Федеральное государственное автономное образовательное учреждение
высшего образования "Уральский федеральный университет
имени первого Президента России Б.Н. Ельцина"

На правах рукописи

Магомедов Шамиль Гасангусейнович

Модели и методы адаптивного риск-ориентированного управления доступом в распределенных информационных системах

Специальность 2.3.6.
Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание учёной степени
доктора технических наук

Екатеринбург — 2025

Работа выполнена на кафедре КБ-4 "Интеллектуальные системы информационной безопасности" Института кибербезопасности и цифровых технологий ФГБОУ ВО "МИРЭА – Российский технологический университет".

Научный консультант: доктор технических наук, профессор
Никульчев Евгений Витальевич

Официальные оппоненты: **Баранкова Инна Ильинична,** доктор технических наук, доцент, ФГБОУ ВО "Магнитогорский государственный технический университет им. Г. И. Носова", заведующая кафедрой информатики и информационной безопасности;

Духан Евгений Изович, доктор технических наук, профессор, войсковая часть № 69617, военнослужащий;

Котенко Игорь Витальевич, доктор технических наук, профессор, ФГБУН "Санкт-Петербургский Федеральный исследовательский центр Российской академии наук", главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности;

Защита состоится 04 марта 2025 г. в 11:00 на заседании диссертационного совета УрФУ 2.3.12.13 по адресу: 620062, г. Екатеринбург, ул. Мира, 19, ауд. И-420 (зал Ученого совета).

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО "Уральский федеральный университет имени первого Президента России Б.Н. Ельцина".
`https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=6629`

Автореферат разослан "____" _____ 2024 года.

Ученый секретарь
диссертационного совета Сафиуллин Николай Тахирович

Общая характеристика работы

Актуальность темы. Изменение геополитической обстановки в последние годы привело к необходимости пересмотра не только текущих аспектов защиты информации, но и фундаментальных основ в области информационной безопасности. Одним из базовых принципов в процессе обеспечения информационной безопасности является применение политик безопасности, позволяющих реализовывать на практике технические, организационные и правовые меры по обеспечению защищенности как объектов критической информационной инфраструктуры и государственных информационных систем, так и обрабатываемой информации. Существующие подходы к управлению безопасностью основаны на применении статических политик безопасности управления доступом на объектах критической информационной инфраструктуры, распределенных информационных системах и других объектах защиты.

Традиционные модели управления доступом используют логику доступа к ресурсам на основе правил управления доступом. Подобный подход решает большинство проблем при разграничении доступа к объектам, однако имеет существенный недостаток, заключающийся в применении статичных, предопределенных политик безопасности, которые не позволяют гибко обеспечивать безопасность объектов доступа в изменяющихся условиях окружающей обстановки. Важным фактором является не только обеспечение безопасности доступа, но и повышение доступности ресурсов – баланс между безопасностью и живучестью. Зачастую избыточные меры безопасности могут существенно снижать доступность услуг. Обеспечение выполнения данного баланса мер возможно за счет использования адаптивных методов управления доступом в изменяющихся условиях.

Критическая информационная инфраструктура (КИИ) и образовательные вычислительные сервисы, имеют ряд общих черт, которые позволяют рассматривать их в одном контексте. Во-первых, и КИИ, и образовательные вычислительные сервисы представляют собой важные информационные системы, от надежности и безопасности которых зависит функционирование критически важных объектов и процессов. Во-вторых, и в КИИ, и в образовательных вычислительных сервисах необходимо обеспечивать высокий уровень информационной безопасности для защиты конфиденциальности, целостности и доступности данных. Это включает в себя меры по выявлению угроз, анализу уязвимостей, установке средств защиты и контролю за безопасностью. В-третьих, переход к современным образовательным вычислительным сервисам, таким как облачные платформы, позволяет повысить доступность, гибкость и отказоустойчивость вычислительных ресурсов, что схоже с задачами обеспечения непрерывности функционирования объектов КИИ. Наконец, и КИИ, и

образовательные вычислительные сервисы требуют высокой точности работы системы управления доступом, позволяя выявлять нелегитимных пользователей и злоумышленников, получивших доступ к аккаунтам легитимных пользователей. Таким образом, несмотря на различия в сферах применения, КИИ и образовательные вычислительные сервисы объединяет необходимость обеспечения информационной безопасности критически важных информационных систем, что позволяет рассматривать их в едином контексте диссертационного исследования.

Для гранулярного управления доступом и организации противодействия деятельности злоумышленников в гетерогенных, распределенных системах возникла необходимость находить новые, адаптивные подходы к решению данных проблем, а также подходы, основанные на оценке рисков информационной безопасности. Задачи, которые ставятся перед средствами защиты, требуют детального анализа контекста (условий выполнения), адаптации под изменяющиеся условия работы, в зависимости от определенных значений индикаторов и уровня риска угроз информационной безопасности образовательных вычислительных сервисов (ОВС). Совершенствование инструментов управления доступом с целью повышения оперативности реагирования и адаптивности является актуальной проблемой, имеющей важное практическое значение для большого количества распределенных информационных систем, например, таких как ОВС.

В настоящее время все больше образовательных услуг переносится в цифровую среду. Основным инструментом цифровой среды обучающихся всех видов и форм обучения становятся образовательные вычислительные сервисы и специализированные приложения, подключенные к распределенным информационным системам сферы образования. При организации доступа к таким системам необходимо осуществлять идентификацию и аутентификацию пользователей, управлять доступом к ресурсам, контролировать передачу и прием данных, обеспечивать целостность системы.

Существующие подходы к управлению доступом не в полной мере адаптируются к задачам ОВС, так как помимо классической задачи управления доступом необходимо учитывать особенности реализации учебного процесса на базе распределенных информационных систем. Анализ научной литературы в предметной области исследований показал, что частично это можно учесть за счет использования ролевых и атрибутивных моделей, но комплексно проблему возможно решить за счет применения риск-ориентированного атрибутивного управления доступом. Это дает возможность представить задачу управления доступом в ОВС в качестве задачи, для решения которой необходимы специализированные теоретические и практические исследования для разработки моделей и методов управления доступом, ориентированных на решение задач обеспечения безопасности доступа при максимальной доступности услуг.

Анализ международных стандартов позволяет выделить специализированные задачи, связанные с организацией управления доступом и анализа рисков. В разделе A.9 ISO/IEC 27001:2013 ("Information technology – Security techniques – Information security management systems – Requirements") указаны требования к управлению доступом, включая политику доступа, идентификацию и аутентификацию, управление привилегиями и доступом. В разделе 9.2 ISO/IEC 27002:2013 ("Information technology – Security techniques – Code of practice for information security controls") представлены рекомендации и контрольные меры для управления доступом в соответствии с принятой политикой и требованиями стандарта. Целью документа ENISA Guidelines on Access Control (European Union Agency for Cybersecurity) являются организация и обеспечение безопасности и управления доступом к информационным ресурсам, снижение рисков и обеспечение конфиденциальности, целостности и доступности данных.

OASIS XACML (eXtensible Access Control Markup Language) является стандартом для унифицированного представления и обработки политик доступа. Он обеспечивает гибкую систему управления доступом и позволяет определять правила на основе различных атрибутов пользователя и контекста. ANSI INCITS 359-2004 ("Role-Based Access Control (RBAC)") определяет ролевую модель управления доступом (RBAC), которая использует роли для определения прав доступа пользователей и описывает стандартные спецификации и рекомендации по реализации, а также методы для разработки и внедрения RBAC. NIST SP 800-162 ("Guide to Attribute Based Access Control (ABAC) Definition and Considerations") предоставляет описание и рекомендации по использованию модели управления доступом на основе атрибутов (ABAC). Модель ABAC представляет собой подход к управлению доступом, основанный на использовании атрибутов пользователей, ресурсов и условий для принятия решений о предоставлении доступа.

ISO/IEC 27005:2018 ("Information technology – Security techniques – Information security risk management") устанавливает общие принципы и указания по управлению рисками информационной безопасности. Он включает в себя рекомендации по идентификации, оценке и управлению рисками, связанными с управлением доступом. В документе ISO/IEC 31000:2018 ("Risk management – Guidelines") определены принципы, руководства и рекомендации по управлению рисками, содержится методология проведения оценки рисков и принятия решений по управлению доступом. В NIST SP 800-30 Rev. 1 ("Guide for Conducting Risk Assessments") представлены методы и процедуры идентификации и оценки рисков управления доступом. Требования к системам управления информационной безопасностью, в т. ч. основные положения о риске и риск-ориентированном подходе, определены в стандарте ISO/IEC 27001:2013 ("Information

technology – Security techniques – Information security management systems – Requirements"). FAIR (Factor Analysis of Information Risk) представляет методологию оценки рисков, связанных с информационной безопасностью. ISO/IEC 21827:2008 ("Systems Security Engineering – Capability Maturity Model (SSE-CMM)") включает рекомендации и практики, связанные с управлением рисками в процессе разработки и настройки систем управления доступом.

Существует также организационно-методическое обеспечение управления доступом и анализу рисков в отечественных стандартах и документах. ГОСТ Р ИСО/МЭК 27005-2018 "Информационная технология. Методы управления рисками информационной безопасности" служит аналогом ISO/IEC 27005:2018 и устанавливает общие принципы и подходы к управлению рисками информационной безопасности, включая управление рисками, связанными с управлением доступом. В ГОСТ Р 54818-2011 "Система стандартов по информационной безопасности. Риск-ориентированный подход" определены основные принципы и требования к риск-ориентированному подходу в области информационной безопасности. В ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы управления информационной безопасностью", который является аналогом ISO/IEC 27001:2013, установлены основные требования к системам управления информационной безопасностью, включены положения о риске и управлении рисками, которые охватывают и управление доступом.

"Методические рекомендации по принципам информационной безопасности государственных информационных систем" ФСТЭК России включают рекомендации по управлению рисками, связанными с управлением доступом в контексте государственных систем. Руководство ФСБ России "О мерах по управлению рисками информационной безопасности" охватывает также аспекты управления рисками, связанные с управлением доступом к информационным ресурсам. ГОСТ Р 52091-2003 "Система менеджмента качества защиты информации. Риск-ориентированный подход" определяет требования к системе менеджмента качества защиты информации с использованием риск-ориентированного подхода, включая требования и методы управления рисками, связанными с управлением доступом.

В ГОСТ Р ИСО/МЭК 27004-2019 "Информационная технология. Методы оценки и измерения эффективности управления информационной безопасностью" представлены методы оценки и измерения эффективности управления информационной безопасностью. ГОСТ Р ИСО/МЭК 27002-2017 "Информационная технология. Методы контроля безопасности. Практическое руководство" (аналог ISO/IEC 27002:2013) содержит рекомендации по использованию методик обеспечения безопасности информации, в т. ч. руководство по управлению рисками, связанными с управлением доступом.

Исходя из анализа представленных нормативно-правовых актов и документов, возможно сделать вывод о необходимости доработки существующих механизмов управления доступом, поскольку большинство из них использует классические подходы на основе мандатных и ролевых моделей. Риск-ориентированный подход позволит решить вопросы гибкости управления доступом и удобства использования сервисов студентами и преподавателями. Таким образом, при выборе модели управления доступом необходимо учитывать специфику организации, ее размер, динамику и другие факторы, чтобы найти оптимальный баланс между безопасностью, гибкостью и удобством администрирования.

Анализ организационно-методического обеспечения в части вопросов реализации риск-ориентированных систем управления доступом показывает, что, несмотря на большое количество общих рекомендаций и методик, для каждой области применения и реализации конкретных систем в зависимости от сферы применения требуется разработка специализированных моделей и методов, направленных на совершенствование механизмов управления защищенностью распределенных информационных систем.

Таким образом, разработка моделей и методов риск-ориентированного атрибутивного управления доступом является актуальной проблемой, имеющей важное теоретическое и практическое значение для информационной безопасности распределенных информационных систем.

Степень разработанности проблемы. Развитие методов управления доступом и анализа рисков – актуальные направления в сфере информационной безопасности. Исследованиями по данным направлениям занимаются многие отечественные и зарубежные ученые.

Разработаны многочисленные модели и методы управления доступом, развивающие классические подходы. К наиболее значимым результатам в этом направлении следует отнести работы Девянина П.Н., Гайдамакина Н.А., Котенко И.В., Лепешкина О.М., Харечкина П.В., Козачка А.В., Зегжды Д.П., Калинина М.О., Бурлова В.Г. В разработке дискреционных моделей управления доступом участвовали: Миронов В.Г., Шелупанов А.А., Югов Н.Т., Киреенко А.Е., Щеглов А.Ю., Osborn S., Sandhu R., Munawer Q., Li N., Tripunitara M.V., Moffett J.D., Jaeger T., Prakash A. Мандатным моделям управления доступом были посвящены исследования: Lindqvist H., Nyanchama M., Osborn S., McCune J.M., Jaeger T., Berger S., Caceres R., Sailer R., Ray I., Kumar M., Jiang Y., Lin C., Yin H., Tan Z., Кулямина В.В., Петренко А.К., Хорошилова А.В., Щепеткова И.В., Колегова Д.Н., Ткаченко Н.О. Разработкой ролевых моделей управления доступом занимались исследователи: Calvo M., Beltrán M., Cheng P.C., Rohatgi P., Keser C., Karger P.A., Wagner G.M., Reninger A.S., Ferraiolo D.F., Sandhu R., Gavrila S., Kuhn D.R., Chandramouli R. Исследованиям в области разграничения доступа на основе атрибутов посвятили свои работы Hu V.C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K.,

Miller R., Scarfone K., Fu X., Nie X., Wu T., Li F., Servos D., Osborn S.L., Ding S., Cao J., Li C., Fan K., Li H., Voas J., Пономарев К.Ю. Риск-ориентированным управлением доступа занимались ученые Зотова А.И., Кириченко М.В., Коробко С.А., Корниенко А.А., Глухов А.П., Диасамидзе С.В., Глухарев М.Л., Бирюков Д.Н., Black J., Baldwin R., Schwander H., Häusermann S., Cheng P.C., Rohatgi P., Keser C., Karger P.A., Wagner G.M., Reninger A.S.

