов управления ресурсами информационных систем, рассмотрены современные подходы к управлению ресурсами на основе контекстной информации об их потребителях (клиентах системы), показана актуальность проведенных исследований.

2) Разработана новая модель доверия к клиентам информационной системы на основе анализа их характеристик и атрибутов. Модель основана на порядковой нормированной шкале критериев доверия к клиенту, по которым проводится их сравнение с эталоном доверия. Эталон задается совокупностью свойств клиента, обеспечивающих наиболее эффективное использование ресурса сервера системы, оценка их важности проводится экспертным путем. Модель учитывает изменения состояния системы и позволяет оценить степень соответствия клиента заданным техническим условиям в определенный момент времени.

3) Разработан метод управления ресурсами клиент-серверной системы на основе оценки доверия, позволяющий более эффективно управлять дефицитными вычислительными и программными ресурсами системы за счет повышения вероятности доступа для клиентов, в большей степени соответствующих заданным техническим условиям. Условия принятия решения о доверии к клиенту формируются динамически исходя из текущего состояния шкалы весовых коэффициентов критериев, что позволяет владельцу системы без ограничений пересматривать настройки модели доверия. Метод предполагает механизм управляющего воздействия на канал связи между клиентами и сервером системы на сетевом уровне стека TCP/IP, это позволяет применять его в функционирующих информационных системах без изменения режимов их работы. Экспериментальные данные показывают увеличение вероятности доступа доверенных клиентов к дефицитным ресурсам сервера на ~43% для рассмотренной системы в сравнении со стандартным режимом работы.

4) Разработана система управления ресурсами в клиент-серверной системе, реализующая предложенный метод управления на основе оценки доверия, которая без существенных финансовых и технических затрат может быть интегрирована в существующие корпоративные информационные системы клиент-серверных архитектур. Предложены способы получения и обработки контекстных данных клиентов для оценки доверия к ним, описана математическая модель анализа связей узлов корпоративной ЛВС на основе логики предикатов первого порядка, позволяющая проводить оценку состояния каналов связи между клиентами и сервером системы.

5) Разработана вероятностная модель доступа клиентов к серверу системы, с помощью которой исследована эффективность метода управления ресурсами. Исследования показали эффективность разработанного метода в сравнении с аналогичными методами управления ресурсами: значение показателя эффективности $\Delta P$ в заданных условиях для разработанного метода составляет ~47%, а для метода на основе атрибутной модели ~41%. Результаты исследования соответствуют экспериментальным данным, что свидетельствует о достоверности модели.

6) Результаты работы внедрены в ряд корпоративных информационных систем АО «ИСС», в частности, разработанная модель доверия используется для принятия решения о согласовании допуска персонала к работе со специализированными программными средствами. Система управления ресурсами на основе разработанного метода внедрена в систему виртуализации графических вычислительных ресурсов и системы управления конкурентными лицензиями. Структура системы использована при разработке концепции и технического проекта распределенной автоматизированной системы обработки служебной информации.

# СПИСОК ЛИТЕРАТУРЫ

1. Барабанов А. Аутентификация и авторизация в микросервисных приложениях: обзор архитектурных подходов [Текст] / А. Барабанов, Д. Макрушин // Вопросы кибербезопасности. – М.: ЗАО НПО Эшелон, 2020. – № 4 (38). – С. 32-43.

2. Басыров А.Г. Конфигурирование вычислительных систем на основе виртуализации ресурсов [Текст] / А.Г. Басыров, Д.И. Казанцев, А.А. Карытко, Н.А. Шаменков // Известия Тульского государственного университета [Технические науки]. – Тула: ТулГУ, 2017. – Вып. 4. – С. 331-345.

3. Бегг К. Базы данных. Проектирование, реализация и сопровождение. Теория и практика: Учебное пособие [Текст] / К. Бегг, Т. Коннолли. – 3-е изд-е. – М.: Изд-во «Вильямс», 2017.

4. Белим С.В. Использование решётки формальных понятий для построения ролевой политики разграничения доступа [Текст] / С.В. Белим, Н.Ф. Богаченко // Информатика и системы управления. Благовещенск: АмГУ, 2018. – № 1(55). – С. 16–28.

5. Белим С.В. Совмещение политик безопасности, основанное на алгоритмах поддержки принятия решений [Текст] / С.В. Белим, Н.Ф. Богаченко, Ю.С. Ракицкий // Информационно-управляющие системы. – СПб.: ГУАП, 2016. – № 5. – С. 66–72.

6. Белим С.В. Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик безопасности [Текст] / С.В. Белим, Н.Ф. Богаченко, Ю.С. Ракицкий // Проблемы информационной безопасности. Компьютерные системы. – СПб.: СПбПУ, 2010. – № 2. – С. 9–17.

7. Бешта А.А. Архитектура агента контроля над внутренним злоумышленником на основе механизма оценки доверия [Текст] / А.А. Бешта // Известия ЮФУ. Технические науки [Тематический выпуск]. – Ростов-на-Дону: ЮФУ, 2012. – С.104-110.

8. Блюмин С.Л. Модели и методы принятия решений в условиях неопределенности: монография [Текст] / С.Л. Блюмин, И.А. Шуйкова. – Липецк: ЛЭГИ, 2001. – 138 с.

9. Богаченко Н.Ф. Локальная оптимизация политики ролевого разграничения доступа = Local Optimization of the Role-Based Access Control Policy [Текст] / Н.Ф. Богаченко // CEUR Workshop Proceedings. Германия: Ахен: RWTH Aachen, 2017. – V. 1965. – Режим доступа: http://ceur-ws.org/Vol-1965/paper14.pdf (дата обращения: 22.10.2020).

10. Борковой В.И. Облачные компьютерные системы для автоматизации бизнес-процессов предприятий общественного питания [Текст] / В.И. Борковой, Р.В. ИГИНОВА // Инновации: перспективы, проблемы, достижения [Материалы Шестой международной научно-практической конференции]. – М.: Вест-Ост-Ферлаг, 2018. – С.427-438.

11. Бутаев М.М. Использование элементов теории массового обслуживания при описании и управлении ресурсами и рабочей нагрузкой адаптивных математических моделей вычислительных систем с технологией виртуализации ресурсов [Текст] / М.М. Бутаев, А.А. Папко, В.Е. Курсонов и др. // XXI век: итоги прошлого и проблемы настоящего плюс. – Пенза: ПензГТУ, 2018. – Т. 7, № 4 (44). – С. 71-78.

12. Викторов А.С. Реализация распределенной вычислительной сети периферийного сервиса [Текст] / А.С. Викторов // Эпоха науки. – Ачинск: Ачинский филиал КрасГАУ, 2018. – № 15 – с. 85-88.

13. Вишняков В.А. Модели аутентификации в облачных вычислениях для мобильных приложений с интеллектуальной поддержкой выбора [Текст] / В.А. Вишняков, М.М. Гондаг Саз // Доклады БГУИР. – Беларусь: Минск: БГИУР, 2017. – № 1 (103). – С. 82-86.

14. Герасименко А.П. Концептуальная модель информационной системы [Текст] /А.П. Герасименко // Россия и АТР. – Владивосток: ФГБУН ИИАЭ ДВО РАН, 2001. – № 4 (34). – С. 145-148.

15. Гильмутдинов Р.Ф. Замкнутые многоканальные системы массового обслуживания с отказами [Текст] / Р.Ф. Гильмутдинов, А.П. Кирпичников // Вестник Казанского технологического университета [журнал]. – Казань: КНИТУ, 2012. – Т. 10(15). – С. 232-234.

16. Гильмутдинов Р.Ф. Математическая модель замкнутой одноканальной системы массового обслуживания [Текст] / Р.Ф. Гильмутдинов, А.П. Кирпичников // Вестник Казанского технологического университета [журнал]. – Казань: КНИТУ, 2012. – Т. 6(15). – С. 189-193.

17. Гильмутдинов Р.Ф. Многоканальные системы массового обслуживания замкнутого типа [Текст] / Р.Ф. Гильмутдинов, А.П. Кирпичников // Вестник Казанского технологического университета [журнал]. – Казань: КНИТУ, 2012. –Т. 8(15). – С. 326-331.

18. Горюнов Е.В. Классификация элементов информационной системы организаций связи [Текст] / Е.В. Горюнов // Журнал Программные продукты и системы. – Тверь: НИИ ЦПС, 2009. – № 2. – С. 153-156.

19. Грекул В.И. Проектирование информационных систем. Курс лекций : Учебное пособие для студентов вузов [Текст] / В.И. Грекул, Г.Н. Денищенко, Н.Л. Коровкина – М., Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ). –2017. – 303 с. – ISBN: 978-5-4487-0089-7.