Перспективным направлением развития систем управления доступом многопользовательских сервисов является анализ поведения пользователей – технологии UBA (User Behavior Analytics). Предложены различные варианты развития UBA: использование интеллектуальных технологий, применение встраиваемых динамических моделей в интернет-приложения (Миронов В.В. и соавт.); ситуационные и прецедентные модели (Csaba K., Peter H. B., Xi X., Zhang T. и др.). Методы поведенческого анализа впервые описаны в работе Скиннера Б.Ф. в 1953 г. и изначально относились к психологическим исследованиям, долгое время оставаясь в домене медицинских исследований. Только в начале XXI века, с появлением технологий поиска информации (Hand D.J.) и машинного обучения (Nasrabadi N.M.) появляются основы применения методов анализа поведения пользователей в сфере информационной безопасности. В настоящее время применяются такие термины как пользовательская информатика (Cao L., Joachims T., Wang C., Gaussier E., Li J., Ou Y., Luo D., Zafarani R., Liu H., Xu G.) и аналитика поведения пользователей (Ryu S., Kang Y.J., Lee H.). Поведенческий анализ – это специфическая область, которая фокусируется на моделировании поведения пользователей в области кибербезопасности. Таким образом, она описывает методы анализа поведения пользователей для обнаружения кибератак и мошенничества, исследованиями в данном направлении занимались ученые Litan A., Nicolett M., Chandola V., Banerjee A., Kumar V.

Предложены различные варианты развития поведенческого анализа: использование интеллектуальных технологий, применение встраиваемых динамических моделей в интернет-приложения (Миронов В.В., Гусаренко А.С.); ситуационные и прецедентные модели (Csaba K., Peter H.B., Xi X., Zhang T. и др.). Также следует отметить разработку методов непрерывной аутентификации, отраженную в исследованиях авторов: Patel V.M., Chellappa R., Chandra D., Barbello B., Stylios I., Kokolakis S., Thanou O., Chatzis S., Mekruksavanich S., Jitpattanakul A., Mosenia A., Sur-Kolay S., Raghunathan A., Jha N.K. Обширный кластер исследований относится к методам непрерывной аутентификации на основе биометрии: распознавание лиц (Crouse D., Han H., Chandra D., Barbello B., Jain A.K., Samangouei P., Patel V.M., Chellappa R., Perera P., Кудинов А.А., Елсаков С.М.); распознавание голоса (Feng H., Fawaz K., Shin K.G., Miguel-Hurtado O., Blanco-Gonzalo R., Guest R., Lunerti C., Zhang L., Tan S., Yang J.); анализ

нажатия клавиш (Bours P., Mondal S., Barghouthi H., Pinto P., Patrão B., Santos H., Stylios I., Skalkos A., Kokolakis S., Karyda M.) и движения мыши (Mondal S., Bours P., Shen C., Cai Z., Guan X., Gao L., Lian Y., Yang H., Xin R., Yu Z., Chen W., Cheng Y., Sayed B., Traoré I., Woungang I., Obaidat M.S.).

Методы количественной оценки риска играют важную роль в информационной безопасности. Их применение дает возможность предсказать и предотвратить потенциальные угрозы. К этим методам относятся вероятностные модели, статистические методы и машинное обучение для оценки вероятности и последствий различных типов атак. Ведутся активные исследования по разработке моделей и методов количественной оценки риска реализации угроз информационной безопасности. Среди наиболее значимых работ следует выделить работы следующих ученых: Аникин А.В., Павленко А.В., Ковалева Е.Г., Радоуцкий В.Ю., Легчекова Е.В., Титов О.В., Прищеп С.В., Ерохин С.С., Je Y.M., You Y.Y., Na K.S., Rueda S., Avila O., Patel S.C., Graham J.H., Ralston P.A.S., Kure H.I., Islam S., Razzaque M.A., de Gusmão A.P.H., Pawar S., Palivela H.

Среди предложенных аналитических моделей и методов риск-ориентированного управления доступом, есть узкоспециализированные, сложные для применения в конкретных видах задач обеспечения безопасности распределенных вычислительных систем. Это не дает возможности для создания комплексного научно обоснованного решения для риск-ориентированного управления доступом с учетом вариативности предоставляемых услуг и гетерогенности защищаемых ресурсов.

Объект исследования. Процессы управления доступом, обеспечения защищенности и оценки риска реализации угроз информационной безопасности в распределенных информационных системах. диссертация

Предмет исследования. Методы, модели и алгоритмы анализа риска и управления доступом в распределенных информационных системах.

Границы исследования. Охватывают область практической реализации разработанных в ходе выполнения исследования моделей и методов риск-ориентированного управления доступом в образовательных вычислительных сервисах.

Научная проблема диссертационного исследования заключается в необходимости создания научно-методического аппарата адаптивного риск-ориентированного управления доступом в распределенных информационных системах, включающего в себя методы, модели, алгоритмы, программное обеспечение. Решение этой проблемы, имеющей важное значение для технической отрасли знаний (информационной безопасности), определяется активным внедрением распределенных информационных систем в различные сферы человеческой деятельности,

классические методы и модели управления доступом не обладают возможностью адаптации к изменяющимся условиям среды, при этом важно не только обеспечить защищенность ресурсов, но и сохранить их доступность для пользователей, повысить удобство использования сервисов без внесения избыточных мер защиты. Механизмы адаптации на базе риск-ориентированных подходов позволят решить данную проблему. Важным аспектом при этом остается доказательство выполнения требований к защищенности.

Целью диссертационной работы является разработка научно-методического аппарата адаптивного риск-ориентированного управления доступом в распределенных информационных системах, включающего в себя методы, модели, алгоритмы, программное обеспечение, позволяющие учитывать динамически изменяющиеся атрибуты доступа и среды в распределенных информационных системах.

Для достижения поставленной цели необходимо было решить следующие **частные научные задачи исследования**:

1. Систематизация и анализ современного состояния теории и практики, технологий, методов и средств управления доступом и анализа рисков в системах информационной безопасности.
2. Разработка риск-ориентированной атрибутивной модели управления доступом, основанной на анализе состояния динамически изменяющихся условий среды и учете получаемых оценок значений риска.
3. Разработка комплексного метода количественной оценки рисков реализации угроз информационной безопасности на основе анализа событий, создаваемых агентами распределенной информационной системы.
4. Разработка метода непрерывной аутентификации пользователей распределенных информационных систем на основе их психологических реакций.
5. Разработка метода оценки эффективности реализации защитных мер на основе анализа затрат ресурсов.
6. Оценка эффективности применения разработанного научно-методического аппарата адаптивного риск-ориентированного управления доступом, основанного на количественном анализе рисков, в распределенных информационных системах.

Научная новизна заключается в следующем:

1. Разработана модель управления доступом, интегрирующая оценку риска при принятии решений о предоставлении доступа, что обеспечивает повышение доступности услуг и выполнение требований к защищенности на основе анализа динамически изменяющихся условий среды. Эта модель позволяет адаптивно реагировать на

изменения условий доступа, учитывая риски и обеспечивая гибкость в управлении правами пользователей, что особенно важно для распределенных информационных систем с высоким уровнем динамичности.

2. Предложен метод количественной оценки рисков, основанный на анализе событий, поступающих от агентов, который предоставляет оперативную информацию о текущем состоянии распределенных информационных систем и учитывает отдельные факторы их функционирования. Метод позволяет не только своевременно выявлять потенциальные угрозы, но и проводить детализированный анализ факторов, влияющих на уровень риска, что способствует более точному и эффективному управлению информационной безопасностью.
3. Разработан метод непрерывной аутентификации, использующий психологические реакции пользователей для обеспечения дополнительного фактора защиты в условиях высокого риска реализации угроз информационной безопасности. Метод включает в себя анализ физиологических и поведенческих характеристик пользователей, что позволяет значительно повысить уровень безопасности за счет учета уникальных психофизиологических параметров каждого пользователя и уменьшить вероятность несанкционированного доступа.
4. Предложен метод оценки эффективности реализованных защитных мер путем анализа затрат ресурсов, позволяющий выявлять факты избыточного потребления ресурсов отдельными механизмами защиты информации в распределенных информационных системах. Этот метод предоставляет возможность оптимизировать использование ресурсов, направленных на защиту информации, и повысить общую эффективность защитных мер, что является ключевым фактором для поддержания высокой производительности и безопасности информационных систем.
5. Разработан научно-методический аппарат риск-ориентированного атрибутивного управления доступом, основанный на количественном анализе рисков в условиях динамически изменяющихся атрибутов доступа и среды в распределенных информационных системах. Этот аппарат обеспечивает адаптивное и гибкое управление доступом, позволяя учитывать как текущее состояние атрибутов доступа, так и внешние условия, что значительно повышает уровень защищенности и устойчивости информационных систем к различным угрозам.

Теоретическая значимость работы. Создан новый научно-методический аппарат, имеющий существенное значение для развития методов, моделей, алгоритмов и программных средств управления доступом и

обеспечения информационной безопасности в распределенных информационных системах. Разработанный научно-методический аппарат впервые представлен в виде совокупности модели и методов риск-ориентированного атрибутивного управления доступом, включающей риск-ориентированную атрибутивную модель управления доступом, отличающуюся учетом значения риска при принятии решения о предоставлении доступа, метод количественной оценки рисков реализации угроз информационной безопасности на основе анализа событий, поступающих от агентов, метод непрерывной аутентификации на основе оценок индивидуальных психомоторных реакций пользователей в результате взаимодействия с элементами интерфейса, метод оценки эффективности реализации защитных мер на основе анализа затрат ресурсов, научно-методический аппарат управления доступом на основе анализа рисков и динамически изменяющихся атрибутов доступа.

Разработанные модели и методы вносят значительный вклад в теорию информационной безопасности, предлагая новые подходы к управлению доступом и оценке рисков. В частности, риск-ориентированная атрибутивная модель управления доступом интегрирует оценку риска при принятии решений о предоставлении доступа, что расширяет существующие теоретические основы адаптивного управления доступом в условиях динамически изменяющейся среды. Метод количественной оценки рисков на основе анализа событий от агентов обогащает теорию новыми инструментами для своевременной и точной оценки состояния распределенных информационных систем.

Метод непрерывной аутентификации на основе психологических реакций пользователей добавляет новый уровень защиты, учитывающий поведенческие и физиологические аспекты, что существенно расширяет теоретические модели аутентификации. Метод оценки эффективности реализации защитных мер посредством анализа затрат ресурсов вносит важный теоретический вклад в понимание баланса между затратами и эффективностью механизмов защиты. Научно-методический аппарат риск-ориентированного атрибутивного управления доступом, основанный на количественном анализе рисков, развивает теоретические подходы к управлению доступом, делая их более гибкими и адаптивными к изменяющимся условиям, что критически важно для повышения устойчивости информационных систем к угрозам. Эти результаты углубляют и расширяют существующие теоретические основы, предлагая новые перспективы для дальнейших исследований и разработки моделей и методов в области информационной безопасности.

Практическая значимость заключается в том, что новый научно-методический аппарат риск-ориентированного атрибутивного управления доступом позволяет совершенствовать механизмы управления доступом,

осуществлять оперативный мониторинг состояния распределенных информационных систем на основе анализа рисков с учетом вариативности внешней среды и комплексности атакующего воздействия, а также обеспечивать адаптацию политик безопасности управления доступом под изменяющиеся условия среды, что вносит значительный вклад в повышение защищенности распределенных информационных систем при обеспечении их высокой доступности для пользователей.

Методология и методы исследования. В работе использованы методы теории вероятностей, математической статистики, управления доступом, анализа рисков, методы планирования экспериментов и статистической обработки экспериментальных данных, методы искусственного интеллекта и машинного обучения, аппарата нечеткой логики.

Положения, выносимые на защиту:

1. Риск-ориентированная атрибутивная модель управления доступом, основанная на анализе состояния динамически изменяющихся условий среды и учете получаемых оценок значений риска, для обеспечения повышения доступности услуг информационной системы и выполнения требований к ее защищенности.
2. Метод количественной оценки рисков реализации угроз информационной безопасности, основанный на оперативном анализе событий, создаваемых агентами распределенной информационной системы, обеспечивающий оценку текущего состояния ее информационной безопасности.
3. Метод непрерывной аутентификации пользователей на основе их психологических реакций, обеспечивающий дополнительную защиту распределенных информационных систем в условиях высокого риска реализации угроз информационной безопасности.
4. Метод оценки эффективности реализованных защитных мер, основанный на анализе затрат ресурсов, позволяющий выявлять факты избыточного потребления ресурсов отдельными механизмами защиты информации в распределенных информационных системах.
5. Научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды в распределенных информационных системах.

Достоверность полученных результатов подтверждается корректностью использованного математического аппарата и теоретических обоснований, непротиворечивостью полученных результатов известным решениям, достаточно широкой апробацией результатов диссертации, использованием методик, проверенных экспериментами и внедренных

в действующие распределенные информационные системы, реализующие сервисы высшего образования.