20. Громов Ю.Ю. Архитектура ЭВМ и систем: учебное пособие [Текст] / Ю.Ю. Громов, О.Г. Иванова, М.Ю. Серегин, М.А. Ивановский, В.Е. Дидрих. – Тамбов: ТГТУ. – 2012. – 200 с.

21. Грушо А.А. Безопасные архитектуры распределённых систем [Текст] / А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина, С.Я. Шоргин // Системы и средства информатики. – М.: ФИЦ ИУ РАН, 2014. – Т. 24, № 3. – С. 18–31.

22. Грязнов Е.С. Система разграничения доступа на основе технологий виртуализации [Текст] / Е.С. Грязнов, С.П. Панасенко, Д.М. Пузырёв, А.В. Хартен // Вопросы защиты информации. – М.: НПЦ ОК «Компас», 2017. – № 2 (117). С. 14-18.

23. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов [Текст] / П.Н. Девянин. – 2-е изд. испр. и доп. – М.: Горячая линия Телеком, 2013. – 338 с.

24. Девянин П.Н. О проблеме представления формальной модели политики безопасности операционных систем = On the problem of representation of the formal model of security policy for operating systems // Труды ИСП РАН. – М., 2017. – Т. 27, вып. 3. – С. 7-16.

25. Девянин П.Н. Обзорные лекции по моделям безопасности компьютерных систем [Текст] // Прикладная дискретная математика. Приложение. – Томск : ТГУ, 2009. – № 2. – С. 151-190.

26. Девянин П.Н. Формирование словаря терминов теории моделирование безопасности управления доступом и информационными потоками в компьютерных системах [Текст] // Прикладная дискретная математика. – Томск: ТГУ, 2011. – № 2(12). – С. 17-39.

27. Дураковский А.П. О доверии в информационных системах на основе интернет-технологий = About trust in the information systems on the basis of internet-based technologies / А.П. Дураковский, Т.А. Кондратьев, Ю.Н. Лаврухин, В.Р. Петров: [электронный ресурс]. – М.: МИФИ, [б. г.]. – Режим доступа: https://bit.mephi.ru/index.php/bit/article/viewFile/126/132 (дата обращения: 06.10.2020).

28. Жаббаров И.Ш. Обоснование выбора системы виртуализации, предоставляющей необходимый функционал для предприятия заданного уровня [Текст] / И.Ш Жаббаров, Т.Д. Фатхулин // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – Ростов-на-Дону: Северо-Кавказский филиал МТУСИ, 2019. – № 1. – С. 233-239.

29. Захаров К.С. Задача оптимизации распределения вычислительных ресурсов в ЦОД [Текст] / К.С. Захаров, А.С. Галченков, С.П. Гольденберг // Информационно-аналитические и интеллектуальные системы в промышленности и социальной сфере: сборник научных трудов общеуниверситетской конференции студентов и молодых ученых. – М.: МГУПП, 2019. – Т. 1. – С. 64-70.

30. Зинина Л.И. Корпоративные информационные системы в архитектуре предприятия [Текст] / Л.И. Зинина, Л.И. Ефремова // Вестник Волжского университета им. В.Н. Татищева. – Тольятти: ВГУ, 2018. – № 3 (2). – С. 132-137.

31. Игнатенко В.Н. Контроль установки и функционирования системы аудита программно-аппаратной части рабочих станций корпоративной сети [Текст] / Н.В. Игнатенко, Р.В. Лебедев, М.Ю. Махонин // XV Международная научная конференция «Решетневские чтения». – Красноярск: СибГАУ. – 2011. – С. 572-273.

32. Истратова Е.Е. Сравнительный анализ методов моделирования сетевого трафика в коммерческих сетях [Текст] / Е.Е. Истратова, Д.А. Березин, А.О. Бородина // Информационные технологии в экономике и управлении: Материалы международной конференции. – Махачкала: Формат, 2020. – Т. 1. – С. 78-80.

33. Каверина М.С. Оптимальное распределение ресурсов физического сервера в условиях неопределенности [Текст] / М.С. Каверина, И.А. Балакирева // В мире компьютерных технологий: Сборник статей всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. – Севастополь: СевГУ, 2020. – Т. 1. – С. 29-33.

34. Каширин Е.В. Анализ протоколов сетевой аутентификации пользователей компьютерных сетей [Текст] / Е.В. Каширин // Сборник научных трудов 6-й Международной молодежной научной конференции «Юность и знания – гарантия успеха». – Курск: ЮЗГУ, 2019. –№ 1. – С. 330-334.

35. Когаловский М.Р. Перспективные технологии информационных систем: учебное пособие [Текст] / М.Р. Когаловский. – М.: ДМК Пресс. – 2003. – 288 с.

36. Кузьмина Э.В. Подходы к определению архитектуры информационной системы [Текст] / Э.В. Кузьмина // Материалы II Международной заочной научно-практической конференции «Инновационные процессы в развитии современного общества». – Краснодар: ООО «ЮрЭксПрактик». – 2014. – С. 361-364.

37. Кутузов О.И. Моделирование телекоммуникационных сетей: учебное пособие [электронный ресурс] / О.И. Кутузов, Т.М. Татарникова .– СПб: Спб. гос. ун-т телеком-й, [б.г.].– Режим доступа: http://dvo.sut.ru/libr/ius/w101kutu/, свободный (дата обращения: 01.10.2020).

38. Лапин С.А. Модель разграничения доступа для систем, содержащих равнозначные объекты [Текст] / С.А. Лапин // Безопасность информационных технологий. – М.: МИФИ, 2016. – № 2. – С. 49–54.

39. Лебедев Р.В. Вычисление весовых коэффициентов в задачах оценки сходства / Р.В. Лебедев, А.В. Мурыгин // Научно-технический вестник Поволжья. – Казань: ООО «Рашин Сайнс», 2020. – № 12. – С. 51-56.

40. Лебедев Р.В. Логическая модель связей между узлами корпоративной вычислительной сети / Р.В. Лебедев, В.Е. Косенко, И.В. Потуремский // Наукоемкие технологии. – М.: Радиотехника, 2015. – Т. 16, № 3. – С. 95-100.

41. Лебедев Р.В. Подход к оценке сходства объектов компьютерных систем с эталоном // Сборник научных статей по итогам IX международной научной конференции «Приоритетные направления инновационной деятельности в промышленности». – Казань: ООО «Конверт», 2020. – Ч. 2. – С. 25-29.

42. Лебедев Р.В. Система контроля программно-аппаратной части рабочих станций корпоративной сети / Р.В. Лебедев, В.Н. Игнатенко, И.В. Потуремский // Решетневские чтения: материалы XV Международной научной конференции. – Красноярск: СибГАУ, – 2011. – Ч. 2. – С. 578-579.

43. Лебедева К.Е. Методика повышения надежности видеоконференцсвязи / К.Е. Лебедева, Р.В. Лебедев, А.В. Мурыгин // Сибирский журнал науки и технологий. – 2017. – № 2. – Т. 18. – С. 274-282.

44. Мартышкин А.И. Возможности варьирования ресурсами и рабочей нагрузкой в адаптивных моделях вычислительных систем [Текст] / А.И. Мартышкин, Д.О. Терешкин // Современные методы и средства обработки пространственно-временных сигналов: Сборник статей XVII Всероссийской научно-технической конференции. – Пенза: Приволжский дом знаний, 2019. – Т. 1. –С. 58-61.

45. Мартышкин А.И. Применение аппарата теории массового обслуживания при описании адаптивных моделей вычислительных систем с виртуализацией ресурсов [Текст] / А.И. Мартышкин // XXI век: итоги прошлого и проблемы настоящего плюс. – Пенза: ПензГТУ, 2018. – Т. 7, № 2 (42). – С. 15-21.

46. Международный стандарт. Информационные технологии. Словарь = Information technologies. Vocabulary [Текст]: ГОСТ 33707-2016 (ISO/IEC 2382:2015). – М.: Изд-во стандартов, 2016.

47. Мочалов В.П. Имитационная модель алгоритмов функционирования узлов программно-конфигурируемых сетей [Электронный ресурс] / В.П. Мочалов, В.А. Моисеенко, Н.Ю. Братченко // Актуальные направления фундаментальных прикладных исследований: Материалы международной научно-практической конференции. – США: Моррисвилл: LuluPress Inc., 2019. – С. 125-132. Режим доступа: https://www.elibrary.ru/download/elibrary_37740761_55456979.pdf, (дата обращения 05.02.2021).