Апробация работы. Основные положения и результаты исследования, составляющие содержание диссертации, докладывались и обсуждались на:

- IV Всероссийской (с международным участием) научно-технической конференции "Интеллектуальные информационные системы: теория и практика". Курск, 21–23 ноября 2023 г.;
- III Всероссийской научной школе-семинаре "Современные тенденции развития методов и технологий защиты информации". Москва, 25–27 октября 2023 г.;
- Национальной научно-практической конференции "Интеллектуальное приборостроение и технические средства обеспечения безопасности". Москва, 18–20 апреля 2023 г.
- II Всероссийской научно-практической конференции с международным участием "Информационный обмен в междисциплинарных исследованиях". Рязань, 14 апреля 2023 г.;
- III Всероссийской научно-технической конференции "Интеллектуальные информационные системы: теория и практика". Курск, 22–24 ноября 2022 г.;
- Всероссийской научно-практической конференции с международным участием "Информационный обмен в междисциплинарных исследованиях". Рязань, 18–20 октября 2022 г.;
- Всероссийской школе-семинаре "Системный анализ и обработка информации в образовании и психологии". Москва, ПИ РАО, 28 февраля 2023 г.;
- XVII Международной научно-практической конференции "Современные информационные технологии и IT-образование". Москва, ВМК МГУ им. М.В. Ломоносова, 24–26 ноября 2022 г.;
- Futuristic Trends in Networks and Computing Technologies (FTNCT-2020). Таганрог, 13–15 октября 2020 г.;
- Научно-практической конференции "Цифровые аналитические инструменты и прикладные программы в образовании". Москва, РАО, 27 октября 2020 г.;
- Big Data & AI Conference 2020. Москва, 17–18 сентября 2020 г.;
- II Всероссийской научно-технической конференции "Состояние и перспективы развития современной науки по направлению "Информационная безопасность". Анапа, 19–20 марта 2020 г.;
- V Региональной научной конференции "Прикладные исследования и технологии" ART2018. Москва, 15–16 августа 2018 г.;
- XXVII Научно-технической конференции "Методы и технические средства обеспечения безопасности информации". Санкт-Петербург, 24–27 сентября 2018 г.;

– III Всероссийской научно-практической конференции "Информационные технологии в экономике и управлении". Махачкала, 29–30 ноября 2018 г.;
– Межвузовской школе-семинаре "Задачи системного анализа, управления и обработки информации". Москва, МТИ, 2017 г., 2019 г.;
– LXVI Международной научно-практической конференции "Технические науки – от теории к практике". Новосибирск, 2017 г.;
– Всероссийской научно-практической конференции "Актуальные проблемы науки и практики в предпринимательстве". 24 марта 2017 г.;
– XX Международной научно-практической конференции "Теории и практика современной науки". 22 марта 2017 г.;
– V Международной научно-практической электронной конференции "Социально-антропологические проблемы информационного общества". 10 марта 2017 г.;
– VI Междуранодной научно-практической электронной конференции "Современные научные исследования: актуальные теории и концепции". 10 апреля 2017 г.;
– XV Международной научно-практической конференции "Научный поиск в современном мире". 30 апреля 2017 г.;
– XIII Международной научно-практической конференции "Теоретические и практические проблемы развития современной науки". 31 марта 2017 г.

Внедрение результатов работы. Диссертация является обобщением результатов исследований, проводившихся автором в течение последних 10 лет в процессе учебно-научной деятельности по направлению "Информационная безопасность" в ФГБОУ ВО "МИРЭА – Российский технологический университет". Полученные результаты реализованы в проекте Ampire РТУ МИРЭА, а также внедрены в деятельность Института кибербезопасности и цифровых технологий для обеспечения безопасности платформы дистанционного обучения, использованы при построении систем дистанционного обучения в АО "Позитив Текнолоджиз". Разработанные методики, программное обеспечение и экспериментальные стенды использованы при проведении оценки защищенности распределенных информационных систем, применяемых в ООО "Непрерывные технологии", ООО "Лаборатория Наносемантика", ФГАНУ "Центр информационных технологий и систем органов исполнительной власти им. А.В. Старовойтова", АО "Перспективный мониторинг".

Соответствие паспорту специальности. Представленная диссертация соответствует паспорту специальности 2.3.6. Методы и системы защиты информации, информационная безопасность: п. 2. "Методы, аппаратно-программные средства и организационные меры защиты систем

(объектов) формирования и предоставления пользователям информационных ресурсов различного вида", п. 8. "Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения" и п. 12 "Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа".

Личный вклад. Все выносимые на защиту результаты получены лично автором. В работах, опубликованных в соавторстве, личный вклад состоит в разработке риск-ориентированной атрибутивной модели управления доступом, отличающейся учетом значения риска при принятии решения о предоставлении доступа, метода количественной оценки рисков реализации угроз информационной безопасности на основе анализа событий, поступающих от агентов, метода непрерывной аутентификации на основе психологических реакций пользователей, метода оценки эффективности реализации защитных мер на основе анализа затрат ресурсов, научно-методического аппарата управления доступом на основе анализа рисков и динамически изменяющихся атрибутов доступа.

Публикации. Основные научные результаты диссертации отражены в 58 работах, из них 40 статей опубликованы в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, включая 22 статьи в изданиях, входящих в международные цитатно-аналитические базы Scopus и Web of Science; 9 свидетельств о государственной регистрации программы для ЭВМ.

Структура и объем диссертационной работы. Диссертация состоит из введения, 5 глав, заключения и 2 приложений. Полный объем диссертации составляет 314 страниц, включая 82 рисунка и 19 таблиц. Список литературы содержит 299 наименований.

Содержание работы

Во **введении** обоснована актуальность, сформулированы цель и задачи, объект и предмет исследования, научная новизна, практическая ценность, приводятся сведения об апробации, основных публикациях, изложена структура диссертации.

Первая глава посвящена анализу методов и моделей управления доступом, моделей и алгоритмов анализа и оценки риска реализации угроз информационной безопасности в распределенных информационных системах, разработке модели угроз и модели нарушителя, формальной постановке научной проблемы проводимого исследования.

Вторая глава посвящена разработке *риск-ориентированной атрибутивной модели управления доступом, основанная на анализе состояния динамически изменяющихся условий среды и учете получаемых оценок*

значений риска. В главе описаны недостатки существующих статичных моделей управления доступом, подробно описаны существующие ограничения в их использовании и предложено решение обнаруженной проблемы за счет разработки динамической риск-ориентированной модели управления доступом.

Риск-ориентированная атрибутивная модель управления доступом представляет собой динамическую модель управления доступом к сервисам, реализуемым системами высшего образования, посредством оценки потенциально возможного риска реализации угроз информационной безопасности, с учетом оценки атрибутов объектов, субъектов и среды. Структурные компоненты риск-ориентированной модели доступа для систем высшего образования представлены на рисунке 1.

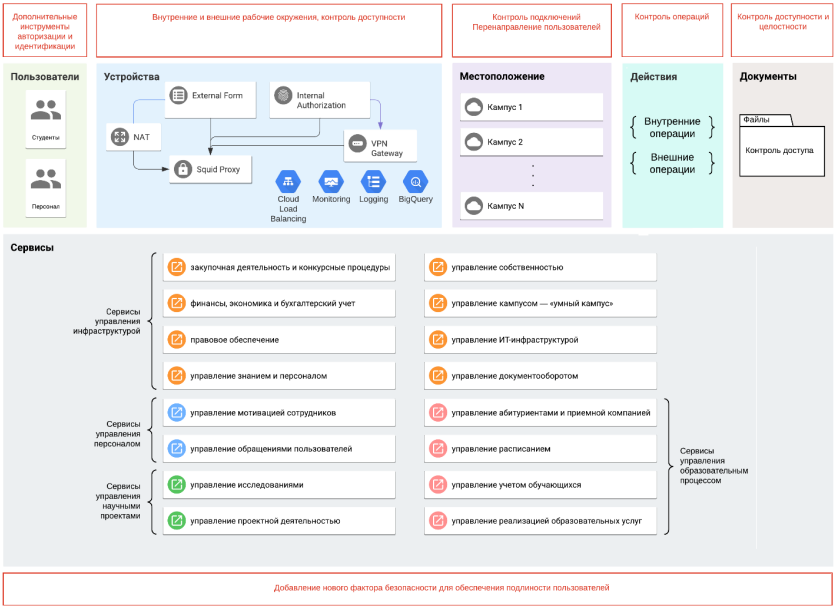

Рис. 1 — Риск-ориентированная атрибутивная модель управления доступом для ОВС системы высшего образования

К основным компонентам риск-ориентированной модели управления доступом относятся субъекты и объекты доступа, а также правила предоставления доступа, формируемые динамически в зависимости от рассчитанного риска. Объектами доступа в риск-ориентированной модели управления доступом являются сервисы, предоставляемые системой высшего образования. Предоставляемые сервисы могут быть разделены на следующие категории:

– сервисы управления образовательной деятельностью (реализация образовательного процесса, формирование расписания занятий, реализация деятельности по набору и поступлению абитуриентов и учет обучающихся);
– сервисы управления научными проектами (реализация и проведение научных исследований, конструкторская и проектная работа);
– сервисы управления персоналом (взаимодействие с внешними организациями и пользователями, внутренняя работа с сотрудниками);
– сервисы управления инфраструктурой (финансовая деятельность, управленческая деятельность, правовое обеспечение, документооборот, кадровая работа, архивное дело).

В качестве атрибутов доступа в разработанной модели управления доступом выступают следующие сущности (рис. 2):

– роль: студент, преподаватель, административный персонал, внешние субъекты, руководители подразделений;
– тип устройства доступа: рабочий персональный компьютер, ноутбук, мобильное устройство;
– тип подключения устройства: локальная вычислительная сеть организации, VPN-подключение, подключение из глобальной сети Интернет;
– тип сервиса: сервисы управления образовательным процессом, сервисы управления научными проектами, сервисы управления персоналом, сервисы управления доступом, сервисы бухгалтерского учета, сервисы управления инфраструктурой;
– местоположение: кампус 1, кампус 2, ..., кампус N, филиал, удаленное рабочее место;
– тип подключения: VPN (Virtual Private Network), внутренняя сеть, сеть Интернет;
– действие: запись, чтение, создание, удаление, модификация.

Атрибуты безопасности доступа позволяют описать возможные действия сотрудников организации системы высшего образования (сценарий), осуществляющих доступ к требуемому сервису или запрашиваемому ресурсу (объекту доступа).

Для учета изменяющихся условий доступа в модели был введен дополнительный атрибут – значение риска реализации угроз информационной безопасности.

Верификация разработанной модели управления доступом производилась по методу проверки моделей на основе перебора различных комбинаций атрибутов доступа.

В третьей главе представлен разработанный *комплексный метод количественной оценки рисков реализации угроз информационной безопасности основанный на оперативном анализе событий, создаваемых агентами распределенной информационной системы.*

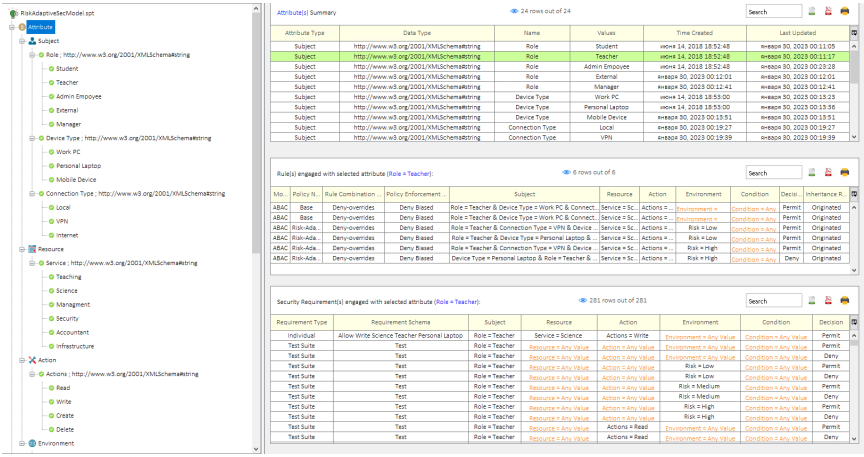

Рис. 2 — Атрибуты объектов и субъектов в модели управления доступом

Метод количественной оценки рисков основан на работе интеллектуальных агентов, осуществляющих мониторинг функционирования объектов распределенных информационных систем (сервисов системы высшего образования). Он включает в себя следующие этапы:

1. Сбор информации о событиях безопасности, относящихся к субъектам (пользователям) и объектам доступа (ресурсам образовательной организации системы высшего образования).
2. Количественная оценка риска на основе правил нечеткой логики на основе информации, полученной от агентов четырех типов (субъектов, ресурсов, действия, среды). Риск рассчитывается на основе обученных алгоритмов машинного обучения (kNN, ядро k=4).

Интеллектуальные агенты создаются с применением методов машинного обучения на основе имеющихся данных и зависят от этих данных. Интеллектуальные агенты не обладают 100%-ным доверием, необходимо учитывать степень доверия при использовании показаний интеллектуальных агентов при расчете значений риска. Доверие определяется на основе рассчитанного значения риска для ресурса в данный момент времени, с учетом факторов надежности используемой интеллектуальной технологии и др.

Для учета степени доверия к агенту предлагается использовать агрегирующую систему мониторинга этих агентов, которая будет принимать решения в зависимости от текущей степени доверия агентам и уровня их критичности. Схема работы агрегирующей системы мониторинга для количественной оценки риска реализации угроз информационной безопасности для распределенных информационных систем представлена на рисунке 3.

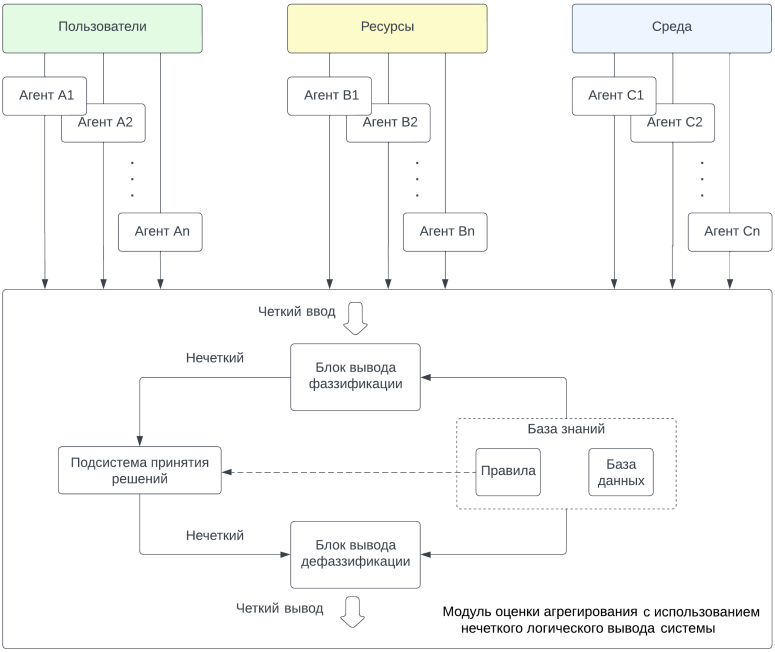

Рис. 3 — Схема работы агрегирующей системы мониторинга

На первом этапе агентами осуществляется сбор информации о событиях безопасности, содержащихся в журналах аудита. Агенты представляют собой компонент системы мониторинга событий безопасности, устанавливаемый на локальные компьютеры и сетевые ресурсы. В зависимости от типа получаемой информации были выделены четыре типа агентов:

Агент 1: агенты наблюдения за субъектами (активными пользователями).
Агент 2: агенты наблюдения за объектом (ресурсом).
Агент 3: агенты наблюдения за инфраструктурой (средой).
Агент 4: агенты наблюдения за субъектами (неудачные попытки аутентификации).

На основании анализа представленных данных выделено четыре типа агентов:

1. Агент наблюдения за объектами – следит за количеством событий удаления пользователей и объектов.
2. Агент наблюдения за пользователями – следит за количеством неудачных попыток входа, выдает уровень риска (от 0 до 10), если таких попыток много за период времени.

3. Агент наблюдения за взаимодействием пользователей и ресурсов – следит за количеством пользователей одновременно (в пределах заданного интервала времени), обращающихся к ресурсу, возвращает повышенный риск при превышении частоты обращения заданного порога. В агенте задан словарь, в котором хранятся ключ - имя сервиса, значение - среднее количество обращений и максимальное количество обращений за 10 минут. Уровень риска формируется по принципу близости к порогу. Нижний порог – это среднее количество обращений, верхний порог - максимально зафиксированный за 10 минут. Если у одного из сервисов количество обращений равно или больше максимального, то риск равен 10. Иначе риск считается как процент от максимума для самого загруженного сервиса.
4. Агент наблюдения за пользователями – следит за количеством активных пользователей. В зависимости от количества пользователей высчитывается риск от 0 до 10. Нижняя и верхняя граница определяются задаваемой конфигурацией. Учитываются только изменения под конец 10-минутного периода. Время сессии одного пользователя – 30 минут.

На втором этапе реализуются анализ и количественная оценка рисков реализации угроз информационной безопасности к ресурсам распределенных информационных систем посредством агрегирования поступающей информации и ранжирования всех событий по шкале от 1 до 10 согласно следующим правилам:

- Правило "Агента 1": если текущее количество операций по удалению объектов или пользователей превышает среднее значение, то уровню риска присваивается значение от 1 до 10 (10 – верхняя граница), иначе уровень риска равен 0.
- Правило "Агента 2": на основе экспериментальных оценок определяется среднее значение количества неудачных попыток авторизации за 10 минут и сравнивается с текущими значением аналогично правилу "Агента 1".
- Правило "Агента 3": если количество обращений к одному сервису равно или больше максимального, то уровень риска соответствует значению 10, в противном случае риск считается как процент от максимума для самого загруженного сервиса (пороговые значения нижняя граница – среднее количество обращений, верхняя – максимально зафиксированное за промежуток времени в 10 минут количество обращений).
- Правило "Агента 4": в зависимости от количества пользователей формируется значение уровня риска для каждого 10-минутного отрезка сеанса пользователя (нижняя и верхняя границы задаются администратором).

Каждый агент возвращает число, описывающее его состояние. Такое число задается либо в некоторой заранее известной шкале (например, от 0 до 10), либо приводится к диапазону $0 \dots 1$ и может быть интерпретировано как уверенность агента в появлении угрозы (в рамках его компетенции). Показания однотипных (например, два агента FaceID с разной версией установленного ПО распознавания лиц) агентов агрегируются путем усреднения, взвешенного усреднения или голосования (для категориальных). Показания разнотипных агентов агрегируются с помощью системы нечеткого логического вывода (FIS, Fuzzy Inference System). Использование нечетких логических правил вместо четких позволяет учитывать недостаточное доверие к показаниям агентов, что регулируется функциями принадлежности их результатов.

Затем осуществляется количественная оценка полученных ранжированных значений уровня риска поступающих от агентов на основе применения системы нечетких логических правил, состоящая из следующих шагов:

- составление базы данных правил и функций принадлежности;
- фаззификация (перевод числовых показаний агентов в нечеткий вид согласно назначенным функциям принадлежности);
- вывод результатов фаззификации (выполнение нечетких правил, определение степени выполнения правила);
- агрегирование результатов фаззификации (возврат нечеткой переменной с рассчитанной функцией принадлежности);
- дефаззификация (перевод нечеткого результата в четкое число, интерпретируемое в дальнейшем как установленный уровень риска).

Для аналитического описания разработанного метода количественной оценки рисков реализации угроз информационной безопасности на основе анализа поступающих от агентов событий, основанного на аппарате нечеткой логики введем следующие обозначения: i – номер агента $(1 \dots 4)$; I – число агентов, передающих показания; R – оценка риска i-м агентом по шкале $0 \dots 10$; D^i – максимальный уровень доверия агенту в диапазоне $0 \dots 10$; b_i^H – степень неоднозначности в оценке агентом риска "низкий"; b_i^C – степень неоднозначности в оценке агентом риска "средний"; b_i^B – степень неоднозначности в оценке агентом риска "высокий"; a_i^H – полуширина неоднозначности в оценке агентом риска "низкий"; a_i^C – полуширина неоднозначности в оценке агентом риска "средний"; a_i^B – полуширина неоднозначности в оценке агентом риска "высокий"; c_i^H – центральное значение i-го агента в оценке риска "низкий"; c_i^C – центральное значение i-го агента в оценке риска "средний"; c_i^B – центральное значение i-го агента в оценке риска "высокий". Для всех агентов установим три градации нечетких значений риска: "низкий", "средний", "высокий".

Тогда функции принадлежности для i-го агента:

– для риска "низкий" $S_i^H = \dfrac{D_i}{1 + [R_i - \frac{c_i^H}{a_i^H}]}$;

– для риска "средний" $S_i^C = \dfrac{D_i}{1 + [R_i - \frac{c_i^C}{a_i^C}]}$;

– для риска "высокий" $S_i^B = \dfrac{D_i}{1 + [R_i - \frac{c_i^B}{a_i^B}]}$.

Для общего (агрегированного) риска используется функция принадлежности того же вида (обозначенная для общего риска как $i = 0$).

Пусть F_i^j – нечеткий логический оператор в j-м правиле для i-го агента. Тогда степень выполнения j-го правила:

$$W_j = F_I^j \circ S_I^{g_{jI}}(R_I) \circ \ \ldots \ \circ F_i^j \circ S_i^{g_{ji}}(R_i) \circ \ \ldots \ \circ F_1^j \circ S_1^{g_{j1}}(R_1). \qquad (1)$$

Здесь $F_I^j = 1$ – тождественный оператор, g_{ij} – конкретное нечеткое значение риска в j-м правиле для i-го агента, $g_{ij} = \{$"н", "с", "в"$\}$.

Введем правила с операторами вида нечеткого "И" (обозначим $\wedge$):

$$W_j = S_I^{g_{jI}}(R_I) \wedge \ldots \wedge S_i^{g_{ji}}(R_i) \wedge \ldots \wedge S_1^{g_{j1}}(R_1). \qquad (2)$$

Согласно правилам вычисления нечетких логических выражений:

$$W_j = \min \left[S_I^{g_{jI}}(R_I), \ \ldots, S_i^{g_{ji}}(R_i), \ \ldots, S_1^{g_{j1}}(R_1) \right]. \qquad (3)$$

Обозначим $A(\cdot)$ как площадь под кривой функции принадлежности. Тогда определим, что для правила j задан результат для общего риска в виде функции $S_j^0(R)$ заданной на той же шкале R от 0 до 10. При заданных ограничениях, агрегированная функция принадлежности будет иметь вид:

$$S^0(R) = \max_{j=1\ldots J} \left[\min(S_j^0(R), W_j) \right]. \qquad (4)$$

Решением уравнения (4), представляющим собой значение общего риска, является число, определяющее центр площадей. Общий риск R^* измеряется в тех же градациях "низкий", "средний", "высокий":

$$A_{R<R^*}(S^0(R)) = A_{R>R^*}(S^0(R)), \qquad (5)$$

с колоколообразными функциями принадлежности по типу 2: S_H, S_C, S_B соответственно.

Экспериментальная оценка разработанного метода количественной оценки риска производилась на данных, полученных из используемой системы сбора и анализа событий безопасности, функционирующей на базе центра дистанционного обучения РТУ МИРЭА. Для каждого агента сформированы пороговые и средние значения на основе собранной статистики в

СДО РТУ МИРЭА за 2023 год. Результаты оценки риска для промежутков времени функционирования агентов представлены на рисунке 4.

Анализ полученных результатов и соответствующие им экспертные оценки показали соответствие рассчитанных значений посредством разработанного метода количественной оценки ожидаемым значениям риска для сервисов системы высшего образования, функционирующих на базе РТУ МИРЭА. Согласованность экспериментальных исследований с реальными данными демонстрирует эффективность и состоятельность разработанного метода, позволяющего осуществлять количественную оценку риска для принятия решений в риск-ориентированной атрибутивной модели управления доступом.

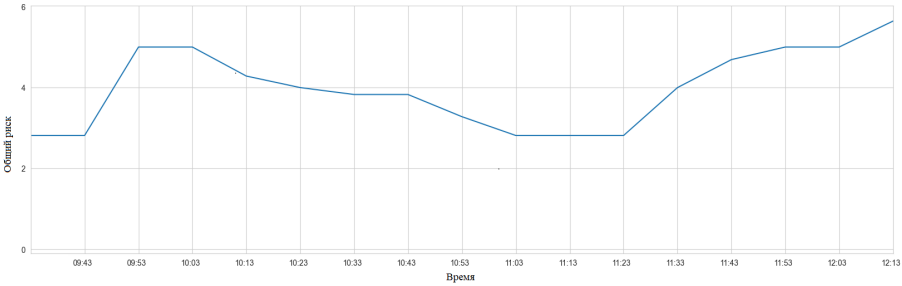

Рис. 4 — Общий уровень риска согласно показаниям Агентов 1–4, с заданным интервалом 10 минут

Разработанный метод количественной оценки значения риска информационной безопасности основан на анализе событий безопасности, поступающих от разработанной системы агентов, посредством математического аппарата нечеткой логики. Разработанная система агентов сбора информации отличается учетом возможных действий и событий как пользователя, так и объектов образовательных вычислительных сервисов организаций высшего образования, а также распределенной информационной системы, на которой строятся образовательные вычислительные сервисы. Применение аппарата нечеткой логики позволило перейти от качественных оценок состояния безопасности к количественным значениям риска реализации угроз.

Результаты экспериментальных исследований с реальными данными демонстрируют эффективность и состоятельность разработанного метода, позволяющего оперативно обрабатывать события полученные от агентов и формировать базы инцидентов безопасности, что в свою очередь, позволяет использовать разработанный метод количественной оценки рисков в разработанной риск-ориентированной атрибутивной модели управления доступом, в которой полученное значение риска может выступать в качестве дополнительного атрибута доступа в процессе предоставления доступа

пользователя к ресурсам на основе разработанной риск-ориентированной модели.

Четвертая глава посвящена разработке *метода непрерывной аутентификации пользователей в распределенных информационных системах на основе их психологических реакций*. Разработанный метод непрерывной аутентификации основан на методе поведенческой биометрии пользователей, использующей в качестве аутентификационного признака время реакции пользователей при осуществлении взаимодействия с объектами доступа.

Методы непрерывной аутентификации относятся к механизму обеспечения информационной безопасности, позволяющему в режиме реального времени осуществлять мониторинг действий пользователя в течение сеанса работы, а также с заданной частотой обновления проверять легитимность предоставления доступа пользователю к системе. Для достижения этой цели поведенческая биометрия непрерывно создает профиль поведения пользователя на основе естественных взаимодействий без необходимости постоянного прерывания действий пользователей для прохождения процедуры аутентификации.

Под временем реакции пользователя в рамках исследования понимается период времени между приложением внешнего стимула и соответствующей двигательной реакцией. Применение указанного аутентификационного признака позволяет незаметно для пользователя в интерактивном режиме отслеживать психофизические характеристики. Время реакции пользователя для конкретного действия можно разделить на:

– минимальное ВР (минимальная латентность ответа);
– максимальное ВР (максимальная латентность ответа);
– усредненное ВР (усредненная латентность ответа).

Метод непрерывной аутентификации на основе психологических реакций пользователя состоит из следующих этапов:

1. Обучение алгоритма анализа поведения пользователя.
2. Анализ поведенческой активности.
3. Обнаружение аномального поведения пользователя.
4. Верификация пользовательских данных.