48. Мяло О.В. Классификация вычислительных систем [Текст] / О.В. Мяло, Ф.Ю. Седин // Научные преобразования в эпоху глобализации: сборник статей международной научно-практической конференции. – Челябинск: МЦИИ Омега Сайнс, 2018. – С. 28-32.

49. Мяло О.В. эксплуатационная надежность компьютерных систем [Текст] / О.В. Мяло, Н.А. Яковенко, А.В. Непомнящих, А.А. Щеголев // Сборник II Международной научно-практической конференции, посвященная 25-летию ФГБОУ ВО Омский ГАУ в статусе университета. – Омск: Омский ГАУ, 2019. – С. 211-216.

50. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения [Текст]: ГОСТ Р 58833-2020. – М.: Изд-во стандартов, 2020.

51. Национальный стандарт Российской Федерации. Защита информации. Термины и определения [Текст] : ГОСТ Р 50922-2007. М. : Изд-во стандартов, 2007.

52. Национальный стандарт Российской Федерации. Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации [Текст]: ГОСТ Р ИСО/МЭК 9594-8-98. – М. : Изд-во стандартов, 1998-05.

53. Национальный стандарт Российской Федерации. Информационная технология. Комплекс стандартов на автоматизированные системы. Требования и

показатели качества функционирования информационных систем (ИС). Общие положения [Текст]: ГОСТ РВ 51987-2002. – М. : Изд-во стандартов, 2002.

54. Национальный стандарт Российской Федерации. Системы менеджмента качества. Основные положения и словарь [Текст]: ГОСТ Р ИСО 9000-2008. М. : Изд-во стандартов, 2008.

55. Николаев В.Н. Оценка эффективности локальной вычислительной сети при решении главной и обеспечивающих задач [Текст] / В.Н. Николаев, С.И. Рогатин, Е.А. Коломиец, О.И. Атакищев // Известия Юго-Западного государственного университета. – Курск: ЮЗГУ, 2019. – № 23(2). – С. 174-185.

56. Оленников А.А. Разработка модели управления доступом для типовой медицинской информационной системы [Текст] / А.А. Оленников, Е.А. Оленников, А.А. Захаров, А.В. Широких, В.В. Варнавский // Программные продукты и системы. – Тверь: НИИ ЦПС, 2016. – № 1. С. 166–169.

57. Платформа Cisco Identity Services Engine [Электронный ресурс] / Cisco Inc. – US: San Jose: Cisco Inc. – [n. y.]. – Access mode: https://www.cisco.com/c/ru_ru/products/security/identity-services-engine/index.html, (Access date 21.01.2021).

58. Подиновский В.В. Введение в теорию важности критериев в многокритериальных задачах принятия решений: учебное пособие [Текст] / В.В. Подиновский. – М.: изд-во Физмалит, 2007. – 64 с.

59. Подиновский В.В. Еще раз о некорректности метода анализа иерархий [Текст] / В.В. Подиновский, О.В. Подиновская // Проблемы управления. – М.: СенСиДат Контрол, 2012. – № 3. – С. 75-78.

60. Подиновский В.В. О некорректности метода анализа иерархий / В.В. Подиновский, О.В. Подиновская // Проблемы управления. – М.: СенСиДат-Контрол, 2011. – № 1. – С. 8-13.

61. Подиновский В.В. Теория важности критериев: современное состояние и направления дальнейшего ее развития / В.В. Подиновский, М.А. Потапов, А.П. Нелюбин, О.В. Подиновская // XII Всероссийское совещание по проблемам управления. – М.: ИПУ РАН, 2014. – С. 7697-7702.

62. Порохненко Ю.С. Сравнительный анализ эмуляторов компьютерных сетей [Электронный ресурс] / Ю.С. Порохненко, П.Н. Полежаев. – Оренбург: Открытая электронная библиотека научно-образовательных ресурсов Оренбуржья, 2017. – 7 с. – Режим доступа: http://elib.osu.ru/bitstream/123456789/5918/1/elibrary_28977477_93977792.pdf, (дата обращения 05.02.2021).

63. Постников В.М. Выбор весовых коэффициентов локальных критериев на основе принципа арифметической прогрессии / В.М. Постников, С.Б. Спиридонов // Наука и образование: Электрон. журн.– М.: МГТУ, 2015. – № 9. – DOI: 10.7463/0915.0802449.

64. Потин А.В. Системно-онтологический анализ предметной области оценивания гарантий информационной безопасности [Текст] / А.В. Потин, Д.С. Комин // Радиоэлектронные и компьютерные системы. – Харьков, Украина: Харьковский университет воздушных сил им. И. Кожедуба, 2010. – № 5 (46). – С. 50-56.

65. Прощаева А.А. Влияние ролевой модели доступа на производительность веб-систем при внедрении 1С-Битрикс [Электронный ресурс] / А.А. Прощаева // Инженерный вестник Дона. – Ростов-на-Дону: ЮФУ, 2017. – № 3. Режим доступа: http://ivdon.ru/ru/magazine/archive/n3y2017/4364 (дата обращения 10.10.2020).

66. Пузиков А.М. Организация автоматизированного контроля состояний компонентов систем информационной безопасности / А.М. Пузиков, Р.В. Лебедев // Решетневские чтения: материалы XVIII Международной научной конференции. – Красноярск: СибГАУ, – 2014. – Т. 2, № 18. – С. 326-328.

67. Роскосмос. Приказы. Об утверждении Отраслевой технической политики Государственной корпорации по космической деятельности «Роскосмос» и ее организаций в области информационных и цифровых технологий [Текст] / Государственная корпорация по космической деятельности «Роскосмос». – М.: 2020. – № 411.

68. Российская федерация. Законы. Об информации, информационных технологиях и о защите информации [Текст] // Собрание законодательства Российской федерации. – 2006. – № 149-ФЗ.

69. Саати Т. Принятие решений. Метод анализа иерархий: перевод с английского [Текст] / Т. Саати, Р.Г. Вачнадзе (перевод). – М: изд. Радио и связь, 1993. – 278 с.

70. Саенко И.Б. Методика формирования единой схемы разграничения доступа к гетерогенным информационным ресурсам в облачных инфраструктурах [Текст] / И.Б. Саенко, С.А. Ясинский, М.А. Бирюков // Информация и космос. СПб.: НТОО «Институт телекоммуникаций», 2019. – № 1. – С. 77-83.

71. Силин А.В. Моделирование промышленных сетей средствами Cisco Packet tracer [Текст] / А.В. Силин, И.В. Силина // Проблемы науки: Материалы Всероссийской научно-технической конференции. – Новомосковск: Новомосковский филиал РХТУ, 2019. – С. 201-204.

72. Скоба А.Н. Математическая модель функционирования распределённой информационной системы на базе трехуровневой клиент-серверной архитектуры [Электронный ресурс] / А.Н. Скоба, Айеш Ахмед Нафеа Айеш (Ирак) // Инженерный вестник Дона. – Ростов-на-Дону: ЮФУ, 2017. – № 4. – URL: http://ivdon.ru/ru/magazine/archive/n4y2017/4482 (дата обращения 05.01.2020).

73. Скоба А.Н. Модель оптимального размещения информационных ресурсов по узлам распределённой информационной системы предприятия на базе двухуровневой архитектуры «клиент-сервер» с учётом влияния блокировок [Текст] / А.Н. Скоба, А.Н. Панфилов // Известия высших учебных заведений. Электромеханика. – Новочеркасск: ЮРГПУ(НПИ) им. М.И. Платова, 2017. – Т. 60 (2). – С. 77-84. – ISSN: 0136-3360.

74. Спиридонов С.Б. Анализ подходов к выбору весовых коэффициентов критериев методом парного сравнения критериев [электронный ресурс] / С.Б. Спиридонов, И.Г Булатова, В.М. Постников // Интернет-журнал «Науковедение», 2017. – Том 9, №6 (2017). – URL: https://naukovedenie.ru/PDF/16TVN617.pdf (дата обращения 25.10.2020).

75. Таланов М.А. Автоматизация оценки уровня доверия в информационной безопасности [Текст] / М.А. Таланов, А.С. Тимохович // Academy [журнал]. – Иваново: ООО «Олимп», 2017. – № 6 (57). –(ISSN 2412-8236). – С. 8-9.

76. Управление доступом в архитектуре Cisco TrustSec [Электронный ресурс] / Д. Казаков. – US: San Jose: Cisco Inc., 2015 – Access mode: https://gblogs.cisco.com/ru/dkazakov_cisco_trustsec/, (access date 21.01.2021). – Заголовок с экрана.