На первом этапе осуществляется формирование данных для обучения алгоритма машинного обучения. В качестве обучающей выборки выступает информация первичного опроса пользователей, а также информация, получаемая посредством взаимодействия с анкетными вопросами или заданными вопросами. На основе хранящихся данных о скорости реакции этого пользователя при работе с элементами интерфейса строится прогнозная модель о реакции.

В процессе анализа поведенческой активности осуществляется мониторинг текущей активности, получение текущих оценок времени реакции.

Полученные значения передаются для обнаружения аномального поведения пользователя. Если полученный экспериментальный результат входит в состав другого квартиля от ожидаемого значения, то запускаются механизмы идентификации и аутентификации пользователя, требующие персонального подтверждения. В противном случае пользователь считается аутентифицированным.

На этапе верификации пользователь повторно проходит все этапы многомерной аутентификации, в том числе первичный этап опроса пользователей разработанного метода непрерывной аутентификации. Разработанный метод непрерывной аутентификации функционально реализован в виде вычислительного комплекса, основанного на клиент-серверном взаимодействии. Вычислительный комплекс реализует следующие возможности:

- предоставляет клиенту одну или несколько услуг;
- включает в состав компьютерные сети и системы управления передачей данных;
- позволяет отправлять инциденты безопасности на облачную платформу для дальнейшего анализа алгоритмами машинного обучения информацию об инцидентах безопасности, обнаруженных во время локального анализа;
- создание постоянного хранилища информации о безопасности и менеджера событий, осуществляющего выбор заранее определенных инцидентов безопасности для локального и удаленного анализа;
- задание заранее определенного интервала времени, на основе которого формируются инциденты безопасности.

Экспериментальная оценка адекватности разработанного метода непрерывной аутентификации проводились с помощью цифровой платформы DigitalPsyTools. Для получения количественных результатов использованы реакции 23102 студентов при ответе на четыре вопроса:

- основа обучения (выбор из трех вариантов: бюджетная, контрактная, целевая);
- Вы поступили на ту специальность, которую хотели? (да, нет);
- укажите профиль Вашего образования (выбор из четырех вариантов: технический, гуманитарный, естественнонаучный, нет профиля);
- программа обучения (выбор из четырех вариантов: бакалавриат, магистратура, специалитет, аспирантура).

Анкета организована в виде веб-интерфейса. В каждом элементе опроса фиксируется ответ и время реакции в миллисекундах (с момента загрузки до выбора ответа и нажатии кнопки "далее"), т.е. время, за которое пользователь прочитал вопрос, выбрал нужный вариант и нажал кнопку "далее".

Проведен эксперимент, в котором участвовали студенты 20 различных вузов, в ходе которого в рамках когнитивных исследований, среди прочего, были заданы следующие три вопроса:

1. Учебная программа (на выбор четыре варианта: бакалавриат, магистратура, специалитет, аспирантура).
2. Основа обучения (выбор из трех вариантов: бюджет, контракт, целевое обучение).
3. Укажите профиль вашего образования (на выбор четыре варианта: техническое, гуманитарное, естественнонаучное, без профиля).

Вопросы 1 и 2 задавались в начале взаимодействия с платформой, вопрос 3 – через час после проведения дополнительных когнитивных тестов. Тесты, содержащие пустые ответы или время реакции на которые составляло менее 2 секунд, удалялись из набора данных. Оставшиеся 22357 записей нормировались, и на основе полученных данных осуществлялся расчет среднего значения для каждого вопроса.

Для качественной оценки отклонений времени реакции введена шкала, делящая отклонения на 4 квартиля в порядке возрастания. Таким образом, у каждого из 22 357 студентов была упорядоченная триада типа (1, 2, 4), представляющая их относительно отклонений времени реакции на вопросы 1–3.

Помимо обобщенных значений, осуществлен анализ индивидуальных реакций трех произвольно выбранных пользователей при ответе на каждый из вопросов. Полученные значения позволяют сделать вывод о том, что замедленная реакция характерна для ответа на все вопросы, средние и быстрые реакции сохраняются при изменении вопроса и количества вариантов ответов, то есть подход позволяет выявить, был ли в процессе ответа на анкетные вопросы заменен пользователь и данные реакции могут быть использованы в предложенном методе аутентификации.

Для качественной оценки отклонений времени реакции была введена шкала, делящая отклонения на 4 квартиля в порядке возрастания. Таким образом, у каждого из 22357 студентов была упорядоченная триада типа (1, 2, 4), представляющая их относительно отклонений времени реакции на вопросы 1–3. Разбиение на квартили пронормированных данных приведено в таблице 1.

Количественный анализ данных отклонений времени реакции показал достоверную корреляцию между отклонениями при ответах на вопросы 1–3. При изучении взаимосвязи отклонений времени реакции для трех вопросов был проведен тест Вальда, демонстрирующий значительную линейную взаимосвязь между отклонениями.

В ходе анализа было обнаружено, что 17002 студентов (76%) принадлежали к одному квартилю по всем трем вопросам или не более чем один квартиль находился рядом с двумя другими, то есть если ответ на первый вопрос попал в определенный квартиль, то он попадет в такой же квартиль

и в следующий ответах. Из полученных гистограмм (рис. 5) и приведенных результатов видно, что, несмотря на изменение времени реакций по всем данным, реакции у большинства пользователей остались неизменными.

Таблица 1 — Границы квартилей отклонений времени реакции

	Квартиль 1	Квартиль 2	Квартиль 3	Квартиль 4
Вопрос 1				
Нижняя граница	0	0,0056	0,0063	0,0068
Верхняя граница	0,0055	0,0062	0,0067	1
Вопрос 2				
Нижняя граница	0	0,0053	0,0071	0,0082
Верхняя граница	0,0052	0,007	0,0071	1
Вопрос 3				
Нижняя граница	0	0,0075	0,011	0,01
Верхняя граница	0,0074	0,0109	0,013	1

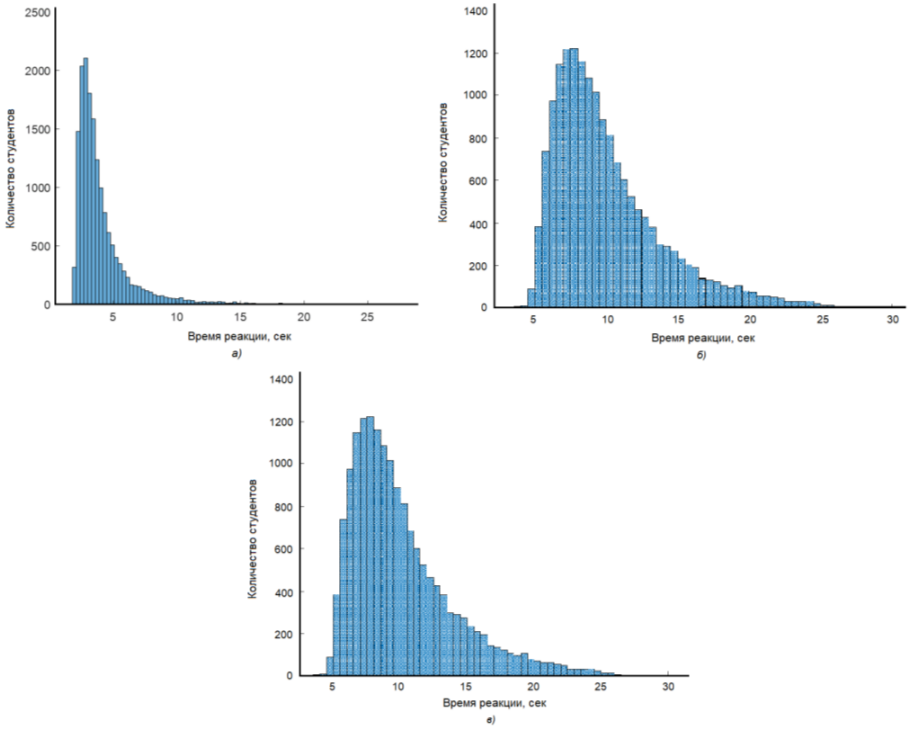

Рис. 5 — Гистограммы экспериментальных данных

Для прогнозирования реакций были проверены возможности построения регрессионных зависимостей, проведен тест Вальда. Тест Вальда

показал, что значимыми могут быть простые модели, то есть проверка и расчет прогноза не потребуют значительного количества вычислительных ресурсов для сбора и передачи данных. Полученные зависимости демонстрируют допустимость построения достоверных прогнозных значений реакций пользователей, что, в свою очередь, позволяет сделать вывод о валидности разработанного метода непрерывной аутентификации и возможности использования данного метода в качестве фактора для осуществления непрерывной аутентификации пользователей в распределенных информационных системах.

На основе подтвержденных гипотез и экспериментальных данных был разработан метод непрерывной аутентификации, использующий психофизические реакции пользователей. Метод состоит из следующих этапов:

1. В интерфейс вычислительной системы встраивается или периодически подключается специализированный интерфейс с заданными анкетными вопросами или иными простыми вопросами.
2. На основе хранящихся данных о скорости реакции этого пользователя при работе с элементами интерфейса строится прогнозная модель о реакции.
3. Прогнозные значения сравниваются с полученными.
4. Если полученный экспериментальный результат входит в состав другого квантиля от ожидаемого значения, то запускаются механизмы идентификации пользователя, требующие персонального подтверждения.
5. Если результаты совпадают (попадают в один квартиль), то пользователь считается верифицированным.

Функциональная схема метода непрерывной аутентификации представлена на рисунке 6.

На основе полученных экспериментальных значений и проведенных исследований в области непрерывной аутентификации разработан метод непрерывной аутентификации на основе психофизических реакций пользователей, позволяющий обеспечить конфиденциальность защищаемых ресурсов и информации посредством учета дополнительных параметров (поведения) пользователей при предоставлении доступа к образовательных вычислительных сервисам организаций высшего образования. Проведенные экспериментальные исследования разработанного метода непрерывной аутентификации позволяют сделать вывод о возможности использования разработанного метода в системах управления доступом в качестве дополнительного фактора аутентификации.

В **пятой главе** представлены *метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов* и *научно-методический аппарат адаптивного риск-ориентированного управления доступом в распределенных информационных системах.*

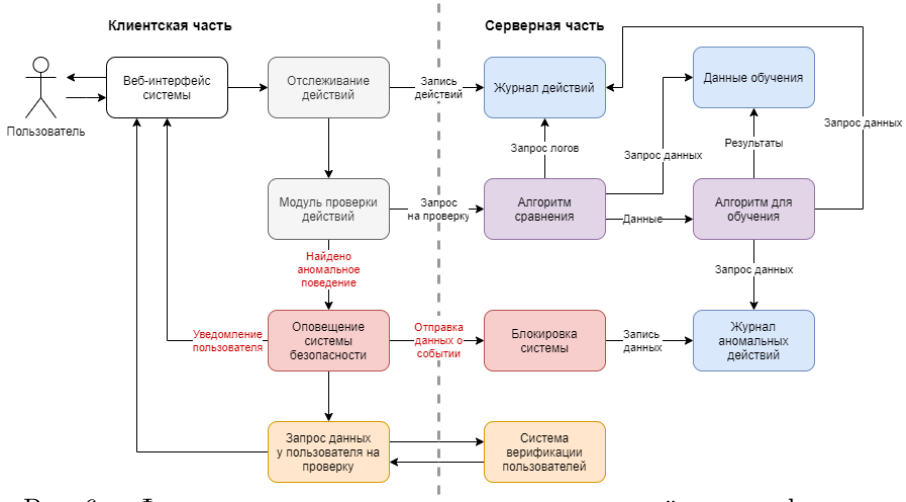

Рис. 6 — Функциональная схема метода непрерывной аутентификации

Разработанный метод оценки эффективности реализованных защитных мер на основе анализа затрат ресурсов позволяет обнаруживать факты избыточного использования ресурсов существующими средствами защиты информации в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах. Кроме того, описан научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды, базирующийся на разработанной риск-ориентированной атрибутивной модели управления доступам и методах количественной оценки рисков, непрерывной аутентификации и оценки эффективности.

Для разработки метода оценки эффективности реализации защитных мер была создана модель и разработана методика, основанная на использовании экспериментальных оценок в среде, имитирующей функционирование системы управления доступом в заданных условиях и ограничениях. В качестве исходных данных для моделирования выступают технико-экономические характеристики функционирования системы управления доступом, представляющие собой набор заданных желаемых диапазонов значений при заданном уровне доступности услуг, планируемую форму и интенсивность запросов к системе.

Пользовательские запросы $x \in X_K$ к системе управления доступом с архитектурой V, для компонента Z_k с допустимыми технико-экономическими характеристиками можно описать следующим выражением:

$$Z_k \subset V : x \xrightarrow{\Phi} R_k \in \mathbf{R}^n, k = \overline{1,q}, \tag{6}$$

где R_k – n-мерный вектор измеряемых вычислительных ресурсов. Отображение Ф является таким, что по наблюдаемому процессу X параметры R_i измеримы.

Отображение Ф в условиях виртуальности ресурсов получено путем построения экспериментального стенда по технологии "инфраструктура как код", представляющего собой программно-конфигурационный код, содержащий виртуальную инфраструктуру, с входным сигналом в форме потока X и измеряемым скалярным выходом вектора измеряемых значений характеристик.

Для эффективности реализации защитных мер разработан метод анализа затрат вычислительных ресурсов для реализации систем управления доступом на основе подхода, использующего виртуальные стенды, обеспечивающие имитационную среду использования вычислительного комплекса на каждом уровне управления доступом. Разработанный метод состоит из 7 шагов:

1. Построение типового запроса пользователя.
2. Создание виртуального экспериментального стенда, имитирующего среду использования компонентов архитектуры.
3. Программная реализация виртуальной инфраструктуры исследуемого компонента архитектуры в форме кода.
4. Формирование случайного сигнала с заданным законом распределения на основе типовых запросов пользователей.
5. Получение оценок значений ресурсов, требуемых для использования системы управления доступом.
6. В случае решения задачи выбора вариантов реализации механизмов защиты – осуществление выбора варианта, имеющего меньшие ресурсные затраты.
7. Формирование архитектуры вычислительного комплекса с учетом полученных значений затрат вычислительных ресурсов.