77. Управление сетевой инфраструктурой HP OpenView Network Node Manager [электронный ресурс]. – HP-Software.ru Проект компании Ай Теко.– Режим доступа: www.openview.ru/nnm_2.htm, (дата обращения 20.10.2020).

78. Усов С.В. О представлении некоторых ролевых моделей разграничения доступа объектно-ориентированной моделью HRU [Текст] / С.В. Усов // Математические структуры и моделирование. – Омск: ФГБОУ ВО «ОмГУ им. Ф.М. Достоевского», 2018. – № 4(48). – С. 128–138.

79. ФСТЭК России. Информационное сообщение об утверждении требований к межсетевым экранам: письмо [Текст] / ФСТЭК России. – М., 2016. – № 240/24/1986.

80. Цербенко К.Н. Моделирование автоматизированной информационной подсистемы в агропромышленном комплексе [Текст] / К.Н Цебренко, О.А. Молявко // Вестник ИМСИТ. – Краснодар: ИМСИТ, 2018. – № 1 (73). – С. 39-41.

81. Чермаков Ю.В. Локальные вычислительные сети. Издание второе, исправленное и дополненное / Ю.В. Чекмарев. – М.: ДМК Пресс, 2009. – 200 с.

82. Чудинов И.Л. Информационные системы и технологии: учебное пособие [Текст] / И.Л. Чудинов, В.В. Осипова. – Томск: ТПИ, 2013. – 145 с.

83. Шипулин П. М. Применение цифровых водяных знаков для организации и управления электронным архивом фотодокументов / П.В, Шипулин, Р.В. Лебедев, М.С. Сосновский // Материалы XXIV Международной научно-практической конференции «Решетневские чтения». – Красноярск: СибГУ, 2020. – Ч. 2. – С. 560-562.

84. Шипулин П.М. Вариант защищенного доступа к конфиденциальным ресурсам локальной сети / П.М. Шипулин, Р.В. Лебедев, А.В. Хандожко, И.В. Потуремский // В сборнике: Актуальные вопросы проектирования автоматических

космических аппаратов для фундаментальных и прикладных научных исследований. – М.: АО «НПО Лавочкина», 2017. – С. 558-565.

85. Шипулин П.М. Применение цифровых водяных знаков на основе моментов Цернике для организации и управления электронным архивом фотодокументов / П.В. Шипулин, Р.В. Лебедев, М.С. Сосновский // Сибирский журнал науки и технологий. – Красноярск: СибГУ, 2021. – Т. 22 (1).

86. Шлаев Д.В. Классификация информационных систем [Текст] / Д.В. Шлаев, К.И. Жукова // Сборник материалов конференции «Информационные системы и технологии как фактор развития экономики региона». – Ставрополь: ООО «Бюро новостей». – 2013. – С. 282-285.

87. Шудрова К.Е. Защищенный доступ к системам видеоконференции / К.Е. Шудрова, Р.В. Лебедев, В.Ю. Почкаенко // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – 2013. – № 1 (47). – С. 100-103.

88. Alian M. Ncap: Network-driven, packet context-aware power management for client-server architecture [Text] / M. Alian, A. H. Abulila, L. Jindal, D. Kim, N. S. Kim // 2017 IEEE International Symposium on High Performance Computer Architecture (HPCA). – US: New York: IEEE, 2017. – pp. 25-36.

89. Andronov N. Trobac model for access control in Document management software systems [Text] / N. Andonov, E. Hadzhikolev, S. Hadzhikoleva // Научни трудове на СУБ [bulg.] – Bulgaria: Plovdiv: СУБ – Пловдив, 2019. – Vol. XVII. – pp. 106-113.

90. Arenas A. Reputation management in collaborative computing systems [Text] / A. Arenas, A. Aziz [etc.]. // Security and Communication Networks. – UK: Portsmouth: University of Portsmouth, 2009. – № 3(6). – pp. 546-564.

91. Bankov D. Mathematical model of LoRaWAN channel access with capture effect [Electronic resource] / D. Bankov, E. Khorov, A. Lyakhov // IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). – US: New York: IEEE, 2017. URL: https://arxiv.org/pdf/2008.03140.pdf (Access date 10.10.2020).

92. Behera P.K. A novel trust based access control model for cloud environment [Text] / P.K. Behera, P.M. Khular // Lecture Notes in Electrical Engineering. – Germany: Berlin: Springer, 2017. – Vol. 395. – P. 285-295.

93. Belim S. An analysis of graphs that represent a role-based security policy hierarchy [Text] / S. Belim, N. Bogachenko, E. Ilushechkin // Journal of Computer Security. Netherlands: Amsterdam: IOS Press, 2015. – Vol. 23, No. 5. – P. 641–657.

94. Belim S.V. Using the Decision Support Algorithms Combining Different Security Policies [Electronic resource] / S.V. Belim, N.F. Bogachenko, A.N. Kabanov, Y.S. Rakitskiy // IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). US: New York: IEEE Press, 2017. – URL: http: //ieeexplore.ieee.org/document/7818976/ (access date 23.10.2020).

95. Cao C. Research on Comprehensive Performance Simulation of Communication IP Network Based on OPNET [Electronic resource] / C. Cao, Y. Zuo, F. Zhang, etc. // 2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). – US: New York: IEEE Press, 2018. – URL: https://ieeexplore.ieee.org/abstract/ document/8332741, (access date 05.02.2021).

96. Denning D.E. A New Paradigm for Trusted Systems [electronic resource].– USA: Washington: Georgetown University: Computer Science Department, 1993. – URL: https://faculty.nps.edu/dedennin/publications/NewParadigmTrustedSystems.pdf (access date 06.10.2020).

97. Ferraiolo D.F. Role-Based Access Controls [Text] / D.F. Ferraiolo, D.R. Kuhn. – UK: London: Artech House, 2003. – 235 p.

98. Gai F. Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network [Text] / F. Gai, B. Wang, W. Deng // Lecture Notes in Computer Science. – Germany: Berlin: Springer, 2018. – Vol. 10828. – P. 666-681.

99. Gong S. Exploiting backscatter-aided relay communications with hybrid access model in device-to-device networks [Text] / S. Gong, L. Gao, J. Xu, Y. Guo, D. T. Hoang, D. Niyato // IEEE Transactions on Cognitive Communications and Networking. – US: New York: IEEE, 2019. –Vol. 5 (4). – pp. 835-848.

100. Hassan H. Enhanced QoS-based model for trust assessment in cloud computing environment [Text] / H. Hassan, A.I. El-Desouky, A. Ibrahim // IEEE Access. – US: New York: IEEE Press, 2020. – Vol. 8. – p. 43752-43763.

101. IEEE Standard for Local and metropolitan area networks. Virtual Bridged Local Area Networks [Electronic resource]: ANSI/IEEE 802.1Q-2005 / IEEE Standards Association; ANSI. – cor. 1: Corrections to the Multiple Registration Protocol. – New York, USA, 2008. – Access mode: https://standards.ieee.org/standard/802_1Q-2018.html (access date 15.10.2020).

102. IEEE Standard for Local and metropolitan area networks. Virtual Bridged Local Area Networks [Electronic resource]: IEEE 802.1v-2001. – New York, USA, 2001. – Access mode: https://standards.ieee.org/standard/802_1v-2001.html (access date 15.10.2020).

103. IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks [Electronic resource]: IEEE 802.1Qbb-2011 / IEEE Standards Association. – New York, USA, 2011. – Access mode: https://standards.ieee.org/standard/802_1Qbb-2011.html (access date 15.10.2020).

104. IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control [Electronic resource]: IEEE 802.1X-2010. – New York, USA, 2010. – Access mode: https://standards.ieee.org/standard/802_1X-2010.html (access date 15.10.2020).

105. Jamsa K. Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more [Text] / K. Jamsa. – US: Burlington: Jones & Bartlett Learning, 2012. – 321 p.

106. Kavis M.J. Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS) [Text] / M.J. Kavis. – US: Hoboken: Wiley, 2014. – 224 p.

107. Kesarwani A. Development of trust based access control models using fuzzy logic in cloud computing [Electronic resource] / A. Kesarwani, P.M. Khilar // Journal of King Saud University (Computer and Information Sciences). – Saud Arabia: Riyadh:

KSU, 2019. – URL: https://doi.org/10.1016/j.jksuci.2019.11.001, (access date: 05.02.2021).

108. Khan Z. IoT connectivity in radar bands: A shared access model based on spectrum measurements [Text] / Z. Khan, J.J. Lehtomaki, S. Iellamo, R. Vuohtoniemi, E. Hossain, Z. Han // IEEE Communications Magazine. – US: New York: IEEE Press, 2017. – Vol. 55 (2). – pp. 88-96.

109. Khilar P.M. Trust-Based Access Control in Cloud Computing Using Machine Learning [Text] / P.M. Khilar, V. Chaudhari, R.R. Swain // Cloud Computing for Geospatial Big Data Analytics. – Germany: Berlin: Springer, 2018. – Vol. 49. – P. 55-79.

110. Kontoudis D. A statistical approach to virtual server resource management [Electronic resource] / D. Kontoudis, P. Fouliras // Concurrency and Computation: Practice and Experience. – US: New-York: Wiley, 2017. – Vol. 30, Issue 4. – URL: https://doi.org/10.1002/cpe.4335, (access date 01.03.2021).

111. Kotari N.B. Improving the cloud server resource management in uncertain load conditions using ACO and linear regression algorithms [Text] / N.B. Kotari, A. Mahalkari // Advances in Intelligent Systems and Computing. – Germany: Berlin: Springer, 2018. – Vol. 870. – P. 79-88.

112. Lacoursière C. FMI Go! A simulation runtime environment with a client server architecture over multiple protocols [Text] / C. Lacoursière, T. Härdin // Proceedings of the 12th International Modelica Conference. – Czech Republic: Prague: CSKI, 2017. – Vol. 1. – pp.653-662.

113. Lawall A. Enterprise Architecture: A Formalism for Modelling Organizational Structures in Information Systems [Text] / A. Lawall, T. Schaller, D. Reichelt // Workshop on Enterprise and Organizational Modeling and Simulation [Lecture Notes in Business Information Processing]. – Berlin, Germany: Springer, 2014. – Vol. 191. – pp. 77-95.

114. Lawall A. Resource Management and Authorization for Cloud Services [Electronic resource] / A. Lawall, D. Reichelt, T. Schaller // Business Process Management [7th International Conference]. – US: New York: ACM, 2015. – № 18. –

pp. 1–8. – Access mode: https://doi.org/10.1145/2723839.2723864 (Access date 10.10.2020).

115. Lebedev R.V. Resource management in client-server computing systems based on trust assessment [Electronic resource] / R.V. Lebedev, A.V. Murigin, V.S. Tynchenko // Journal of Physics: Conference Series. – UK: IOP Science, 2020. – Vol. 1679. – DOI:10.1088/1742-6596/1679/3/032030, URL: https://iopscience.iop.org/article/10.1088/1742-6596/1679/3/032030/pdf (access date 09.02.2021).

116. Li T. Research on TCP/IP congestion control based on NS-2 network simulation platform [Text] / T. Li // Telecommunications and Radio Engineering. – US: Danbury: Begell House, 2019. – Vol. 78 (19). – P. 1737-1745.

117. Lim M. C2CFTP: Direct and Indirect File Transfer Protocols Between Clients in Client-Server Architecture [Text] / M. Lim // IEEE Access. US: New York: IEEE, 2020. – Vol. 8. – pp. 102833-102845.

118. Marsh S. Formalising Trust as a Computational Concept: [PhD thesis] / S. Mash. – UK: University of Stirling: Department of Computing Science and Mathematics, 1994. – 184 p.

119. McCollum C.J. Beyond the Pale of MAC and DAC --Defining New Forms of Access Control [Text] / C.J. McCollum, J.R. Messing, L. Notargiacomo // IEEE Computer Society Proceedings – US: Washington: IEEE Computer Society, 1990. Vol. 1. – 190 p.

120. McLean J. The specification and modeling of computer security [Text] / J. McLean // IEEE Computer. – US: New York: IEEE, 1990. – Vol. 23, Issue 1. – P. 9–16.

121. Namasudra S. PpBAC: popularity based access control model for cloud computing [Text] / S. Namasudra, P. Roy // Journal of Organizational and End User Computing (JOEUC). – US: Hershey: IGI Global, 2018.– Vol. 30 (4). – pp. 14-31.

122. Ouaddah A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT [Text] / A. Ouaddah, A.A. Elkalam, A. A. Ouahman // Europe and MENA cooperation advances in information and communication technologies [Advances in Intelligent Systems and Computing]. – Berlin, Germany: Springer, 2017. – Vol.520. – pp. 523-533.

123. Potapov V.I. Reliability in the model of an information system with client-server architecture [Electronic resource] / V.I. Potapov, O.P. Shafeeva, A.S. Gritsay, V.V. Makarov, O.P. Kuznetsova, L.K. Kondratukova // Journal of Physics: Conference Series. – UK: Bristol: IOP Publishing, 2019. – Vol. 1260 (2). – Access mode: https://iopscience.iop.org/article/10.1088/1742-6596/1260/2/022007/pdf (Access date 10.10.2020).

124. Review: HP Intelligent Management Center (IMC) [Electronic resource] / HP Inc. – US: Palo Alto: HP Inc., 2020. – Access mode: https://www.networkmanagement software.com/ hp-intelligent-management-center-imc-review, (access date 21.01.2021).

125. RFC: 791. Internet protocol (Интернет протокол) [Text] / Information Sciences Institute University of Southern California.– Marina del Rey, 1981.

126. Riad K. Multi-Factor Synthesis Decision-Making for Trust-Based Access Control on Cloud [Electronic resource] / K. Riad, Z. Yan // International Journal of Cooperative Information Systems. – Singapore: World Scientific, 2017. – Vol.26 (04). – URL: https://doi.org/10.1142/S0218843017500034, (access date: 05.02.2021).

127. Rosaci D. Integrating Trust Measures in Multi-Agent Systems [Text] / D. Rosaci, G. Sarne, S. Garruzzo // International Journal of Intelligent Systems (IJIS). – Wiley Periodicals, Inc., 2012. – Vol. 27. – (ISSN 1098-111X). – pp. 1-15.

128. Ruj S. DACC: Distributed Access Control in Clouds [Text] / S. Ruj, A. Nayak, I. Stojmenovic // Proc. of IEEE 10th International Conference «Trust, Security and Privacy in Computing and Communications (TrustCom)». – US: New York: IEEE Press, 2011. – P. 91–98.

129. Sandhu R.S. Role-Based Access Control Models [Electronic resource] / R.S. Sandhu // Advances in Computers. – Netherlands: Amsterdam: Elsevier, 1998. – Vol. 46. – P. 237–286.

130. Sandhu, R.S. Lattice-based access control models [Text] / R.S. Sandhu // IEEE Computer. – US: New York: IEEE Press, 1993. – Vol. 26 (11). – pp. 9–19.

131. Sharma P. Portfolio-driven resource management for transient cloud servers [Electronic resource] / P. Sharma, D. Irwin, P. Shenoy // Proceedings of the ACM on Measurement and Analysis of Computing Systems. – US: New-York: ACM, 2017. – Vol.

1, No. 1, Article No. 5. – URL: https://doi.org/10.1145/3084442, (access date 01.03.2021).

132. Singh A. An adaptive mutual trust based access control model for electronic healthcare system [Text] / A. Singh, K. Chatterjee // Journal of Ambient Intelligence and Humanized Computing. – Germany: Berlin: Springer, 2020. – Vol. 11. – P. 2117-2136.

133. Singh A. Trust based access control model for securing electronic healthcare system [Text] / A. Singh, K. Chatterjee // Journal of Ambient Intelligence and Humanized Computing. – Germany: Berlin: Springer, 2019. – Vol. 10. – P. 4547-4565.

134. SWI-Prolog reference manual: справочное руководство [электронный ресурс].– Режим доступа: http:// www.swi-prolog.org/pldoc/refman/, (дата обращения 25.10.2020). – Заглавие с экрана.

135. Takalkar V. Trust-Based Access Control in Multi-role Environment of Online Social Networks [Text] / V. Takalkar, P.N. Mahalle // Wireless Personal Communications. – Germany: Berlin: Springer, 2018. – Vol. 100. – P. 391-399.

136. Tejas G.S. Intelligent Access Control: A Self-Adaptable Trust-Based Access Control (SATBAC) Framework Using Game Theory Strategy [Text] / G.S. Thejas, T.C. Pramod, S.S. Iyengar, N.R. Sunitha // Proceedings of International Symposium on Sensor Networks, Systems and Security. – Germany: Berlin: Springer, 2018. – Vol. 1. – P. 97-111.

137. Wang N. ENORM: A framework for edge node resource management [Text] / N. Wang, B. Varghese, M. Matthaiou, etc. // IEEE Transactions on Services Computing. – US: New-York: IEEE press, 2020. – Vol. 13, Issue 6. – P. 1086-1099.