Предложенный метод позволяет экспериментально решить задачи построения сбалансированных решений: может быть решена задача выбора количества ресурсов, требуемых для полного внедрения управления доступом, либо задача сокращения количества используемых модулей в условиях ограниченности ресурсов, заданных технико-экономическими требованиями к вычислительному комплексу, другие задачи, связанные с ограничением ресурсов, количества пользователей или допустимых внедрений элементов управления доступом без затрат на дополнительные средства управления доступом.

Для проведения экспериментальных исследований были использованы следующие данные: объем исходного файла с данными составляет 450 Мб; файл содержит 12000 записей ResearchSubject и 55458 записей ResearchResult; данные представлены в слабоструктурированном формате JSON. Перед началом эксперимента создаются 3 виртуальные машины

(Client, Server, Database) с заданными характеристиками. Для повторных экспериментов, если они были созданы ранее, предварительно удаляются существующие виртуальные машины для обеспечения чистоты эксперимента между повторениями. Структура экспериментального стенда приведена на рисунке 7, а в таблице 2 приведены параметры виртуальных машин.

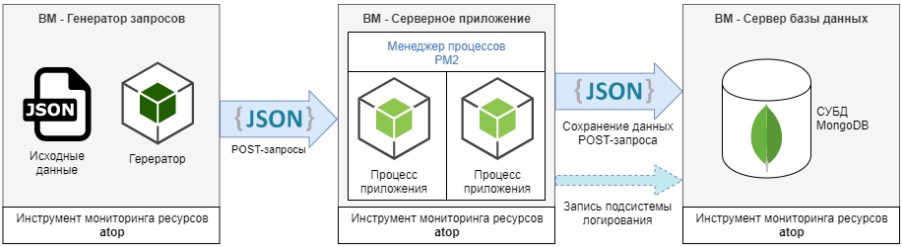

Рис. 7 — Структурная схема экспериментального стенда

Таблица 2 — Основные характеристики виртуальных машин (ВМ)

	Количество ядер ЦПУ (шт)	Объем ОЗУ (Мб)	Максимальная разрешенная загрузка ядер ЦПУ (%)	Пропускная способность подсистемы ввода-вывода (Мб)
Client	4	8192	100	–
Server	2	2048	100	–
Database (MongDB)	2	2048	50	25

На первом этапе эксперимента производилась отправка POST-запросов к серверу для получения записей ResearchSubject, представляющих собой сохраненные логи действий пользователя на основе анализа нажатий клавиш клавиатуры. На втором этапе производилась отправка POST-запросов к серверу на сохранение записей ResearchResult, представляющих собой результаты сравнения полученных на первом этапе эталонов действий пользователя с профилем текущих действий пользователя. В обоих случаях каждый POST-запрос содержит информацию только об одной записи. Таким образом, число запросов соответствует количеству исходных записей данных.

Эксперимент производится с двумя различными конфигурациями серверного программного обеспечения. В первом случае производится только сохранение данных, во втором – к конфигурации добавлялся программный код, осуществляющий логирование каждого запроса, полученного серверным программным обеспечением. Сбор данных об используемых ресурсах осуществлялся с интервалом в 1 секунду, отправка запросов осуществлялась в 4 потока, до 10 одновременных запросов, задержка между

отправками пакетов по 10 запросов составила 300 мс, а задержка между этапами эксперимента – 60 с, максимальное ожидание ответа от сервера – 10 с. Результаты проведенного эксперимента представлены в таблице 3.

Таблица 3 — Показатели ресурсных затрат на применение метода непрерывной аутентификации пользователей

Ресурсный показатель	Значение без использования метода непрерывной аутентификации	Значение с использованием метода непрерывной аутентификации	Разница в %
ЦП ВМ Client	7,49	7,21	3,3
ЦП ВМ Server	19,71	22,23	12,7
ЦП ВМ MongoDB	2,85	3,37	52,9
Память ВМ Client	1296827,18	1295665,4	0,08
Память ВМ Server	41344,79	39146,05	5,32
Память ВМ MongoDB	340911,11	341359,78	0,13

Полученные результаты экспериментальных оценок позволяют сделать вывод о том, что использование разработанного метода непрерывной аутентификации пользователей существенно влияет только на загрузку процессора серверной компоненты и развернутой на базе серверной компоненты базы данных MongoDB, при этом незначительно увеличивая общую загрузку памяти серверной компоненты. Указанная особенность позволяет осуществлять внедрение разработанного метода в системы управления доступом при условии выделения дополнительных вычислительных мощностей в существующих распределенных информационных системах.

Научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды реализован на базе системы дистанционного дистанционного обучения, представляет собой подсистему управления доступом для образовательных вычислительных сервисов организаций высшего образования. Обобщенная схема разработанных предложений по практической реализации научно-методического аппарата представлена на рисунке 8.

Оценка эффективности разработанных практических предложения по реализации научно-методического аппарата риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа и среды в системах управления доступом осуществлялась на базе СДО РТУ МИРЭА

(рис. 9) в "Подсети-1"и "Подсети-2"с задействованием центра безопасности операций.

На первом этапе оценки эффективности разработанного научно-методического аппарата проводилось тестирование на устойчивость разработанной системы к высоким нагрузкам с сохранением требуемого уровня доступности сервисов СДО и удобства их использования. На рисунке 10 представлены полученные результаты тестирования. Стоит отметить, что среднее время доступа к сервисам составило 90 мс при среднем значении количества запросов в секунду, равном 10000. Тестирование осуществлялось в течение 24 часов.

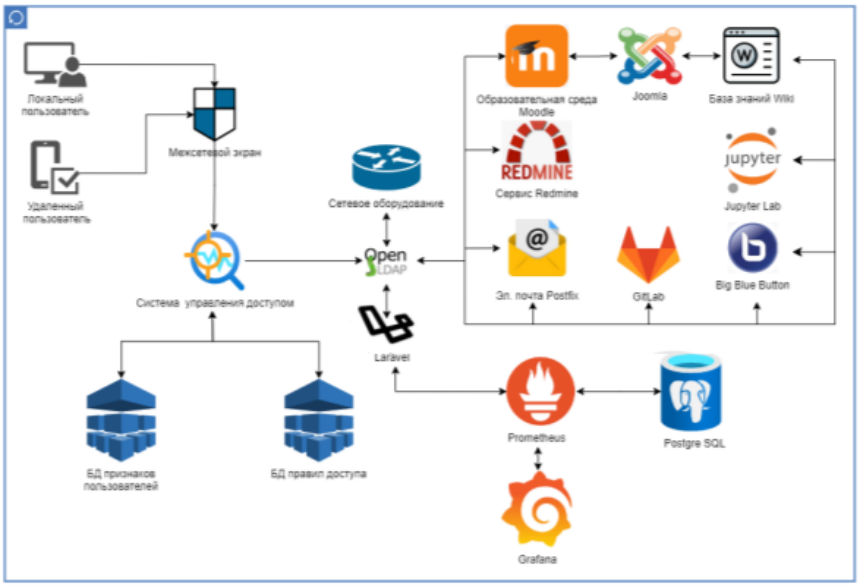

Рис. 8 — Обобщенная схема разработанных предложений по практической реализации научно-методического аппарата

Корректность применения политик безопасности в зависимости от значения риска осуществляется в автоматическом режиме на основе нечетких правил, для проверки точности и адекватности разработанного решения используется модуль сбора статистики и модуль расчета значения риска, отображаемого в платформе мониторинга и анализа данных Grafana. Результаты рассчитанного значения риска от агентов сбора данных представлены на рисунке 11.

Помимо расчета значений риска для каждого запроса доступа субъекта к объекту системы управления доступом осуществляется логирование всех полученных атрибутов от агентов сбора данных (рис. 12).

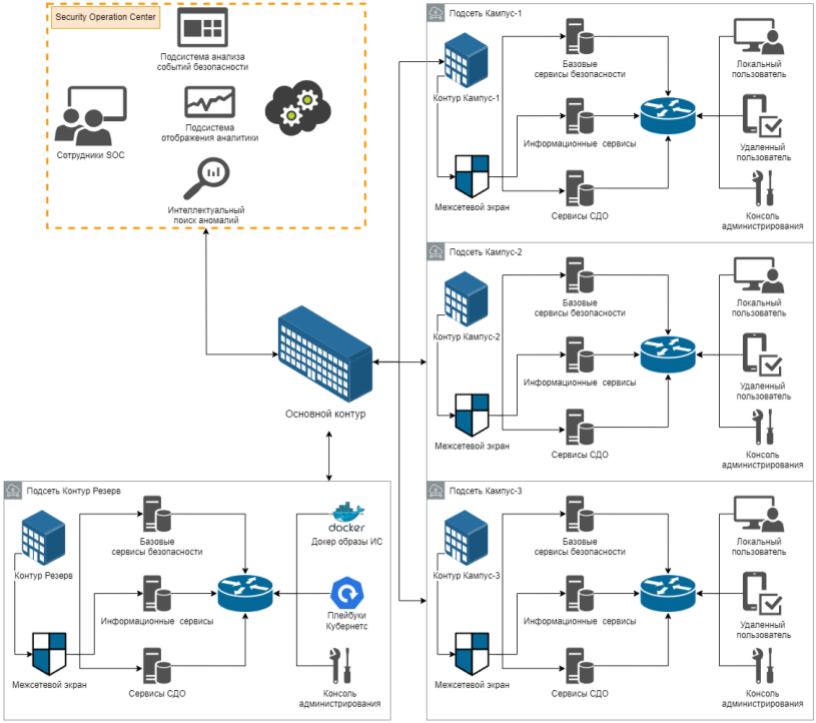

Рис. 9 — Обобщенная схема системы дистанционного образования РТУ МИРЭА

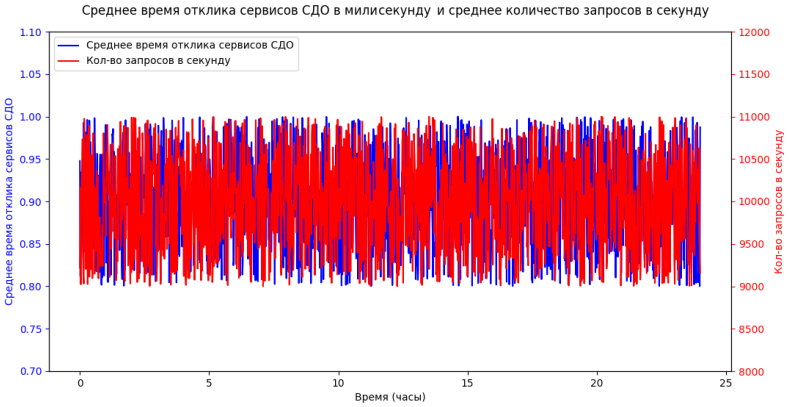

Рис. 10 — Тестирование разработанной системы управления доступом в СДО МИРЭА

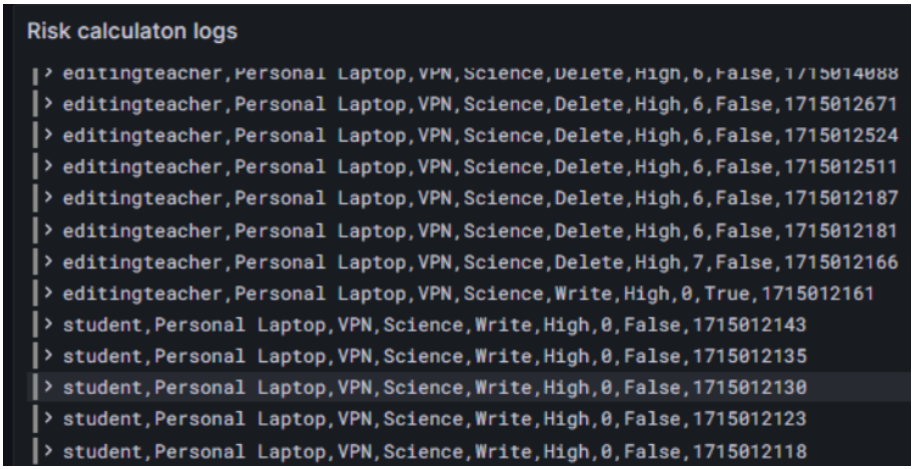

Рис. 11 — Результаты мониторинга и отображения данных о текущем значении риска разработанной системы управления доступом

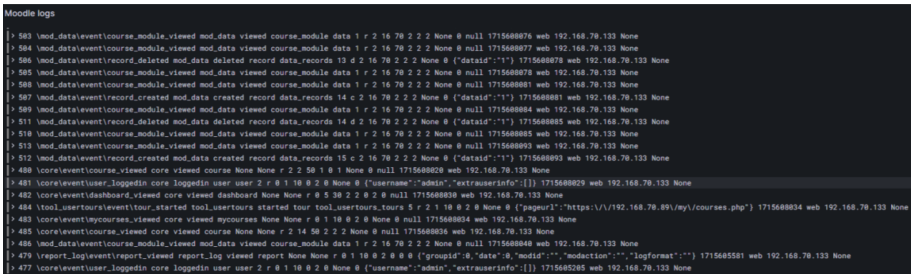

Рис. 12 — Логирование атрибутов, полученных от агентов сбора данных

Динамические атрибуты — атрибуты, которые могут меняться в зависимости от контекста или поведения пользователя. В контексте управления доступом динамические атрибуты включают: местоположение пользователя, используемое устройство, тип соединения, тип запрашиваемой операции, контекст доступа к ресурсам и психологические признаки работы пользователя в системе (модель пользователя).