138. Zeng W. Content-Based Access Control: [PhD thesis]/ W. Zeng. – USA: University of Kansas, 2015. – 152 p.

139. Zhang D. Efficient graph based approach to large scale role engineering [Electronic resource] / D. Zhang, K. Ramamohanarao, R. Zhang, etc. // Transactions on data privacy. – Sweden: Skövde: TDS, 2014. – No. 7. – P. 1-26. – URL: https://www.researchgate.net/profile/Kotagiri_Ramamohanarao/publication/290539893_Efficient_Graph_Based_Approach_to_Large_Scale_Role_Engineering/links/5baabe18

a6fdccd3cb733295/Efficient-Graph-Based-Approach-to-Large-Scale-Role-Engineering.pdf, (access date: 05.02.2021).

140. Zhang Y. Research on services encapsulation and virtualization access model of machine for cloud manufacturing [Text] / Y. Zhang, G. Zhang, Y. Liu, D. Hu // Journal of Intelligent Manufacturing. – Germany: Berlin: Springer, 2017. – Vol. 28 (5). – pp. 1109-1123.

## ПУБЛИКАЦИИ ПО ТЕМЕ РАБОТЫ

В журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендуемых ВАК:

1) Лебедев Р.В. Вычисление весовых коэффициентов в задачах оценки сходства / Р.В. Лебедев, А.В. Мурыгин // Научно-технический вестник Поволжья. – Казань: ООО «Рашин Сайнс», 2020. – № 12. – С. 51-56.

2) Лебедев Р.В. Логическая модель связей между узлами корпоративной вычислительной сети / Р.В. Лебедев, В.Е. Косенко, И.В. Потуремский // Наукоемкие технологии. – М.: Радиотехника, 2015. – Т. 16, № 3. – С. 95-100.

3) Шудрова К.Е. Защищенный доступ к системам видеоконференции / К.Е. Шудрова, Р.В. Лебедев, В.Ю. Почкаенко // Вестник Сибирского государственного аэрокосмического университета имени академика М.Ф. Решетнева. – 2013. – № 1 (47). – С. 100-103.

4) Лебедева К.Е. Методика повышения надежности видеоконференцсвязи / К.Е. Лебедева, Р.В. Лебедев, А.В. Мурыгин // Сибирский журнал науки и технологий. – 2017. – № 2. – Т. 18. – С. 274-282.

В журналах, входящих в перечень рецензируемых научных журналов и изданий в системе Web of Science:

5) R.V. Lebedev, A.V. Murigin and V.S. Tynchenko. Resource management in client-server computing systems based on trust assessment // APITECH II Journal of Physics: Conference Series 1679 (2020) 032030 IOP Publishing doi:10.1088/1742-6596/1679/3/032030.

В других изданиях:

6) Лебедев Р.В. Подход к оценке сходства объектов компьютерных систем с эталоном // Сборник научных статей по итогам IX международной научной конференции «Приоритетные направления инновационной деятельности в промышленности». – Казань: ООО «Конверт», 2020. – Ч. 2. – С. 25-29.

7) Шипулин П.М. Вариант защищенного доступа к конфиденциальным ресурсам локальной сети / П.М. Шипулин, Р.В. Лебедев, А.В. Хандожко, И.В.

Потуремский // В сборнике: Актуальные вопросы проектирования автоматических космических аппаратов для фундаментальных и прикладных научных исследований. – М.: АО «НПО Лавочкина», 2017. – С. 558-565.

8) Пузиков А.М. Организация автоматизированного контроля состояний компонентов систем информационной безопасности / А.М. Пузиков, Р.В. Лебедев // Решетневские чтения. 2014. Т. 2. № 18. С. 326-328.

9) Игнатенко В.Н. Контроль установки и функционирования системы аудита программно-аппаратной части рабочих станций корпоративной сети / // Решетневские чтения: материалы XV Международной научной конференции (10-12 ноября 2011, г. Красноярск): в 2 ч. – 2011. – Ч. 2. – С. 572-573.

10) Лебедев Р.В. Система контроля программно-аппаратной части рабочих станций корпоративной сети / Р.В. Лебедев, В.Н. Игнатенко, И.В. Потуремский // Решетневские чтения: материалы XV Международной научной конференции (10-12 ноября 2011, г. Красноярск): в 2 ч. – 2011. – Ч. 2. – С. 578-579.

Зарегистрированные программные средства:

1) Программа анализа связей между узлами корпоративной вычислительной сети. Свидетельство о государственной регистрации программы для ЭВМ № 2020660233 / Лебедев Р.В. // Правообладатель: АО «Информационные спутниковые системы» имени академика М.Ф. Решетнева. Дата государственной регистрации в Реестре программ для ЭВМ 31.08.2020.

# СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АРМ: Автоматизированное рабочее место персональный компьютер, ПЭВМ;

ИТКС: Информационно-телекоммуникационная сеть;

ИС: Информационная система;

ЛВС: Локальная вычислительная сеть;

МЭ: Межсетевой экран;

ОПК: Оборонно-промышленный комплекс;

ОПО: Общесистемное программное обеспечение;

ОС: Операционная система;

ПО: Программное обеспечение;

ПЭВМ: Персональная электронно-вычислительная машина;

САПР: Система автоматизированного проектирования;

СМО: Система массового обслуживания;

СПО: Специализированное программное обеспечение;

СППР: Система поддержки принятия решений;

СУБД: Система управления базами данных;

ФСТЭК: Федеральная служба по техническому и экспортному контролю;

ЦОД: Центр обработки данных;

ЭВМ: Электронно-вычислительная машина;

ABAC (англ. Attribute Based Access Control): Подход к управлению доступом на основе атрибутов;

ACL (англ. Access Control List): Формализованный список разрешающих правил межсетевого экрана;

CBAC (англ. Context Based Access Control): Подход к управлению доступом на основе контекстной информации о субъекте, объекте и условиях доступа;

IaaS (англ. Infrastructure as a Service): Концепция предоставления вычислительных ресурсов в формате инфраструктуры вычислительной системы;

IoT (англ. Internet of Things): Технологии интернета вещей;

IP (англ. Internet Protocol): Протокол сетевой передачи данных;

PaaS (англ. Platform as a Service): Концепция предоставления вычислительных ресурсов в формате технических средств;

QoS (англ. Quality of Service): Технология управления качеством передачи данных в компьютерных сетях;

RBAC (англ. Role Based Access Control): Подход к управлению доступом на основе ролей;

SaaS (англ. Software as a Service): Концепция предоставления вычислительных ресурсов в форме программного обеспечения;

TCP (англ. Transmission Control Protocol): Протокол транспортного уровня протоколов TCP/IP;

TCP/IP: Стек сетевых протоколов передачи данных в IP-сетях.

# ПРИЛОЖЕНИЕ А

## Свидетельство о регистрации программы для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

# СВИДЕТЕЛЬСТВО

**о государственной регистрации программы для ЭВМ**

**№ 2020660233**

**Программа анализа связей между узлами корпоративной вычислительной сети**

Правообладатель: ***Акционерное общество «Информационные спутниковые системы» имени академика М.Ф. Решетнёва» (RU)***

Автор: ***Лебедев Роман Владимирович (RU)***

Заявка № **2020619350**
Дата поступления **19 августа 2020 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***31 августа 2020 г.***

*Руководитель Федеральной службы по интеллектуальной собственности*

*Г.П. Ивлиев*

# ПРИЛОЖЕНИЕ Б

## Справка о внедрении результатов диссертационной работы

Акционерное общество
«ИНФОРМАЦИОННЫЕ СПУТНИКОВЫЕ СИСТЕМЫ»
имени академика М.Ф. Решетнёва»

РЕШЕТНЕВ
АО «ИСС»

ул. Ленина, д. 52, г. Железногорск, ЗАТО Железногорск, Красноярский край, Российская Федерация, 662972
Тел. (3919) 76-40-02, 72-24-39, Факс (3919) 72-26-35, 75-61-46, e-mail: office@iss-reshetnev.ru, http: //www.iss-reshetnev.ru
ОГРН 1082452000290, ИНН 2452034898

**УТВЕРЖДАЮ**
Начальник управления информатики
и вычислительной техники
_____ И. В. Потуремский
«21» 10 2020 г.

**СПРАВКА**
о внедрении результатов диссертационной работы
Лебедева Романа Владимировича «Управление доступом в клиент-серверных информационных системах на основе оценки доверия к субъектам доступа»

Модель оценки доверия к субъектам доступа, предложенная в диссертационной работе используется в системе поддержки принятия решений при согласовании допуска персонала к работе со специализированными информационными ресурсами и сервисами. Метод управления доступом на основе оценки доверия планируется к внедрению в систему управления доступом к вычислительным ресурсам корпоративной системы виртуализации графических задач и к серверам распределения конкурентных лицензий. Техническая модель клиент-серверной информационной системы, реализующая метод управления доступом на основе оценки доверия к субъектам, применена при разработке концепции и технического проекта корпоративной распределенной автоматизированной системы обработки служебной информации.