Система управления доступом успешно продемонстрировала свою способность учитывать динамические атрибуты доступа в зависимости от контекста и параметров среды. Были протестированы различные сценарии, в том числе изменение места работы пользователя, использование различных устройств и сетевых сред, и система успешно изменяла уровень доступа в соответствии с заданными критериями. Одним из элементов динамических атрибутов является модель поведения пользователя.

Отслеживание активности пользователей включает в себя мониторинг поведения и взаимодействия пользователей с целевым веб-приложением. На основе собранных данных принимается решение в рамках созданных политик безопасности системы управления доступом. С веб-страниц возможно собирать множество различных событий. Ограничением выступает лишь возможности принимающей стороны (как правило, CRM или система аналитики) и платформы, на которой размещена СДО (в том числе язык программирования). Среди показателей можно выделить следующие базовые действия: клик (нажатие на кнопку, значок или область) по элементу; переход по ссылке; заполнение форм или отдельных полей; события аутентификации.

Пример сфрмированной модели пользователя на основе перемещений курсора представлен на рисунке 13.

Рис. 13 — Тепловая карта перемещения курсора пользователя для создания модели поведения пользователя

Каждый пользователь имеет уникальную тепловую карту движения курсора мыши в виду наличия психологических и биологических особенностей каждого человека. Добавив несколько дополнительных фильтров для извлечения необходимых последовательностей для пользовательских сессий, возможно более тонко изучать поведения отдельных пользователей СДО и формировать более точные модели поведения пользователей. В отличие от прочих динамических моделей на основе риска, модель на основе нечеткой логики не требует снижения доступности и удобства использования услуг ради обеспечения безопасности, при этом минимизируя расходуемые ресурсы системы.

Риск-ориентированная модель управления доступом является динамической моделью, которая функционирует в режиме реального времени

и использует контекстную информацию для принятия решений о доступе к объекту. Эта модель выполняет расчет риска по каждому запросу на доступ к объекту и принимает решение динамически на основе полученного значения риска. Риск в данном контексте выступает дополнительным атрибутом управления доступом, участвующем в процессе принятия решения о предоставлении доступа. Основные компоненты модуля управления доступом:

1. Агенты сбора данных (сенсоры) передают информацию о различных факторах риска, таких как история доступа, тип устройства, местоположение, время доступа и другие.
2. Модуль оценки значения риска использует нечеткую логику для получения значения уровня риска на основе информации, полученной от агентов сбора данных.
3. Модуль принятия решений использует результаты оценки риска для принятия решений о доступе к ресурсам.

В рамках испытаний были проведены расчеты показателей риска на основе собранных агентами безопасности атрибутов. Система успешно продемонстрировала свою способность отслеживать и анализировать эти показатели в реальном времени, а также предоставлять информацию о них в удобном для пользователя формате. Для проверки корректности применения политик безопасности на основе динамического расчета рисков, определения пороговых значений были смоделированы возможные варианты доступа к ресурсам СДО.

В ходе оценки производительности и масштабируемости разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления доступом, обрабатывались сценарии, содержащие взаимодействие большого количества пользователей и запросов для оценки конечных значений производительности или простоев. В процессе тестирования производительности и масштабируемости системы были внедрены механизмы управления доступом для системы дистанционного образования Moodle. Модернизированная система СДО была протестирована в учебной сети РТУ МИРЭА и показала высокие результаты при аутентификации пользователей с ошибкой второго рода, равной 0. Нагрузочное тестирование осуществлялось на основе тестов и созданных ботов, имитирующих поведение реальных пользователей при входе в систему СДО.

Одновременно система управления доступом смогла обработать 10000 запросов на авторизацию пользователей без снижения производительности и скорости работы для реальных пользователей. Система управления доступом должна быть способна интегрироваться с другими системами и приложениями, такими как системы управления обучением или информационные системы для учащихся.

Были выполнены тесты на совместимость разработанной системы, реализующей научно-методический аппарат риск-ориентированного атрибутивного управления, с другими системами, используемыми в процессе обучения в РТУ МИРЭА: Jupyter Lab, Wiki, Redmine, NodeJS. Были протестированы различные сценарии, включая интеграцию с системами управления учебным процессом, системами электронного документооборота и другими сервисами. Разработанная система успешно прошла проверку на совместимость с другими системами. Научно-методический аппарат может быть интегрирован в образовательные вычислительные сервисы организаций высшего образования, базирующиеся на распределенных информационных системах.

Разработанная система, реализующая научно-методический аппарат риск-ориентированного атрибутивного управления, позволяет осуществлять анализ активности пользователей в реальном времени и формирование отчетов на основе полученных данных о действиях пользователей, а также производительности системы. Сбор информации (метрик доступа) реализуется посредством системы мониторинга Prometheus.

Разработанные методы и модель, а также полученные значения эффективности разработанных мер защиты позволили создать научно-методический аппарат риск-ориентированного атрибутивного управления доступом на основе количественного анализа рисков в условиях динамически изменяющихся атрибутов доступа в распределенных информационных системах, функционирующих в системах высшего образования. Проведенные количественные и качественные оценки разработанной системы. реализующей научно-методический аппарат риск-ориентированного атрибутивного управления доступом, позволили обосновать возможность применения разработанного научно-методического аппарата риск-ориентированного атрибутивного управления доступом в образовательных вычислительных сервисах организаций высшего образования, базирующихся на распределенных информационных системах, что, в свою очередь, позволяет сделать вывод о достижении цели исследования.

В **заключении** приведены основные результаты работы, которые заключаются в следующем:

1. Сформулированы требования и ограничения, накладываемые на разрабатываемую модель управления доступом, а также методы оценки рисков, непрерывной аутентификации и оценки эффективности реализации защитных мер, позволяющие повысить защищенность объектов распределенных информационных систем от угроз информационной безопасности.
2. Разработана риск-ориентированная атрибутивная модель управления доступом, позволяющая формировать и применять динамически изменяющиеся правила доступа к объектам распределенных информационных систем в зависимости от реализуемых действий

субъектов и количественной оценки риска угроз информационной безопасности.

3. Для практической реализации риск-ориентированной атрибутивной модели управления доступом разработан метод количественной оценки рисков реализации угроз информационной безопасности, основанный на поступающей от интеллектуальных агентов информации о событиях безопасности, возникающих в процессе взаимодействия субъектов и объектов распределенных информационных систем, посредством применения математического аппарата нечеткой логики.
4. Предложенные решения в области управления доступом позволили разработать метод непрерывной аутентификации пользователей при доступе к ресурсам распределенных информационных систем, основанный на оценке психологических реакций, позволяющий в режиме реального времени осуществлять непрерывную аутентификацию пользователей.
5. Для оценки предложенных решений в области защиты ресурсов распределенных информационных систем от несанкционированного доступа разработан метод оценки эффективности реализации защитных мер, основанный на анализе затрачиваемых ресурсов при реализации разработанного метода непрерывной аутентификации и риск-ориентированной атрибутивной модели управления доступом.
6. Апробация предложенных решений осуществлялась посредством внедрения разработанного научно-методического аппарата управления доступом на основе анализа рисков и динамически изменяющихся атрибутов доступа в распределенные информационные системы на примере систем высшего образования. Полученные результаты свидетельствуют об эффективности научных и практических результатов исследования и достижения цели диссертационного исследования.

Одним из перспективных **направлений дальнейших исследований** является разработка научно обоснованных принципов и методов интеграции в разработанную риск-ориентированную атрибутивную модель управления доступом пользователей распределенных информационных систем методов искусственного интеллекта и машинного обучения, использование которых, как можно ожидать априори, обеспечит прогнозирование угроз информационной безопасности и автоматизацию адаптации правил и механизмов управления доступом пользователей распределенных информационных систем.

Публикации автора по теме диссертации

Статьи, опубликованные в рецензируемых научных журналах и изданиях, определенных ВАК РФ и Аттестационным советом УрФУ

1. *Смирнов, С. И.* Критерии и показатели оценивания качества проведения расследования инцидента информационной безопасности при целевой кибератаке [Текст] / С. И. Смирнов, М. А. Еремеев, *Ш. Г. Магомедов*, Д. А. Изергин // Russian Technological Journal. — 2024. — Т. 12, № 3. — С. 25—36. — (1,92 п. л. / 0,48 п. л.)
2. *Шитов, А. В.* Программный комплекс механизма управления доступом на основе риск-ориентированной атрибутивной модели [Текст] / А. В. Шитов, Н. Е. Стельмах, *Ш. Г. Магомедов* // International Journal of Open Information Technologies. — 2024. — Т. 12, № 6. — С. 133—142. — (0,82 п. л. / 0,27 п. л.)
3. *Магомедов, Ш. Г.* Метод оценки рисков реализации угроз несанкционированного доступа к образовательным сервисам на основе анализа событий безопасности с использованием нечеткой логики [Текст] / Ш. Г. Магомедов // Защита информации. Инсайд. — 2023. — № 6. — С. 42—49. — (0,58 п. л.)
4. *Раковский, С. А.* Обеспечение безопасности открытых проектов Python: проблема оценки потенциально разрушительного функционала [Текст] / С. А. Раковский, *Ш. Г. Магомедов* // International Journal of Open Information Technologies. — 2023. — Т. 11, № 10. — С. 113—118. — (0,42 п. л. / 0,23 п. л.)
5. *Magomedov, S.* Risky model of mobile application presentation [Текст] / S. Magomedov, M. Izergin, S. Eremeev // Journal of Computer Virology and Hacking Techniques. — 2023. — Т. 19, № 3. — С. 419—441. — (1,4 п. л. / 0,5 п. л., Scopus).
6. *Магомедов, Ш. Г.* Инструменты статистической обработки результатов онлайн тестирования студентов [Текст] / Ш. Г. Магомедов, Н. Ш. Газанова, А. В. Тарасов, Я. С. Грюкан, Е. В. Никульчев // International Journal of Open Information Technologies. — 2023. — Т. 11, № 5. — С. 94—99. — (0,45 п. л. / 0,1 п. л.)
7. *Магомедов, Ш. Г.* Архитектура вычислительного комплекса для веб-сервисов и порталов с многоуровневым контролем доступа по общедоступным сетям [Текст] / Ш. Г. Магомедов // International Journal of Open Information Technologies. — 2021. — Т. 9, № 3. — С. 36—43. — (0,64 п. л.)

8. *Nikulchev, E.* Isolated Sandbox Environment Architecture for Running Cognitive Psychological Experiments in Web Platforms [Текст] / E. Nikulchev, D. Ilin, P. Kolyasnikov, *S. Magomedov*, A. Alexeenko, A. Kosenkov, S. Malych // Future Internet. — 2021. — Т. 13, № 10. — С. 1—17. — (1,13 п. л. / 0,11 п. л., Scopus).

9. *Magomedov, S.* User's reaction time for improvement of security and access control in web services [Текст] / S. Magomedov, A. Gusev, D. Ilin, E. Nikulchev // Applied Science. — 2021. — Т. 11, № 6. — С. 2561. — (1,0 п. л. / 0,25 п. л., Scopus, WoS).

10. *Magomedov, S.* Resource Analysis of the Log Files Storage Based on Simulation Models in a Virtual Environment [Текст] / S. Magomedov, D. Ilin, E. Nikulchev // Applied Science. — 2021. — Т. 11, № 11. — С. 4718. — (1,0 п. л. / 0,25 п. л., Scopus).

11. *Magomedov, S.* Protected network architecture for ensuring consistency of 2 medical data through validation of user behavior and DICOM 3 archive integrity [Текст] / S. Magomedov, A. Lebedev // Applied Science. — 2021. — Т. 11, № 5. — С. 2072. — (1,3 п. л. / 1,0 п. л., Scopus, WoS).

12. *Magomedov, S.* Software for analyzing security for healthcare organizations [Текст] / S. Magomedov // Communications in Computer and Information Science. — 2021. — Т. 1395. — С. 181—189. — (1,0 п. л., Scopus).

13. *Magomedov, S. G.* Automatic parallelization of affine programs for distributed memory systems [Текст] / S. G. Magomedov, A. S. Lebedev // Communications in Computer and Information Science. — 2021. — Т. 1396. — С. 91—101. — (1,0 п. л. / 0,1 п. л., Scopus).

14. *Magomedov, S. G.* A system for off-line validation of medical data in DICOM archive [Текст] / S. G. Magomedov // Journal of Physics: Conference Series. — 2021. — Т. 1727. — С. 012011. — (0,42 п. л., Scopus).

15. *Shaporenko, M.* A technique for analyzing banking transactions to identify fraudulent activities in E-commerce [Текст] / M. Shaporenko, *S. Magomedov*, A. Lebedev // IEEE 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET). — 2021. — С. 1—4. — (0,32 п. л. / 0,15 п. л., Scopus).

16. *Магомедов, Ш. Г.* Архитектура информационной системы для проверки подлинности медицинских данных в архиве DICOM [Текст] / Ш. Г. Магомедов // International Journal of Open Information Technologies. — 2020. — Т. 8, № 10. — С. 84—89. — (0,46 п. л.)

17. *Magomedov, S. G.* Using of redundant signed-digit numeral system for accelerating and improving the accuracy of computer floating-point calculations [Текст] / S. G. Magomedov, S. A. Otsokov // International Journal of Advanced Computer Science and Applications. — 2020. — Т. 11, № 9. — С. 357—363. — (0,45 п. л. / 0,15 п. л., Scopus).