Начальник отдела 714 Ю. М. Ершов

# ПРИЛОЖЕНИЕ В

## Исходные данные для ранжирования критериев доверия

Общий вид опросного листа экспертов приведен в таблице В.1, заполненные листы экспертов в таблицах В.2-В.11.

Таблица В.1 – Общий вид опросного листа для экспертов (и пример заполнения).

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | | | | | | | | | | + | + | + |
| 2 | | | | | | + | + | | | | | | |
| 3 | | | | | + | | | + | | + | | | |
| 4 | | | | + | | | | | + | | | | |
| 5 | | + | | | | | | | | | | | |
| 6 | + | | + | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Примечание

| | |
|---|---|
| Ad_fail | Способ управления учетной записью клиента |
| Usr_arm | Сведения о допуске клиента к работам класса 1 |
| Usr_krm | Сведения о допуске клиента к работам класса 2 |
| Au_fail | Наличие набора 1 программного обеспечения клиента |
| Av_fail | Наличие набора 2 программного обеспечения клиента |
| Au_flsh | Наличие набора 1 технических средств клиента |
| Au_mdm | Наличие набора 2 технических средств клиента |
| Au_game | Наличие набора 3 технических средств клиента |
| Astra_1 | Наличие событий типа 1 системы безопасности |
| Astra_2 | Наличие событий типа 2 системы безопасности |
| Astra_3 | Наличие событий типа 3 системы безопасности |
| Av_infct | Наличие событий типа 1 системы мониторинга |
| Av_dsbl | Наличие событий типа 2 системы мониторинга |

Правила заполнения и обработки опросного листа:

– Эксперт ставит отметку в ячейке опросной таблице для каждого критерия доверия согласно его приоритету (растет с увеличением ранга);

– Для одного критерия может быть поставлено несколько отметок, однако при обработке учитываются отметки, соответствующие максимальному рангу;

– При заполнении опросной таблицы не должно оставаться пустых строк.

Таблица В.2 – Опросный лист эксперта 1.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | | | + | |
| 3 | | | | | | | + | | | + | | | + |
| 4 | | | | | | + | | | + | | | | |
| 5 | | | | + | | | | | | | | | |
| 6 | + | | | | + | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.3 – Опросный лист эксперта 2.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | | | + | |
| 3 | | | | | | | + | | | + | | | + |
| 4 | | | | | | + | | | + | | | | |
| 5 | + | | | + | + | | | | | | | | |
| 6 | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.4 – Опросный лист эксперта 3.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | | | + | |
| 3 | | | | | | | | | | + | | | |
| 4 | | | | | | | | | + | | | | + |
| 5 | | | | | | + | + | | | | | | |
| 6 | + | | | + | + | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.5 – Опросный лист эксперта 4.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | + | | | |
| 3 | | | | | | | | | + | | | + | |
| 4 | | | | | | + | + | | | | | | + |
| 5 | + | | | + | + | | | | | | | | |
| 6 | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.6 – Опросный лист эксперта 5.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | | | |
| 2 | | | | | | | | + | | + | + | | |
| 3 | | | | | | | | | + | | | + | |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | | | | | | + | + | | | | | | + |
| 5 | | | | + | | | | | | | | | |
| 6 | + | | | | + | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.7 – Опросный лист эксперта 6.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | | | |
| 2 | | | | | | | | + | | + | + | | |
| 3 | | | | | | + | + | | + | | | + | |
| 4 | | | | | | | | | | | | | + |
| 5 | | | | + | | | | | | | | | |
| 6 | + | | | | + | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.8 – Опросный лист эксперта 7.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | + | | | |
| 3 | | | | | | + | | | + | | | + | |
| 4 | | | | | | | + | | | | | | + |
| 5 | | | | + | + | | | | | | | | |
| 6 | + | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.9 – Опросный лист эксперта 8.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | | | |
| 2 | | | | | | | | + | | + | + | | |
| 3 | | | | | | + | | | + | | | + | |
| 4 | | | | | | | + | | | | | | + |
| 5 | + | | | + | + | | | | | | | | |
| 6 | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.10 – Опросный лист эксперта 9.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | + | | |
| 2 | | | | | | | | + | | + | | | |
| 3 | | | | | | | | | + | | | + | |
| 4 | | | | | | + | + | | | | | | + |
| 5 | | | | + | | | | | | | | | |
| 6 | + | | | | + | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Таблица В.11 – Опросный лист эксперта 10.

| Ранг | Критерии доверия | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_arm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Au_game | Astra_1 | Astra_2 | Astra_3 | Av_infct | Av_dsbl |
| 1 | | + | + | | | | | | | | | | |
| 2 | | | | | | | | + | | + | + | | |
| 3 | | | | | | | | | + | | | + | |
| 4 | | | | | | + | + | | | | | | + |
| 5 | + | | | + | + | | | | | | | | |
| 6 | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

Матрицы парных сравнений $A^{\langle y \rangle}$, составленные на основе опросных листов экспертов, индекс $y = 1, \dots, 10$ обозначает номер эксперта. Столбцы матриц соответствуют порядку критериев доверия в опросном листе. Элемент матрицы $a_{ij}$ равен 1, если ранг критерия $m_i$ равен либо превосходит ранг $m_j$.

$$A^{\langle 1 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 2 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 3 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 4 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 5 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 6 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 7 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 8 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 9 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A^{\langle 10 \rangle} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

## ПРИЛОЖЕНИЕ Г

### Расчет значений оценки доверия для выборки клиентов системы

В таблице Г.1 приведены расчетные значения критериев доверия и итоговое значение оценки доверия для выборки из 400 клиентов.