18. *Magomedov, S.* Dataset of User Reactions When Filling Out Web Questionnaires [Текст] / S. Magomedov, D. Ilin, A. Silaeva, E. Nikulchev // Data. — 2020. — Т. 5, № 4. — С. 1—7. — (0,45 п. л. / 0,15 п. л., Scopus).

19. *Nikulchev, E.* Digital Psychological Platform for Mass Web-Surveys [Текст] / E. Nikulchev, D. Ilin, A. Silaeva, P. Kolyasnikov, V. Belov, A. Runtov, P. Pushkin, N. Laptev, A. Alexeenko, *S. Magomedov*, A. Kosenkov, I. Zakharov, V. Istamullina, S. Malykh // Data. — 2020. — Т. 5, № 4. — С. 1—16. — (1,0 п. л. / 0,05 п. л., Scopus).

20. *Magomedov, S. G.* On the possibility of implementing high-precision calculations in residue numeral system [Текст] / S. G. Magomedov, S. A. Otsokov // International Journal of Advanced Computer Science and Applications. — 2019. — Т. 10, № 11. — С. 9—13. — (0,35 п. л. / 0,25 п. л., WoS).

21. *Magomedov, S. G.* Forming the composition of functions and instructions of microprocessor devices for access control systems [Текст] / S. G. Magomedov, V. P. Los // Automatic Control and Computer Sciences. — 2019. — Т. 53, № 8. — С. 883—888. — (0,35 п. л. / 0,25 п. л., Scopus).

22. *Магомедов, Ш. Г.* Особенности использования микропроцессорных устройств в системах контроля доступа [Текст] / Ш. Г. Магомедов, Ф. И. Шамхалов // Промышленные АСУ и контроллеры. — 2018. — № 3. — С. 16—19. — (0,28 п. л. / 0,14 п. л.)

23. *Магомедов, Ш. Г.* Формирование состава типовых макроопераций для систем разграничения и контроля доступа [Текст] / Ш. Г. Магомедов // Информация и безопасность. — 2018. — Т. 21, № 1. — С. 118—123. — (0,45 п. л.)

24. *Магомедов, Ш. Г.* Классификация рубежей доступа и связанных с ними факторов влияния в системе контроля доступа [Текст] / Ш. Г. Магомедов // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника и информатика. — 2018. — № 1. — С. 62—70. — (0,40 п. л.)

25. *Magomedov, S. G.* Increasing the efficiency of microprocessors in an access control systems [Текст] / S. G. Magomedov // International Journal of Engineering and Technology (UAE). — 2018. — Т. 7, № 4. — С. 80—83. — (0,25 п. л., Scopus).

26. *Magomedov, S.* Anomaly detection with machine learning and graph databases in fraud management [Текст] / S. Magomedov, S. Pavelyev, I. Ivanova, A. Dobrotvorsky, M. Khrestina, T. Yusubaliev // International Journal of Advanced Computer Science and Applications. — 2018. — Т. 9, № 11. — С. 33—38. — (0,35 п. л. / 0,15 п. л., Scopus).

27. *Magomedov, S. G.* Application of artificial intelligence technologies for the monitoring of transactions in aml-systems using the example of the developed classification algorithm [Текст] / S. G. Magomedov, A. S. Dobrotvorsky, M. P. Khrestina, S. A. Pavelyev, T. R. Yusubaliev // International Journal of Engineering and Technology (UAE). — 2018. — Т. 7, № 4. — С. 76—79. — (0,35 п. л. / 0,15 п. л., Scopus).

28. *Magomedov, S. G.* The technology of secure dataprocessing in production systems based on the use of special microcontrollers [Текст] / S. G. Magomedov // International Journal of Engineering and Technology (UAE). — 2018. — Т. 7, № 4. — С. 84—87. — (0,45 п. л., Scopus).

29. *Magomedov, S. G.* An approach to emergency situation forecasting in the field of road maintenance based on big data analysis [Текст] / S. G. Magomedov, I. I. Antonova, V. V. Nikonov, E. M. Mikliaev // International Journal of Engineering and Technology (UAE). — 2018. — Т. 7, № 4. — С. 88—91. — (0,35 п. л. / 0,10 п. л., Scopus).

30. *Magomedov, S. G.* Organization of Secured Data Transfer in Computers Using Sign-Value Notation [Текст] / S. G. Magomedov // ITM Web of Conference. — 2017. — Т. 10. — No. 04004. — (0,35 п. л., Scopus).

31. *Магомедов, Ш. Г.* Место контроля доступа в системах обеспечения информационной безопасности объектов обработки данных [Текст] / Ш. Г. Магомедов, В. П. Лось, Е. Д. Тышук // Информация и безопасность. — 2017. — Т. 20, № 3. — С. 356—361. — (0,45 п. л. / 0,15 п. л.)

32. *Магомедов, Ш. Г.* Построение системы обмена закрытыми данными в вычислительных сетях на основе использования систем счисления остаточных классов [Текст] / Ш. Г. Магомедов // Промышленные АСУ и контроллеры. — 2017. — № 1. — С. 42—46. — (0,24 п. л.)

33. *Магомедов, Ш. Г.* Выбор оптимального варианта совершенствования системы защиты информации [Текст] / Ш. Г. Магомедов // Промышленные АСУ и контроллеры. — 2017. — № 3. — С. 47—51. — (0,54 п. л.)

34. *Магомедов, Ш. Г.* Мультиагентный подход для защиты данных в информационном тумане [Текст] / Ш. Г. Магомедов, В. П. Лось, Г. В. Росс // Промышленные АСУ и контроллеры. — 2017. — № 6. — С. 47—50. — (0,45 п. л. / 0,15 п. л.)

35. *Магомедов, Ш. Г.* Построение моделей описания рисков охранных действий по защите внешних периметров организации [Текст] / Ш. Г. Магомедов, В. Ф. Шуршев, Г. А. Попов, А. Ф. Дорохов, М. Ф. Руденко // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника и информатика. — 2017. — № 3. — С. 31—39. — (0,48 п. л. / 0,18 п. л.)

36. *Магомедов, Ш. Г.* Системный анализ процесса разграничения доступа при дискреционной политике управления [Текст] / Ш. Г. Магомедов, Ю. В. Колотилов // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника и информатика. — 2017. — № 4. — С. 39—44. — (0,5 п. л. / 0,25 п. л.)

37. *Magomedov, S.* Big data processing for full-text search and visualization with elasticsearch [Текст] / S. Magomedov, A. Voit, A. Stankus, I. Ivanova // International Journal of Advanced Computer Science and Applications. — 2017. — Т. 8, № 12. — С. 76—83. — (0,45 п. л. / 0,15 п. л., Scopus).

38. *Magomedov, S.* Comparative analysis of various methods treatment expert assessments [Текст] / S. Magomedov, G. Popov // International Journal of Advanced Computer Science and Applications. — 2017. — Т. 8, № 5. — С. 35—39. — (0,2 п. л. / 0,1 п. л., Scopus).

39. *Магомедов, Ш. Г.* Обеспечение безопасности передачи данных в вычислительных сетях на основе использования систем остаточных классов [Текст] / Ш. Г. Магомедов, Т. Ю. Морозова, Д. А. Акимов // Проблемы информационной безопасности. Компьютерные системы. — 2016. — № 3. — С. 43—47. — (0,52 п. л. / 0,18 п. л.)

40. *Магомедов, Ш. Г.* Математическое моделирование охранных действий на объекте защиты [Текст] / Ш. Г. Магомедов // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника и информатика. — 2016. — № 1. — С. 70—80. — (0,44 п. л.)

Свидетельства о регистрации программ для ЭВМ

41. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный модуль количественной оценки рисков угроз информационной безопасности [Текст] / Ш. Г. Магомедов. — № 2024614586 ; заявл. 14.02.2024 ; опубл. 27.02.2024, 2024612847 (Рос. Федерация).

42. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный модуль риск-ориентированного управления доступом [Текст] / Ш. Г. Магомедов. — № 2024614470 ; заявл. 15.02.2024 ; опубл. 26.02.2024, 2024612919 (Рос. Федерация).

43. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный модуль интеллектуального анализа потоковых видеоданных на основе методов машинного обучения [Текст] / Ш. Г. Магомедов, А. С. Сигов, А. В. Рагуткин, И. А. Александров, М. Е. Ставровский, М. И. Сидоров, А. А. Татарканов. — № 2021664913 ; заявл. 25.08.2021 ; опубл. 15.09.2021, 2021663715 (Рос. Федерация).

44. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный модуль интеллектуального автоматизированного поиска ситуационных событий в видеопотоке [Текст] / Ш. Г. Магомедов, А. С. Сигов, А. В. Рагуткин, И. А. Александров, М. Е. Ставровский, М. И. Сидоров, А. А. Татарканов. — № 2021664645 ; заявл. 25.08.2021 ; опубл. 10.09.2021, 2021663707 (Рос. Федерация).

45. *Свидетельство о гос. регистрации программы для ЭВМ.* Конфигуратор настройки параметров работы сервера [Текст] / Ш. Г. Магомедов, А. С. Сигов, А. В. Рагуткин, И. А. Александров, М. Е. Ставровский, М. И. Сидоров, А. А. Татарканов. — № 2021664584 ; заявл. 25.08.2021 ; опубл. 09.09.2021, 2021663658 (Рос. Федерация).

46. *Свидетельство о гос. регистрации программы для ЭВМ.* Многофункциональная программная платформа видеоаналитики [Текст] / Ш. Г. Магомедов, А. С. Сигов, А. В. Рагуткин, И. А. Александров, М. Е. Ставровский, М. И. Сидоров, А. А. Татарканов. — № 2021664454 ; заявл. 31.08.2021 ; опубл. 07.09.2021, 2021663637 (Рос. Федерация).

47. *Свидетельство о гос. регистрации программы для ЭВМ.* Программный комплекс обнаружения вредоносной активности в корпоративной сети [Текст] / Ш. Г. Магомедов, С. И. Смирнов, И. А. Прибылов, Д. А. Изергин. — № 2021614531 ; заявл. 10.03.2021 ; опубл. 25.03.2021, 2021613300 (Рос. Федерация).

48. *Свидетельство о гос. регистрации программы для ЭВМ.* Программа для определения сходства семантических сетей [Текст] / Ш. Г. Магомедов, А. Г. Мустафаев, Г. Х. Ирзаев. — № 2015617768 ; заявл. 25.05.2015 ; опубл. 22.07.2015, 2015614331 (Рос. Федерация).

49. *Свидетельство о гос. регистрации программы для ЭВМ.* AeroMobileRaport [Текст] / Ш. Г. Магомедов, А. А. Бабаев, Г. С. Коняфиев, Н. Ш. Газанова, А. Т. Тарланов. — № 2021669368 ; заявл. 25.11.2021 ; опубл. 29.11.2021, 2021668781 (Рос. Федерация).

Статьи в других изданиях

50. *Магомедов, Ш. Г.* Риск-ориентированная атрибутивная модель управления доступом для организаций высшего образования [Текст] / Ш. Г. Магомедов, А. В. Козачок, А. Т. Тарланов // Правовая информатика. — 2023. — № 1. — С. 72—82. — (2,0 п. л. / 0,5 п. л.)

51. *Магомедов, Ш. Г.* Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей [Текст] / Ш. Г. Магомедов, П. В. Колясников, Е. В. Никульчев // Российский технологический журнал. — 2020. — Т. 8, № 6. — С. 34—46. — (2,04 п. л. / 0,68 п. л.)

52. *Магомедов, Ш. Г.* Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения [Текст] / Ш. Г. Магомедов // Cloud of Science. — 2020. — Т. 7, № 3. — С. 685—704. — (0,54 п. л.)

53. *Ильин, Д. Ю.* Архитектура вычислительного комплекса цифровой платформы DigitalPsyTools междисциплинарных исследований в системе образования [Текст] / Д. Ю. Ильин, П. В. Колясников, Н. В. Лаптев, А. С. Алексеенко, Е. В. Никульчев, *Ш. Г. Магомедов* // Cloud of Science. — 2020. — Т. 7, № 4. — С. 936—949. — (2,44 п. л. / 0,66 п. л.)

54. *Магомедов, Ш. Г.* Проектирование микропроцессорных устройств, разработанных для систем контроля и управления доступом [Текст] / Ш. Г. Магомедов // Cloud of Science. — 2019. — Т. 6, № 4. — С. 752—761. — (0,38 п. л.)

55. *Изергин, Д. А.* Оценка уровня информационной безопасности мобильной операционной системы Android [Текст] / Д. А. Изергин, М. А. Еремеев, С. И. Смирнов, *Ш. Г. Магомедов* // Российский технологический журнал. — 2019. — Т. 7, № 4. — С. 44—55. — (1,32 п. л. / 0,44 п. л.)

56. *Магомедов, Ш. Г.* Система автоматического распараллеливания линейных программ для машин с общей и распределенной памятью [Текст] / Ш. Г. Магомедов, А. С. Лебедев // Российский технологический журнал. — 2019. — Т. 7, № 5. — С. 7—19. — (1,04 п. л. / 0,52 п. л.)

57. *Магомедов, Ш. Г.* Алгоритмы и структуры преобразования числовых данных из позиционной системы счисления в систему остаточных классов [Текст] / Ш. Г. Магомедов, Ш. М. А. Исмаилов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. — 2018. — 5(65). — С. 159—169. — (1,1 п. л. / 0,84 п. л.)

58. *Магомедов, Ш. Г.* Управление технологическим процессом формирования структур интегральных элементов [Текст] / Ш. Г. Магомедов, А. Г. Мустафаев, А. М. Савинова // Вестник Астраханского государственного технического университета. Серия: Управление. Вычислительная техника и информатика. — 2012. — № 2. — С. 56—61. — (0,73 п. л. / 0,58 п. л.)