Таблица Г.1 – Расчет оценки доверия

| Номер клиента | Проверка критериев доверия | | | | | | | | | | | | | Оценка доверия |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ad_fail | Usr_aarm | Usr_krm | Au_fail | Av_fail | Au_flsh | Au_mdm | Av_dsbl | Astra_1 | Astra_2 | Astra_3 | Au_game | Av_infct | |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0,093 | 0,081 | 0 | 0 | 0 | 0 | 0,760 |
| 5 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 8 | 0,137 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,739 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 10 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,827 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,912 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 15 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0,034 | 0 | 0 | 0,682 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 18 | 0,137 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,729 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 20 | 0 | 0 | 0,134 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,817 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,885 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 24 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,822 |
| 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 26 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,927 |
| 27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 28 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 29 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0,093 | 0 | 0 | 0,034 | 0 | 0 | 0,781 |
| 30 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 31 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 32 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 33 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0,081 | 0 | 0 | 0,024 | 0,024 | 0,805 |
| 34 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 35 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 36 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,829 |
| 37 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 38 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0,034 | 0 | 0 | 0,885 |
| 39 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,897 |
| 40 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,695 |
| 41 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 42 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,761 |
| 43 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 44 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 45 | 0,137 | 0 | 0,134 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,680 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 46 | 0 | 0,124 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,742 |
| 47 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0,946 |
| 48 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0,874 |
| 49 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 50 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0,854 |
| 51 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,907 |
| 52 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0,024 | 0,798 |
| 53 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0,093 | 0 | 0,054 | 0 | 0 | 0,024 | 0,763 |
| 54 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,715 |
| 55 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,897 |
| 56 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 57 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 58 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0,024 | 0,895 |
| 59 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,791 |
| 60 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 61 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 62 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 63 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,827 |
| 64 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,809 |
| 65 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 66 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 67 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 68 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 69 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,874 |
| 70 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 71 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,917 |
| 72 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 73 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 74 | 0 | 0,124 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,702 |
| 75 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 76 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 77 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 78 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,900 |
| 79 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,024 | 0,791 |
| 80 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 81 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 82 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,866 |
| 83 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 84 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0,024 | 0,818 |
| 85 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 86 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,853 |
| 87 | 0,137 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,737 |
| 88 | 0 | 0,124 | 0,134 | 0,093 | 0 | 0,049 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,519 |
| 89 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 90 | 0,137 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,770 |
| 91 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 92 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 93 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 94 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 95 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0,081 | 0,054 | 0 | 0 | 0 | 0,799 |
| 96 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 97 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,912 |
| 98 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 99 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 100 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,880 |
| 101 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 102 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,024 | 0,710 |
| 103 | 0 | 0 | 0,134 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,720 |
| 104 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 105 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,842 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 106 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 107 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,910 |
| 108 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 109 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 110 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 111 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0,093 | 0,081 | 0,054 | 0 | 0 | 0 | 0,638 |
| 112 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,729 |
| 113 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,863 |
| 114 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,842 |
| 115 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 116 | 0 | 0 | 0 | 0,093 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0,034 | 0,024 | 0,024 | 0,722 |
| 117 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0,034 | 0 | 0 | 0,792 |
| 118 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 119 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 120 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 121 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 122 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 123 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,859 |
| 124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 125 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,782 |
| 126 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,795 |
| 127 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 128 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,729 |
| 129 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 130 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 131 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0,024 | 0,764 |
| 132 | 0 | 0,124 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,749 |
| 133 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 135 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 136 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,873 |
| 137 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 138 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0,024 | 0,942 |
| 139 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 140 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 141 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,839 |
| 142 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 143 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,797 |
| 144 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,900 |
| 145 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 146 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0,034 | 0 | 0,024 | 0,861 |
| 147 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,853 |
| 148 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 149 | 0,137 | 0,124 | 0 | 0,093 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,580 |
| 150 | 0,137 | 0,124 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,559 |
| 151 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,795 |
| 152 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,024 | 0,883 |
| 153 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 154 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,976 |
| 155 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 156 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 157 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 158 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 159 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 160 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,739 |
| 161 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 162 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 163 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 164 | 0,137 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,739 |
| 165 | 0 | 0,124 | 0 | 0,093 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,691 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 166 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 167 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,770 |
| 168 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |
| 169 | 0 | 0,124 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,742 |
| 170 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 171 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0,024 | 0 | 0,850 |
| 172 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,827 |
| 173 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 174 | 0,137 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,739 |
| 175 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 176 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,825 |
| 177 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 178 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,839 |
| 179 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0,066 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,717 |
| 180 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,783 |
| 181 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0,024 | 0 | 0,856 |
| 182 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,788 |
| 183 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 184 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,815 |
| 185 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,826 |
| 186 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |
| 187 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,795 |
| 188 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 189 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0,054 | 0 | 0 | 0 | 0,741 |
| 190 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,810 |
| 191 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 192 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 193 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 194 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 195 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 196 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0,081 | 0 | 0 | 0 | 0 | 0,826 |
| 197 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,839 |
| 198 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,827 |
| 199 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,024 | 0,790 |
| 200 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 201 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 202 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 203 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 204 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 205 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,853 |
| 206 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,976 |
| 207 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |
| 208 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,866 |
| 209 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 210 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0,034 | 0 | 0 | 0,792 |
| 211 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0,066 | 0,093 | 0 | 0,054 | 0,034 | 0 | 0 | 0,660 |
| 212 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 213 | 0,137 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,814 |
| 214 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0,054 | 0 | 0 | 0,024 | 0,841 |
| 215 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 216 | 0 | 0,124 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,708 |
| 217 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,846 |
| 218 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 219 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0,034 | 0 | 0 | 0,873 |
| 220 | 0 | 0,124 | 0 | 0,093 | 0,092 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,591 |
| 221 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |
| 222 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,866 |
| 223 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,866 |
| 224 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,912 |
| 225 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0,093 | 0 | 0 | 0 | 0 | 0,024 | 0,817 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 226 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,738 |
| 227 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 228 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 229 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,885 |
| 230 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,822 |
| 231 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0,066 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,707 |
| 232 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,841 |
| 233 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 234 | 0,137 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0,024 | 0 | 0,756 |
| 235 | 0,137 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,705 |
| 236 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,782 |
| 237 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 238 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 239 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 240 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0,066 | 0,093 | 0,081 | 0 | 0 | 0 | 0 | 0,668 |
| 241 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 242 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0,024 | 0,856 |
| 243 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,853 |
| 244 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,854 |
| 245 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0,034 | 0 | 0 | 0,780 |
| 246 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 247 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,822 |
| 248 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,885 |
| 249 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 250 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 251 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,800 |
| 252 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |
| 253 | 0,137 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,771 |
| 254 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,814 |
| 255 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 256 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,815 |
| 257 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 258 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,917 |
| 259 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,797 |
| 260 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 261 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 262 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 263 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 264 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 265 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,897 |
| 266 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,853 |
| 267 | 0 | 0 | 0,134 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,719 |
| 268 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0,024 | 0 | 0,942 |
| 269 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,668 |
| 270 | 0 | 0 | 0 | 0,093 | 0,092 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,761 |
| 271 | 0,137 | 0,124 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,673 |
| 272 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,815 |
| 273 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,775 |
| 274 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 275 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 276 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 277 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 278 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 279 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 280 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 281 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,831 |
| 282 | 0 | 0 | 0 | 0,093 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,766 |
| 283 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 284 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 285 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,859 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 286 | 0 | 0 | 0,134 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,739 |
| 287 | 0,137 | 0 | 0 | 0,093 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,631 |
| 288 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 289 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 290 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 291 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,927 |
| 292 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,770 |
| 293 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 294 | 0,137 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,814 |
| 295 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,776 |
| 296 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,773 |
| 297 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 298 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,814 |
| 299 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,917 |
| 300 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0,024 | 0,818 |
| 301 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 302 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,917 |
| 303 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,827 |
| 304 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 305 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 306 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,900 |
| 307 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0,054 | 0 | 0,024 | 0 | 0,841 |
| 308 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,910 |
| 309 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0,034 | 0 | 0 | 0,885 |
| 310 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 311 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,827 |
| 312 | 0 | 0 | 0,134 | 0 | 0,092 | 0 | 0 | 0,093 | 0,081 | 0 | 0 | 0 | 0 | 0,600 |
| 313 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,842 |
| 314 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,885 |
| 315 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,863 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 316 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,866 |
| 317 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,976 |
| 318 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0,946 |
| 319 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0,024 | 0 | 0,910 |
| 320 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 321 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 322 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 323 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,858 |
| 324 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 325 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,912 |
| 326 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 327 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0,066 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,748 |
| 328 | 0,137 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,770 |
| 329 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,829 |
| 330 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,761 |
| 331 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 332 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 333 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,976 |
| 334 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0,054 | 0 | 0 | 0 | 0,853 |
| 335 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 336 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 337 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 338 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0,034 | 0 | 0 | 0,912 |
| 339 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 340 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,880 |
| 341 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 342 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 343 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0,024 | 0 | 0,758 |
| 344 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 345 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 346 | 0 | 0,124 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,784 |
| 347 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0,081 | 0 | 0 | 0,024 | 0 | 0,802 |
| 348 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 349 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,805 |
| 350 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 351 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,910 |
| 352 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,831 |
| 353 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 354 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 355 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 356 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,797 |
| 357 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,858 |
| 358 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0,024 | 0 | 0,942 |
| 359 | 0 | 0 | 0 | 0,093 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0,024 | 0,708 |
| 360 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,927 |
| 361 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 362 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 363 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 364 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 365 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 366 | 0 | 0,124 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,793 |
| 367 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 368 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,876 |
| 369 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,859 |
| 370 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 371 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0,024 | 0,927 |
| 372 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 373 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,826 |
| 374 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 375 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0,024 | 0,798 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 376 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 377 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 378 | 0 | 0 | 0 | 0 | 0,092 | 0,049 | 0 | 0,093 | 0,081 | 0 | 0 | 0,024 | 0 | 0,661 |
| 379 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,966 |
| 380 | 0 | 0 | 0,134 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,773 |
| 381 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,885 |
| 382 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 383 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 384 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 385 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,951 |
| 386 | 0 | 0 | 0,134 | 0,093 | 0 | 0,049 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,724 |
| 387 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,897 |
| 388 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 389 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,782 |
| 390 | 0,137 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,829 |
| 391 | 0 | 0,124 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,034 | 0 | 0 | 0,842 |
| 392 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,081 | 0 | 0 | 0 | 0 | 0,919 |
| 393 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0,054 | 0 | 0,024 | 0 | 0,856 |
| 394 | 0 | 0 | 0 | 0 | 0 | 0,049 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,897 |
| 395 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,093 | 0 | 0 | 0 | 0 | 0 | 0,907 |
| 396 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,054 | 0 | 0 | 0 | 0,946 |
| 397 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |
| 398 | 0 | 0 | 0 | 0 | 0 | 0 | 0,066 | 0 | 0 | 0 | 0 | 0 | 0 | 0,934 |
| 399 | 0 | 0 | 0 | 0 | 0,092 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0,908 |
| 400 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1,000 |